ARTICLES AND SPEECHES

INTRODUCTION TO REGULATING INNOVATION IN HEALTHCARE: PROTECTING THE PUBLIC OR STIFLING PROGRESS?  
KATHY L. CERMINARA
Marilyn Uzdavines

THE PERSISTENCE OF OPPORTUNISTIC BUSINESS MODELS IN HEALTHCARE AND A STRONGER ROLE FOR INSURANCE REGULATORS IN CONTAINING HEALTH CARE COSTS  
JACKSON WILLIAMS

STATE LAW GOVERNANCE OF HEALTH INFORMATION TECHNOLOGY  
CASON SCHMIT

KEEPING INTERNET PIRATES AT BAY: RANSOMWARE NEGOTIATION IN THE HEALTHCARE INDUSTRY  
PAUL R. DEMURO

PATIENT SAFETY SHOULD INCLUDE PATIENT PRIVACY: THE SHORTCOMINGS OF THE FDA’S RECENT DRAFT GUIDANCE REGARDING CYBERSECURITY OF MEDICAL DEVICES  
CHRISTOPHER KERSBERGEN

CARDIAC DEFIBRILLATORS NEED TO HAVE A BULLETPROOF VEST: THE NATIONAL SECURITY RISKPOSED BY THE LACK OF CYBERSECURITY IN IMPLANTABLE MEDICAL DEVICES  
MICHAEL WOODS
NOVA LAW REVIEW

VOLUME 41    SPRING 2017    ISSUE 3

EXECUTIVE BOARD

ALISON P. BARBIERO
Editor-in-Chief

JOSEPH R. KADIS
Executive Editor

TIMOTHY D. SHIELDS
Managing Editor

KRISTAL A. ACOSTA
Lead Articles Editor

SAMANTHA E. BOWEN
Lead Technical Editor

ARTICLES EDITORS

OLIVIA S. CHIONG
KRISTI DE SOIZA
MICHELLE DIAZ
ELYSE MALOUF
DINA L. ROSENBAUM
MARIA D. VERA

ASSOCIATE EDITORS

CHANELLE J. VENTURA
Assistant Lead Articles Editor

ALEC ZAVELL
Assistant Lead Technical Editor

RICHARD J. RAFULS
Goodwin Editor

CHRISTAL ROBINSON
Alumni Relations Editor

FACULTY ADVISORS

HEATHER BAXTER
ELINA MARTY-NELSON

Published by NSUWorks, 2017
SENIOR ASSOCIATES

KAREN BLACK
DAIRON BUEIRO
NATALIE CIMADEVILLA
ALEXANDER DEFILIPPO
NADIA ENNAJI
MIGUEL A. ESPINOSA III

LILIAN GUZMAN
JAZLYN JUDA
DOREEN MONK
HENRY NORWOOD
MAXWELL H. SAWYER
SAMANTHA E. SCHEFF

JUNIOR ASSOCIATES

STEPHEN O. AYENI JR.
CLAUDIA CUADOR
AMANDA L. DECKER
PAUL V. DENT III
MARIA G. DIAZ DELGADO
BRITTANY EHRENMAN
BRANDON FERNÁNDEZ
VANESSA FONTS
JONATHAN D. GOMER
STEPHEN C. JIMENEZ
SHAMAYIM KASKEL
SHERISSE A. C. LEWIS
STEPHANIE M. MARTIN

NADINE W. MATHIEU
MAYDA Z. NAHHAS
JAMIE KAINALU NAKOA
NICHOLAS A. PALOMINO
BETHANY PANDHER
MICHAEL PEDOWITZ
OMAR J. PEREZ
BRITTNEY I. POLO
ADRIENNE RODRIGUEZ
SHIRLEY SHARON
SAMI SLIM
MORGAN SPENCER
ADAM R. WAGNER
NOVA SOUTHEASTERN UNIVERSITY
SHEPARD BROAD COLLEGE OF LAW

ADMINISTRATION

OFFICE OF THE DEAN
Jon M. Garon, B.A., J.D. Dean & Professor of Law
Debra Moss Curtis, B.A., J.D., Associate Dean for Academic Affairs &
Professor of Law
Tracey-Ann Spencer Reynolds, Executive Assistant to Dean Jon M. Garon
Lynda Harris, Executive Assistant to Associate Dean for Academic Affairs

DEANS AND DIRECTORS
Lynn Acosta, B.A., M.S., Assistant Dean for Student Services
Catherine Arcabascio, B.A., J.D., Associate Dean for International
Programs & Professor of Law
Timothy Arcaro, B.S., J.D., Associate Dean for AAMPLE and Online
Programs & Professor of Law
Sara Berman, B.A., J.D., Director of Critical Skills Program and Academic
Support
Megan F. Chaney, B.A., J.D., Director of Trial & Appellate Advocacy &
Professor of Law
Laura Dietz, Director of Alumni Relations
Olympia R. Duhart, B.A., J.D., Director of Legal Research and Writing
Program & Professor of Law
Jennifer Gordon, J.D., Director of Public Interest Programs
Richard Grosso, B.S., J.D., Director, Environment & Land Use Law Clinic
& Professor of Law
Elena Maria Marty-Nelson, B.A., J.D., LL.M., Associate Dean for
Diversity, Inclusion, and Public Impact & Professor of Law
Jennifer McIntyre, B.S., M.S., Assistant Dean for Online Programs
Joshua Metz, B.S., B.A., CPA, Director of Administrative Operations
Elena Rose Minicucci, B.A., J.D., Director of Alumni Relations, Critical
Skills Director & Adjunct Professor of Law
Frank A. Orlando, B.S., J.D., Director of the Center for the Study of Youth
Policy and Adjunct Professor
William D. Perez, Assistant Dean of Admissions
Nancy Sanguigni, B.S., M.B.A., Assistant Dean for Clinical Programs
Susan Stephan, B.S., J.D., M.A., Director of Development & Adjunct
Professor of Law
Michele N. Struffolino, B.A., M.Ed., J.D., Associate Dean of Students & Professor of Law
Fran L. Tetunic, B.A., J.D., Director, Alternative Dispute Resolution Clinic & Professor of Law
Chelsea Thorn, M.S., Director for Recruitment Marketing, Communications, and Publications

LAW LIBRARY & TECHNOLOGY CENTER ADMINISTRATION
Rebecca A. Rich, A.B., M.S., J.D., Senior Associate Director, Law Library and Technology Center & Adjunct Professor of Law
Wanda Hightower, Assistant to the Associate Dean of the Law Library & Technology Center
Beth Parker, Assistant Director, Operations and Collections
Nikki Williams, Assistant Circulation Manager
Alison Rosenberg, Assistant Director of Research and Reference Services
Rob Beharriell, B.A., J.D., Outreach and Reference Services Librarian & Adjunct Professor of Law
Michelle Murray, Research and Reference Services Librarian
Daniel Buggs, Technical Services Assistant
Susana Franklin, Technical Services Assistant

STAFF
Tresha Barracks, Legal Assistant for Clinical Programs
Mary Butler, Coordinator of Advanced Lawyering Skills & Values
Lakaye Carter, Admissions Coordinator
Wendy Clasen, Administrative Assistant for Clinical Programs
Natalia Enfort, B.S., Graduation & Records Advisor for Student Services
Robert Jacobs, Secretary for Critical Skills Program
Jessica Mcfarlane, Secretary for Critical Skills Program
Jesse Monteagudo, Legal Secretary
Kathleen Perez, Assistant to the Director of Alumni & Development
Nicole Rodriguez, Building Operations Manager
Catherine Zografos, Administrative Assistant to the Career & Professional Development Office
Naomi Scheiner, Administrative Coordinator for Student Affairs
Chantelle Spence, Faculty Assistant
FACULTY

FULL-TIME FACULTY
Catherine Arcabascio, B.A., J.D., Associate Dean for International Programs & Professor of Law
Timothy Arcaro, B.S., J.D., Associate Dean for AAMPLE and Online Programs & Professor of Law
Heather Baxter, B.A., J.D., Assistant Professor of Law
Brion Blackwelder, B.S., J.D., Director of Children & Families Clinic & Associate Professor of Law
Randolph Braccialarghe, B.A., J.D., Professor of Law
Ronald B. Brown, B.S.M.E., J.D., LL.M., Professor of Law
Timothy A. Canova, B.A., J.D., Professor of Law and Public Finance
Kathy Cerminara, B.S., J.D., LL.M., J.S.D., Professor of Law
Megan F. Chaney, B.A., J.D., Director of Trial & Appellate Advocacy & Professor of Law
Phyllis G. Coleman, B.S., M.Ed., J.D., Professor of Law
Leslie L. Cooney, B.S., J.D., Professor of Law
Jane E. Cross, B.A., J.D., Director of Caribbean Law Program & Associate Professor of Law
Debra Moss Curtis, B.A., J.D., Associate Dean for Academic Affairs & Professor of Law
Michael J. Dale, B.A., J.D., Professor of Law
Mark Dobson, A.B., J.D., LL.M., Professor of Law
Douglas L. Donoho, B.A., J.D., LL.M., Professor of Law
Olympia R. Duhart, B.A., J.D., Director of Legal Research and Writing Program & Professor of Law
Michael Flynn, B.A., J.D., Professor of Law
Amanda M. Foster, B.A., J.D., Associate Professor of Law
Jon M. Garon, B.A., J.D., Dean & Professor of Law
Pearl Goldman, B.C.L., M. Phil., LL.B., J.D., LL.M., Professor of Law
Joseph M. Grohman, B.A., M.A., J.D., Professor of Law
Richard Grosso, B.S., J.D., Director, Environment & Land Use Law Clinic & Professor of Law
Linda F. Harrison, B.A., J.D., Associate Professor of Law
Joseph Hnylka, B.A., J.D., Associate Professor of Law
Areti Imoukhuede, B.A., J.D., Professor of Law
Robert M. Jarvis, B.A., J.D., LL.M., Professor of Law
Judith R. Karp, B.A., M.L.S., J.D., Professor of Law
Shahabudeen Khan, J.D., Associate Professor of Law
Ishaq Kundawala, B.A., J.D., Professor of Law
Camille Lamar, B.A., J.D., Professor of Law
James B. Levy, B.A., J.D., Associate Professor of Law
Kenneth L. Lewis Jr., B.S., M.S., J.D., Assistant Professor of Law
Donna Litman, A.B., J.D., Professor of Law
Elena Maria Marty-Nelson, B.A., J.D., LL.M., Associate Dean for
Diversity, Inclusion, and Public Impact & Professor of Law
Michael R. Masinter, B.A., J.D., Professor of Law
Jani E. Maurer, B.A., J.D., Professor of Law
Joel A. Mintz, B.A., J.D., LL.M., J.S.D., Professor of Law
Roma Perez, B.A., J.D., Professor of Law
Michael L. Richmond, A.B., M.S.L.S., J.D., Professor of Law
John Sanchez, B.A., J.D., LL.M., Professor of Law
Florence Shu-Acquaye, LL.B., LL.M., J.S.M., J.S.D., Professor of Law
Michele N. Struffolino, B.A., M.Ed., J.D., Associate Dean of Students &
Professor of Law
Fran L. Tetunic, B.A., J.D., Director, Alternative Dispute Resolution Clinic
& Professor of Law
Marilyn Uzdavines, B.A., J.D., Assistant Professor of Law
Kathryn Webber, B.A., J.D., Associate Professor of Law
James D. Wilets, B.A., M.A., J.D., Professor of Law

EMERITUS FACULTY
John Anderson, J.D., Professor Emeritus of Law
Marilyn Cane, B.A., J.D., Professor Emerita of Law
Lynn A. Epstein, B.S., J.D., Professor Emerita of Law
Joseph Harbaugh, B.S., LL.B., LL.M, Dean Emeritus, Professor Emeritus
of Law
Howard Messing, A.B., J.D., Professor Emeritus of Law
Gail Richmond, A.B., M.B.A., J.D., Professor Emerita of Law
Bruce S. Rogow, B.B.A., J.D., Professor Emeritus of Law
Marc Rohr, B.A., J.D., Professor Emeritus of Law
Michael Rooke-Ley, J.D., Professor Emeritus of Law
Joseph Smith, J.D., Professor Emeritus of Law
Steven Wisotsky, B.A., J.D., LL.M., Professor Emeritus of Law

CRITICAL SKILLS PROGRAM INSTRUCTORS
Sara Berman, B.A., J.D., Director of Critical Skills Program and Academic
Support
Meg Chandelle, B.S., M.B.A., J.D., Critical Skills Instructor & Adjunct
Professor of Law
Robert Gregg, B.A., J.D., Critical Skills Instructor
Chance Meyer, B.S., J.D., Critical Skills Instructor & Adjunct Professor of Law
Elena Rose Minicucci, B.A., J.D., Director of Alumni Relations, Critical Skills Director & Adjunct Professor of Law
Heddy Muransky, B.A., M.Ed., J.D., Critical Skills Instructor
Marlene Murphy, Critical Skills Instructor & Adjunct Professor of Law
Rodney Rawls, B.S., J.D., LL.M., Critical Skills Instructor

**ADJUNCT FACULTY**
Andrew L. Adler, B.A., J.D., Adjunct Professor of Law
Edward R. Almeyda, B.S., J.D., Adjunct Professor of Law
Rifat Azam, Adjunct Professor of Law
Ross L. Baer, B.A., J.D., Adjunct Professor of Law
Steven Ballinger, B.A., J.D. Adjunct Professor of Law in the Master of Science Program
Roshawn Banks, B.S., J.D., Adjunct Professor of Law
Courtney Jared Bannan, Adjunct Professor of Law
Rob Beharriell, J.D., M.L.I.S., Outreach and Reference Services Librarian, & Adjunct Professor of Law
Christopher E. Benjamin, B.A., J.D., Adjunct Professor of Law in the Master of Science Program
Richard H. Bergman, Adjunct Professor of Law
Paul D. Bianco, Adjunct Professor of Law
Vanesti E. Brown, B.S., J.D., Adjunct Professor of Law in the Master of Science Program
Robert Campbell, Adjunct Professor of Law in the Master of Science Program
Laura Cancilla-Miller, Adjunct Professor of Law in the Master of Science Program
Lydia B. Cannizzo, Adjunct Professor of Law in the Master of Science Program
Meg Chandelle, B.S., M.B.A., J.D., Critical Skills Instructor & Adjunct Professor of Law
Michele Chang, Adjunct Professor of Law in the Master of Science Program
Tracey L. Cohen, J.D., B.A., Adjunct Professor of Law
Jude Cooper, Adjunct Professor of Law
Arthur T. Daus III, B.A., J.D., Adjunct Professor of Law
Rachel Turner Davant, B.A., J.D., Adjunct Professor of Law in the Master of Science Program
Hon. Robert F. Diaz, A.A., B.A., J.D., Adjunct Professor of Law
Ken S. Direktor, Adjunct Professor of Law
Gerald Donnini II, B.B.A., J.D., LL.M, Adjunct Professor of Law
Cynthia Henry Duval, B.A., J.D., Associate Director of Career and Professional Development & Adjunct Professor of Law
Hon. Rex J. Ford, Adjunct Professor of Law
Amy M. Foust, B.A., J.D., Adjunct Professor of Law
John A. Frusciante, Adjunct Professor of Law
Myrna Galligano-Kozlowski, Adjunct Professor of Law in the Master of Science Program
Daniel Krawiec, Adjunct Professor of Law in the Master of Science Program
Andrew Garofalo, Adjunct Professor of Law
Jason A. Glusman, B.A., J.D., Adjunct Professor of Law
Adam Scott Goldberg, B.S., J.D., LL.M., Adjunct Professor of Law
Evan J. Goldman, Adjunct Professor of Law
Anthony Gonzales, B.A., J.D., Adjunct Professor of Law
Carlos F. Gonzalez, Adjunct Professor of Law
Saman M. Gonzalez, B.A., J.D., Adjunct Professor of Law
Shanika A. Graves, Adjunct Professor of Law
Tonja Haddad-Coleman, J.D., Adjunct Professor of Law
Ross Hartog, B.S., J.D., Adjunct Professor of Law
A. Margaret Hesford, Adjunct Professor of Law
Peter Homer, B.A., J.D., M.B.A., Adjunct Professor of Law
Hon. Alfred Horowitz, B.A., J.D., LL.M., Adjunct Professor of Law
Julie E. Hough, Adjunct Professor of Law
Jacqueline F. Howe Esq., Adjunct Professor of Law
Nick Jovanovich, B.S., J.D., LL.M., Adjunct Professor of Law
Kimberly Kanoff Berman, Adjunct Professor of Law
Connie Kaplan, B.S., J.D., Adjunct Professor of Law
Neil Karadbil, Adjunct Professor of Law
Jason Katz, Adjunct Professor of Law
Daniel Kaufman, B.S., J.D., Adjunct Professor of Law
Kamran Khurshid, B.A., J.D., Adjunct Professor of Law
Daniel Krawiec, Adjunct Professor in the Master of Science Program
Sandra E. Krumbein, B.A., M.S., J.D., Adjunct Professor of Law
Warren Kwavnick, Adjunct Professor of Law
Cathy Lerman, B.A., M.B.A., J.D., Adjunct Professor of Law
Allan M. Lerner, B.A., J.D., Adjunct Professor of Law
James Lewis, Adjunct Professor of Law
Rochelle Marcus, B.S., M.Ed., J.D., Adjunct Professor of Law
Raymond G. Massie, B.A., J.D., LL.M., Adjunct Professor of Law
Chance Meyer, B.S., J.D., *Critical Skills Instructor & Adjunct Professor of Law*

Catherine M. Michael, *Adjunct Professor of Law in the Master of Science Program*

Daniel Mielnicki, *Adjunct Professor of Law*

Elena Rose Minicucci, B.A., J.D., *Director of Alumni Relations, Critical Skills Director & Adjunct Professor of Law*

Gerald M. Morris, B.A., J.D., LL.M, *Adjunct Professor of Law in the Master of Science Program*

Charles B. Morton, Jr., B.A., J.D., *Adjunct Professor of Law*

Marlene Murphy, *Critical Skills Instructor & Adjunct Professor of Law*

Jennifer D. Newton, B.S., J.D., *Adjunct Professor of Law in the Master of Science Program*

Robert N. Nicholson, *Adjunct Professor of Law*

Kamlesh Oza, *Adjunct Professor of Law*

Vanessa L. Prieto Esq., *Adjunct Professor of Law*

Rebecca A. Rich, A.B., M.S., J.D., *Senior Associate Director, Law Library and Technology Center & Adjunct Professor of Law*

Michael J. Rocque, *Adjunct Professor of Law*

Jose A. Rodriguez-Dod, B.S., J.D., *Adjunct Professor of Law*

Morgan Rood, *Adjunct Professor of Law*

Thomas ‘Tom’ E. Runyan Esq., *Adjunct Professor of Law*

Amy Roskin, B.A., M.D., J.D., *Adjunct Professor of Law in the Master of Science Program*

Maria Schneider, B.A., J.D., *Adjunct Professor of Law*

Robert H. Schwartz, *Adjunct Professor of Law*

Stacy Schwartz, B.S., J.D., *Adjunct Professor of Law*

Neal B. Shniderman, B.A., J.D., *Adjunct Professor of Law*

Jodi Siegel, *Adjunct Professor of Law in the Master of Science Program*

Scott Smiley, BSEE, J.D., *Adjunct Professor of Law*

Grasford Smith, B.S., J.D., *Adjunct Professor of Law in the Master of Science Program*

Mindy F. Solomon, B.S., J.D., *Adjunct Professor of Law*

Susan Stephan, B.S., J.D., M.A., *Director of Development & Adjunct Professor of Law*

Richard Stone, *Adjunct Professor of Law*

Maxine K. Streeter, B.A., J.D., *Adjunct Professor of Law*

Jennifer Swirsky, B.S., J.D., *Adjunct Professor of Law in the Master of Science Program*

Meah Tell, Esq., B.A., M.B.A., J.D., LL.M, *Adjunct Professor of Law*

Steven Tepler, *Adjunct Professor of Law*

Damian Thomas, *Adjunct Professor of Law*
Emilie M. Tracy Esq., *Adjunct Professor of Law*
Dawn Traverso, B.A., J.D., *Adjunct Professor of Law*
Laura Varela, B.A., J.D., *Adjunct Professor of Law*
Marilyn Vestal, *Adjunct Professor of Law*
Ethan Wall, *Adjunct Professor*
Lee Weintraub, B.S., B.A., J.D., *Adjunct Professor of Law*
Camille L. Worsnop, B.S., J.D., LL.M., *Adjunct Professor of Law*
It is the policy of Nova Law Review to support equality of opportunity. No person shall be denied membership in Nova Law Review or participation in any of its activities on the basis of race, color, religion, national or ethnic origin, sex, sexual orientation, age, or disability.

PERMISSION

Nova Law Review hereby grants permission to nonprofit organizations to reproduce and distribute the contents of its journal, in whole or in part, for educational purposes, including distribution to students, provided that the copies are distributed at or below cost and identify the author, Nova Law Review, the volume, the number of the first page of the article, the year of publication, and proper notice is affixed to each copy—unless, a separate copyright notice of an author appears on the article. All other rights reserved. All other inquiries for permission, including articles with a separate copyright notice of an author, should be sent to the attention of the Editor-in-Chief.

MANUSCRIPTS

Nova Law Review invites submissions of unsolicited manuscripts. Articles submitted to Nova Law Review should conform to the guidelines set forth in The Bluebook: A Uniform System of Citation (20th ed. 2015). Articles may be submitted via mail, or e-mail and must be available on Microsoft Word. E-mail submissions may be sent to the Assistant Lead Articles Editor, accessible at http://nsulaw.nova.edu/students/orgs/lawreview/. All articles not chosen for publication are discarded after consideration. Nova Law Review does not assume responsibility for the return of any materials.

SUBSCRIPTIONS

The Nova Law Review is published three times per year by students of the Shepard Broad College of Law. The current annual subscription rate is $35.00. Single issues are available for $12.00. Canadian subscribers should add $5.00 for postage fees. Foreign subscribers should add $20.00 for postage fees. Subscriptions are automatically renewed unless notification to the contrary is received by Nova Law Review.

Please notify Nova Law Review of any changes of address at least 30 days prior to issue release for the change to take effect. The postal service will not forward your copies unless extra postage is provided by the subscriber. Duplicate copies will not be sent free of charge. Subscribers should report non-receipt of copies within 1 month of the expected mailing date. Address any correspondence to:

Nova Law Review
Shepard Broad College of Law
3305 College Avenue
Fort Lauderdale, Florida 33314
Phone: (954) 262-6196
ARTICLES AND SPEECHES

INTRODUCTION TO REGULATING INNOVATION IN HEALTHCARE: PROTECTING THE PUBLIC OR STIFLING PROGRESS? ........................................... KATHY L. CERMINARA MARILYN UZDAVINES 305

THE PERSISTENCE OF OPPORTUNISTIC BUSINESS MODELS IN HEALTH CARE AND A STRONGER ROLE FOR INSURANCE REGULATORS IN CONTAINING HEALTH CARE COSTS ........................................ JACKSON WILLIAMS 313

STATE LAW GOVERNANCE OF HEALTH INFORMATION TECHNOLOGY ........................................ CASON SCHMIT 341

KEEPING INTERNET PIRATES AT BAY: RANSOMWARE NEGOTIATION IN THE HEALTHCARE INDUSTRY ........................................... PAUL R. DEMURO 349

PATIENT SAFETY SHOULD INCLUDE PATIENT PRIVACY: THE SHORTCOMINGS OF THE FDA’S RECENT DRAFT GUIDANCE REGARDING CYBERSECURITY OF MEDICAL DEVICES ........................................ CHRISTOPHER KERSBERGEN 397

CARDIAC DEFIBRILLATORS NEED TO HAVE A BULLETPROOF VEST: THE NATIONAL SECURITY RISK POSED BY THE LACK OF CYBERSECURITY IN IMPLANTABLE MEDICAL DEVICES ........................................ MICHAEL WOODS 419
INTRODUCTION TO REGULATING INNOVATION IN HEALTHCARE: PROTECTING THE PUBLIC OR STIFLING PROGRESS?

KATHY L. CERMINARA
MARILYN UZDAVINES

I. INTRODUCTION

Growing up seeing flames leaping and smoke billowing out of the smokestacks of steel mills along the river, children of southwestern Pennsylvania in the 1960s tended to develop one of two attitudes toward regulation in general. As the 1960s faded into the 1970s, it was regulation that rid the neighborhood of the rotten-egg stench of sulfurous fumes. It was regulation that cleared the air so that air quality index warnings receded into the past, enabling all citizens, including the elderly and young children, to go outside every day. Along with the clearer skies and non-toxic air, however, came the decline of the American steel industry. Certainly regulation was not the sole cause of that decline, and one also can attribute the decrease in pollution to the decline, but industry blamed increased environmental regulation in part for high production costs that led to foreign steel dominance. By 1983, unemployment had hit 13.9% in Allegheny County, home of Pittsburgh, the industrial center of the area. Mills continued to close up and down the Monongahela River Valley over the next few years, and it was easy for millworkers and their families to focus on the negatives of regulation, holding it responsible for at least part of their economic strife.

The tall, steep hill across the Monongahela River from the Clairton Works steel mill, however, demonstrates the benefits of regulation. During the 1960s and 1970s, no plant would grow on that hillside. Poisonous haze and particulates prevented any greenery from sprouting. Lacking vegetation anchoring the scant dirt covering its rocks, that hillside gave way periodically, and drivers had to detour around rockslide after rockslide closing the road below. Beginning with the onset of environmental regulation and continuing today, thanks to regulation, the hillside is covered in greenery holding the soil firmly in place. There are no more rockslides. The regulation some blamed at least in part for their misfortune was that

1. Bill Toland, In desperate 1983, there was nowhere for Pittsburgh’s economy to go but up, PGH. POST-GAZETTE (Dec. 23, 2012, 10:00 AM), http://www.post-gazette.com/business/businessnews/2012/12/23/In-desperate-1983-there-was-nowhere-for-Pittsburgh-s-economy-to-go-but-up/stories/201212230258.
2. Id.
hillside’s savior. Those enjoying clear skies and breathing cleaner air also were thankful for that greenery, the sight of which still pre-disposes some to look favorably upon regulation of business in general.

II. REGULATION OF THE FREE MARKET GUIDED BY ETHICS

This symposium issue of the *Nova Law Review* addresses regulation of the healthcare industry, not the environment; but that hillside outside of Clairton, Pennsylvania, symbolizes the recurring “regulation versus free market” debate in this country. Steel and associated heavy industries dominated southwestern Pennsylvania beginning in the late 1870s; by the 1940s, operating virtually free of environmental regulation, they had filled the sky with smoky haze, rendering Pittsburgh as dark as midnight in late morning. Skies began to clear after smoke control began in that city in 1946, but battles continued over regulatory expansion throughout the region. The memory of that hillside as it existed in the 1960s illustrates the effect of the free market, only recently regulated, on that particular patch of Earth. In contrast, its condition today, after increasing state and federal regulation, illustrates the benefits of regulation. Such an illustration can shape overall attitudes toward regulation regardless of the subject being regulated.

Titled *Regulating Innovation in Healthcare: Protecting the Public or Stifling Progress?*, the articles to follow comment on various aspects of the politically sensitive topic of healthcare regulation. Politicians and policymakers generally range from those favoring intense regulation, such as that with which “Americans had a love affair” from the 1880s to the late 1970s, to those advocating the “Age of Deregulation,” marked by some as beginning around 1978. The range of opinions is just as broad in healthcare, as the 2016 presidential campaign and the debates characterizing the beginning of the Trump Administration illustrate.

3. See Stefan Lorant, *Pittsburgh: The Story of an American City* 376 (2d ed. 1975) (illustrating downtown Pittsburgh with all lights on at 11 a.m. in 1945). Lorant describes Pittsburgh as “the hearth of the nation” beginning in the late 1800s. *Id.* at 177, 324 (picturing a “bleak scene” at 3:00 PM).

4. See *id.* at 381, 390 (noting that, despite the passage of a city ordinance in 1941, World War II postponed its operation until 1946 and explaining that state legislation to expand smoke control beyond the city first was introduced in 1947).


The authors in this symposium issue presented their ideas at Nova Southeastern University’s Shepard Broad College of Law in the autumn of 2016, marking the 50th anniversary of Henry K. Beecher’s “bombshell” of an article in *The New England Journal of Medicine* with the unassuming title *Ethics and Clinical Research*. In that article, Beecher documented 22 examples of “unethical or questionably ethical [medical research] studies.” At the time Beecher wrote the piece, only 21 years after the Nuremberg trials, it was tempting to conclude that only Nazi physicians—not Americans—required regulation to guard against unethical behavior in medical research. Beecher’s findings, in many readers’ eyes, revealed otherwise. He himself, while not wishing to point a finger at particular researchers, explained:

Evidence is at hand that many of the patients in the examples to follow never had the risk [of research protocols] satisfactorily explained to them, and it seems obvious that further hundreds have not known that they were the subjects of an experience although grave consequences have been suffered as a direct result of experiences described here. There is a belief prevalent in some sophisticated circles that attention to these matters would “block progress.” But, according to Pope Pius XII, “. . . science is not the highest value to which all other orders of values . . . should be subordinated.”

Beecher himself did not favor regulation. To him, the solution to the problem presented by unethical conduct of medical research rested primarily not on informed consent—the requirement of which is a form of regulation—but on a “more reliable safeguard provided by the presence of an intelligent, informed, conscientious, compassionate, responsible investigator.” After all, in medicine, the opposite of regulation is not purely the free market, as it is in the steel industry. Rather, the opposite of regulation in medicine is the free market guided by professionalism and ethics of a sort that does not dominate in the steel industry—or any other heavy industry for that matter.

---

9. See Jones at 2293–2294 (describing the Nuremberg Code’s appearance after World War II and noting that “[n]any U.S. scientists believed that the Code . . . did not apply to them”).
11. *Id.* at 372.
As bioethicist Robert Veatch writes, Beecher did not believe the researchers conducting the studies he described were consciously pursuing their self-interest and ignoring their ethical obligations. Rather, “for Beecher, the problem [was] well-meaning but thoughtless investigators who fail[ed] to grasp what they [were] doing,” and “consciousness-raising” was the solution.\(^{13}\)

In contrast, Beecher’s former student, physician and bioethicist Jay Katz, operated under the conviction “that well-designed legal procedures could regulate (though not totally supplant) professional standards, which [Katz] found insufficient in themselves as a check on unethical practices.”\(^{14}\) As Veatch explains, “[b]y 1973, it was becoming more and more obvious that professional self-regulation was inadequate” in medical research.\(^{15}\) A whistleblower had revealed details of the Tuskegee Syphilis Study, through which the United States Public Health Service, under the guise of treatment, had studied untreated syphilis among poor, African-American men in Macon, Georgia, for the past forty years.\(^{16}\) In hearings thereafter, which led eventually to creation of the institutional review board (IRB) system of governmental regulation of research, Beecher testified that he favored “a massive professional education effort” instead.\(^{17}\) Nevertheless, as bioethicist Alexander Morgan Capron notes, “there is no question that [both] Beecher and Katz played pivotal roles in closing the post Nuremberg [ethical] lacuna that had become glaringly apparent by 1972.”\(^{18}\) Although Beecher favored reliance on ethics to govern the “free market” of medical research and Katz believed in research regulation, the development of such regulation in the United States stemmed at least partially from Katz’s “admiration for [Beecher’s] courage—Beecher’s willingness to risk his privileged position by lifting the veil that shielded the activities of his biomedical peers from public view.”\(^{19}\) For that reason, even research regulation advocates admire

---


\(^{15}\) Veatch, *supra* note 13, at 15.


\(^{17}\) Veatch, *supra* note 13, at 16 (quoting Beecher as saying, “I think it is a little too soon for this to be frozen into law.”).

\(^{18}\) Capron, *supra* note 14, at 75.

\(^{19}\) *Id.*
and honor Beecher to this day, and it seemed fitting to hold a symposium in his honor on the 50th anniversary of the article by which most know him.

III. HEALTHCARE REGULATION BEYOND MEDICAL RESEARCH

The topics of innovation and the role that its regulation plays raise questions in many areas of healthcare, not just clinical research. This symposium addresses important aspects of healthcare innovation dealing with delivery, payment, data collection, and technology. In organizing the symposium at NSU, we brought together experts from across the country in academia, government, and private practice to address the challenges in the transformation of healthcare. The result was an explicitly interprofessional event, during which the legal, medical, public health, and patient communities learned from each other. These articles provide insight on both sides of the question of whether regulating innovation is helping or hurting the future of healthcare.

Jackson Williams, the Director of Government Affairs for Dialysis Patient Citizens, addresses the need for innovation in healthcare business models. He argues that a business model change could be a solution to the current problem of high costs and low quality of healthcare in the United States. Specifically, Williams “argues that insurance regulators [could] catalyze cost containment efforts by encouraging, or mandating, insurers to act vigorously as agents of consumers in obtaining low prices from providers.” He also notes that insurance regulators could police provider misconduct in healthcare markets, providing extra protection for patients. Williams discusses how an insurance commissioner’s regulatory authority could solve the collective action problem by apportioning costs and thereby incentivizing provider cooperation. Williams’ innovative proposal could alleviate the skyrocketing cost-sharing obligations that currently exist in the majority of employer-sponsored health insurance plans.

Another equally important area of innovation is digital health information technology. As the healthcare industry has shifted from paper to digital, new legal issues have arisen with how to keep patients and their privacy interests protected. Cason Schmit, Research Assistant Professor of Public Health at Texas A&M University, introduces a research project undertaken by the Centers for Disease Control to examine the regulatory framework of state statutes dealing with health information technology. The

21. Id.
22. Id.
research reveals that there are literally thousands of state laws addressing digital health information in healthcare. Schmit notes that as technology has continued to outpace legislation at an exponential rate, the states have stepped up to create a patchwork of laws to try and keep up. Schmit argues that this complicated patchwork of state laws could be impeding advancements in health information technology because it is difficult to discern the applicable laws, and, therefore, businesses that want to avoid exposure to liability may steer clear of innovation for this reason. Schmit notes, however, that some laws are helpful in enabling entities to engage in new and innovative health information technology. In these instances, instead of regulation becoming a barrier to innovation, the regulations actually encourage and enable innovation. Schmit highlights how the law has been both a benefit and a burden to innovation in healthcare.

While there are numerous benefits to be gained from the shift from paper to digital, there are also new vulnerabilities associated with the data that did not exist before this transition. This cycle of innovation and legal catch-up is not uncommon in the law. Since its inception, the organization now known as the Food and Drug Administration (“FDA”) has been charged with protecting a vulnerable public from the manufacturers and sellers of medical products. Initially, its purview was over products characterized as drugs, but as medical devices became more sophisticated, and consequently more dangerous, the FDA’s scope expanded to cover them as well.23 Despite its best efforts, however, the FDA and the regulations that govern it have always lagged behind the pace of technological advances, resulting in a cycle of inaction, tragedy, and reaction.24

Innovation in health information technology mirrors the last century of innovation in medical devices in that they both outpace the advancements in law. They both also carry with them risks to a vulnerable public in different ways. As advancements in health information technology bring benefits to healthcare, they bring the potential for damage – not only physical injury, as with medical devices, but also damage to financial and privacy interests. Paul R. DeMuro, Associate Professor of Pharmacy at NSU, examines the cybersecurity risks inherent in health information technology. Specifically, DeMuro’s article discusses ransomware, a virus cybercriminals use to bring patient care to a halt while they hold patients’ health information captive. Ransomware has the potential to destroy privacy and prevent appropriate care from being delivered to patients because computer systems

24. See id. at § 12:7.
are frozen until the ransom is paid to the cybercriminal. As innovation creates new technology, existing security measures and regulations have proven insufficient to protect against the vulnerabilities. DeMuro analyzes the existing legal framework governing digital health information in the healthcare industry and argues that negotiation theory should be applied to the ransomware context to shed light on whether healthcare organizations should be permitted to engage in ransom negotiations with cybercriminals.

As discussed above, this same tension between innovation and regulation arises with the societal desire for advancement in medical devices. Whether it is an improved implantable cardioverter defibrillator or an insulin pump, most would agree that innovation in medical devices benefits the public. However, as technology has increased with medical devices, so has the ability to capture sensitive patient information through vulnerabilities in the hardware or software. As Chris Kersbergen, Assistant Professor at Keiser University, discusses in his article, it is easy hack into such devices. Kersbergen examines a recent draft FDA guidance on cybersecurity for manufacturers of wirelessly connected, implanted medical devices. He discusses why it is so easy to hack into such devices and critiques three aspects of the draft guidance, suggesting that the FDA should include patient privacy within the concept of patient safety when regulating in this area. Kersbergen argues for additional FDA regulation that focuses heavily on the financial and other “identity” implications of hacking into medical devices as a way to obtain patient data.

Not only is there a risk that patient health information can be exploited for financial gain, but the patient’s physical safety also could be jeopardized by these various vulnerabilities. Michael Woods’s article focuses on the physical safety aspect of cybersecurity of the same devices. Woods is not as concerned about financial identity theft or patient data; he is mainly concerned about patient physical safety and about terrorists who could hack into medical devices to physically hurt patients. He does not focus on any one agency or any one regulation or guidance document; part of his point is that too many agencies are responsible for monitoring

27. Id. at 417–18.
28. Id. at 412–14.
29. Id. at 401.
cybersecurity of such devices, in various ways. Similar to Schmit’s highlighting of the complicated patchwork of regulations, Woods seeks clarification among the various government agencies regulating in this area. This is an area characterized by duplication of laws and overlap of authority, creating problems in effective enforcement of the law. When the potential for serious harm is so high, Woods argues, there should be a unified approach to regulation among agencies. Without a unified, proactive approach to these regulations, the United States could be facing another cycle of inaction, tragedy, and reaction.

The transformation of healthcare is certain. If and how regulation will respond to this transformation will have a profound personal impact on us all. This symposium explores the highly political question of how much involvement the law should have in the innovation of healthcare. We hope it adds to the discourse and exposes areas where changes in the law can help shape the healthcare industry.


31. Id. at 440–42.
THE PERSISTENCE OF OPPORTUNISTIC BUSINESS MODELS IN HEALTH CARE AND A STRONGER ROLE FOR INSURANCE REGULATORS IN CONTAINING HEALTH CARE COSTS

JACKSON WILLIAMS*

I. INTRODUCTION ................................................................. 313

II. THE INSURANCE COMPANY AS AN AGENT OF PURCHASERS .... 315

III. THE PROBLEM OF EXCESS PRICES ..................................... 315

A. Provider Market Concentration ......................................... 316
B. Excessive Prices for Must-Have Providers ............................ 319
C. Out-of-Network Hospital-Based Providers and Surprise Billing .......................................................... 320

IV. POLICY OPTIONS TO ADDRESS PROVIDER PRICING PROBLEMS .... 323

A. All-Payer Rate Setting for Providers as a Policy Option ....... 323
B. Insurance Regulation as an Alternative to Rate-Setting for Providers .......................................................... 325

1. Use of Rate-Setting Authority to Require Pushback on Prices .................................................................. 327
2. Commissioners’ Catchall Authority to Declare Insurance Acts and Practices Unfair ............................... 331
3. Convening Insurers to Fight Balance Billing .................. 334

V. CONCLUSION ........................................................................ 340

I. INTRODUCTION

While much is heard about new “value-based” payment models for health care, the reality is that old-fashioned business models emphasizing higher unit prices and discrete billable services still prevail and succeed in driving up health care costs. Indeed, providers have cited the spread of

* Jackson Williams is Director of Government Affairs at Dialysis Patient Citizens. He received an MPA from Governors State University in 1996, his J.D. from Loyola University of Chicago School of Law in 1988, and his B.A. from the University of Illinois at Chicago in 1985. From 2010 to 2013 he worked at the Centers for Medicare and Medicaid Services. Previously he was a health services researcher in the AARP Public Policy Institute and a lobbyist on health policy issues for three non-profit associations. He is an NAIC Funded Consumer Representative, and also was in 2003-2004. He has taught courses in political science and law at the University of Illinois at Chicago, IIT-Kent College of Law, and Pennsylvania State University, Harrisburg.

1. See Robert Berenson, Addressing Pricing Power in Integrated Delivery: The Limits of Antitrust, 40 J. HEALTH POL’Y & L. 711, 712 (2015); Matthew Rae et al.,
global payment models as an excuse for continued market consolidation by providers.\(^2\) Even relatively low-cost integrated delivery systems, such as Kaiser-Permanente, profit from opportunistic behavior by competing providers, since their premiums can “shadow” those of insurers who must contract with high-cost providers.\(^3\)

Ideally, insurers would act as purchasing cooperatives on behalf of consumers, obtaining the lowest possible unit prices from providers.\(^4\) But the most effective tools that purchasers could deploy—including antitrust and other litigation against providers who act opportunistically—go unused.\(^5\) As the late health economist Warren Greenberg argued,\(^6\) this is partly because of the collective action problem inherent in a multi-payer market.\(^7\)

In this context, the collective action problem refers to the fact that while many purchasers share an interest in lower unit prices for health care, it is not always in the interest of an individual purchaser to expend resources on measures, such as initiating costly litigation or provoking an acrimonious impasse that, if successful, would likely benefit competing insurers or employers as well.\(^8\) But, more generally, it has been observed that payers have not “pushed back” on prices.\(^9\)

This Article argues that insurance regulators can catalyze cost containment efforts by encouraging, or mandating, insurers to act vigorously as agents of consumers in obtaining low prices from providers to include policing provider misconduct in health care markets.\(^10\) The Insurance Commissioner’s regulatory authority can solve the collective action problem

---

\(^2\) See CTR. FOR STUDYING HEALTH SYS. CHANGE, WALL STREET COMES TO WASHINGTON 2 (2004); Robert A. Berenson et al., The Growing Power of Some Providers to Win Steep Payment Increases from Insurers Suggests Policy Remedies May Be Needed, 31 HEALTH AFF. 973, 979 (2012).


\(^4\) See Berenson et al., supra note 2, at 979.

\(^5\) See Berenson, supra note 1, at 714.


\(^7\) See id.

\(^8\) See id. at 122–23.

\(^9\) DIANA FARRELL ET AL., MCKINSEY GLOB. INST., ACCOUNTING FOR THE COST OF US HEALTH CARE: A NEW LOOK AT WHY AMERICANS SPEND MORE 105 (2008); see also infra Section IV.B.

\(^10\) See infra Section IV.B.
by apportioning costs and, thereby, incentivize cooperation.\textsuperscript{11} The Commissioner can also serve as a coordinator of, and spokesperson for, joint efforts to bring down provider prices.\textsuperscript{12}

II. THE INSURANCE COMPANY AS AN AGENT OF PURCHASERS

Two recent trends have significantly changed the way consumers interface with health insurance: Rising deductibles and self-funded plans.\textsuperscript{13} Today, for most consumers, the most important function of a health insurance company in a given year will not be paying for health utilization, but negotiating prices with providers.\textsuperscript{14}

In 2003, only about half of employer-sponsored insurance (“ESI”) that covered workers’ health plans had a deductible at all—by 2013, it was 81%.\textsuperscript{15} In 2003, the average deductible was $518, a decade later it was $1273, a 146% increase.\textsuperscript{16} In about 20% of workplaces, employees have access to only high-deductible health plans, with a deductible averaging $2100.\textsuperscript{17} For about forty-two million Americans with ESI who spend over $300 on care but do not meet the average deductible in a given year, a 5% reduction in provider prices would yield an average of $30 in direct and immediate savings on out-of-pocket costs.\textsuperscript{18} For this group, the principal role of the insurance company is that of purchasing cooperative—combining the buying power of multiple enrollees to obtain the lowest price.\textsuperscript{19}

III. THE PROBLEM OF EXCESS PRICES

Comparisons of health care costs across the thirty industrialized countries, for which the Organization for Economic Cooperation and Development (“OECD”) publishes data, demonstrates “that the United States spends more on health care than any of the other OECD countries spend, without providing more services than the other countries do. This suggests

\textsuperscript{11} See infra Section IV.B.II.
\textsuperscript{12} See infra Section IV.B.II.
\textsuperscript{13} CTR. FOR STUDYING HEALTH SYS. CHANGE, supra note 2, at 2.
\textsuperscript{16} Id. at 5.
\textsuperscript{17} Rae et al., supra note 1.
\textsuperscript{18} See id.
\textsuperscript{19} See Berenson et al., supra note 2, at 979.
that the difference in spending is mostly attributable to higher prices of goods and services.”

According to the International Federation of Health Plans 2015 Comparative Price Report, an annual survey comparing medical prices per unit in Australia, New Zealand, South Africa, Spain, Switzerland, United Kingdom, and United States, the United States has the highest prices for two of five diagnostic tests compared, eight of eight surgical procedures compared, and hospital costs per day. In a finding that will amaze any American who has traveled to Switzerland and paid the equivalent of five dollars for a bottle of Coke, the survey reported that patients in Geneva, Illinois or Geneva, New York could expect to pay twice the price for a colonoscopy or magnetic resonance imaging (“MRI”) scan paid in those towns’ European namesake.

We know that in some local markets, provider unit prices are exceptionally high. A 2005 United States Government Accountability Office Report found that in 28 of 232 metropolitan areas studied, hospital prices were 25% or higher than the national average, and in 32 of 319 metropolitan areas—many in Wisconsin, Oregon, Arkansas, Montana, and Louisiana—physician prices were 16% or higher than the national average.

Three factors driving higher prices are provider consolidation, provider “must-have” status, and the refusal of providers to participate in insurers’ networks.

A. Provider Market Concentration

In an analysis of commercial “insurance claims between 2007 and 2011 from three of the five largest U.S. insurers, Aetna, Humana, and United

20. Gerard F. Anderson et al., It’s the Prices, Stupid: Why the United States is So Different from Other Countries, 22 HEALTH AFF. 89, 90 (2003).
22. Id. at 3, 11–24.
23. See id. at 13–14.
25. Id.
Health care,” reported to the Health Care Cost Institute (“HCCI”), Cooper and colleagues compared private health spending levels among 306 Hospital Referral Regions. They concluded that “health spending on the privately insured varies by more than a factor of three across the 306 hospital referral regions (“HRRs”) in the [United States],” and that “hospital transaction prices play a large role in driving inpatient spending variation across HRRs.”

We find that hospitals’ negotiated transaction prices vary substantially across the nation. For example, looking at the most homogeneous of the seven procedures that examine, hospital-based MRIs of lower-limb joints, the most expensive hospital in the nation has prices twelve times as high as the least expensive hospital. What is more, this price variation occurs across and within geographic areas. The most expensive HRR has average MRI prices for the privately insured that are five times as high as average prices in the HRR with the lowest average prices. Likewise, within HRRs, on average, the most expensive hospital has MRI negotiated transaction prices twice as large as the least expensive hospital.

Cooper and colleagues concluded that even after controlling for such variables as “for-profit [status], having more medical technologies,” regional labor costs and patient mix,

Monopoly hospitals have 15.3[%] higher prices than markets with four or more hospitals. Similarly, hospitals in duopoly markets have prices that are 6.4[%] higher and hospitals in triopoly markets have prices that are 4.8[%] higher than hospitals located in markets with four or more hospitals. While we cannot make strong causal statements, these estimates do suggest that hospital market structure is strongly related to hospital prices.

In a study tracking hospital prices in California from 2004 to 2013, Melnick and Fonkych found that “[h]ospital prices increased substantially during a period of slow economic growth, and may have been driven in part

27. Cooper et al., supra note 26, at 1–2.
28. Id. at 2.
29. Id. at 3.
30. Id.
by increased market power by large, multi-hospital systems—and possibly other smaller systems—practicing all-or-none contracting.” They concluded that:

[T]he market power effects of large hospital systems do not necessarily require consolidation between local competitors. Indeed, many of the hospitals in California’s largest systems do not have substantial overlapping markets with other system member hospitals. This suggests that hospitals in large hospital systems, by tying their hospitals together, are able to achieve market power over prices beyond any local market advantages.

[W]ith large size comes the potential to expand and protect market power. Large hospital systems that conduct “all-or-none” contracting have reportedly added other anti-competitive language to their contracts to protect and expand their market power including clauses that prohibit health plans or employers from developing “tiered” benefit packages that would allow them to . . . develop new products to stimulate competition through differential cost sharing across member hospitals. Another example is so-called gag-clauses which prohibit health plans from sharing detailed hospital specific utilization and pricing data with large employers which might be used to develop benefit packages that provide incentives for employees to use lower priced—and/or higher quality—hospitals.

Stanford University researcher Laurence C. Baker has assembled a database of county-level data on competition among physician practices, as measured by the Hirschman-Herfindahl Index (“HHI”), and average prices for physician services. Baker notes that the “trend toward fewer and larger [physician practice] groups could increase . . . market concentration, resulting in fewer practices facing less competition and with greater economic power. This in turn could lead health plans to pay higher prices for physician services.”

An analysis by Baker and colleagues of the relationship between physician competition and prices paid for common office visits found that:

Less competition among physician practices is statistically significantly associated with substantially higher

32. Id. at 6.
33. Id.
34. Id. at 5–6.
36. Id. at 1654.
prices paid by private [Preferred Provider Organizations] to physicians in [ten] large specialties for office visits. . . . [T]he level of competition observed at the [ninetieth] percentile of the HHI distribution was associated with a price for an intermediate office visit with an established patient—CPT code 99213—between $5.85 and $11.67 higher than at the [tenth] percentile of the HHI distribution. Across all [ten] types of office visits, this difference in HHI was associated with mean prices for office visits 8.3% to 16.1% higher.37

A subsequent study by Austin and Baker examining prices for fifteen common high-cost services, such as knee replacements and arthroscopic surgery, yielded similar findings.38 In that article, Austin and Baker reported that they “frequently found market concentration levels that appear high, relative to the commonly encountered view that HHI levels above 2500 are concerning. HHIs were 2500 or more in more than half of [the] counties studied among the chosen procedures and specialties.”39 Indeed, both the mean and median HHI for the many hundreds of counties in “[f]ourteen of the fifteen procedure-specialty combinations” they studied exceeded the Federal Trade Commission’s 2500 HHI benchmark for a highly concentrated market.40 The scale of price differentials was sobering.41 For urology, where even the tenth percentile of HHI exceeded 2500, the amount paid for a vasectomy or kidney stone treatment in counties at the ninetieth percentile of prices, exceeded the amount in counties at the tenth percentile by two and a half times.42

B. Excessive Prices for Must-Have Providers

Certain large and prestigious hospitals and physician groups are recognized as must-have parties to insurers’ provider networks, and demand and receive prices disproportionate to their clinical outcomes.43 Insurers find they cannot exclude these providers from their networks, nor place them in lower tiers, and pass the costs along in the form of higher premiums.44

37. Id. at 1659.
39. Id. at 1759.
40. Id. at 1756–57.
41. See id. at 1759.
42. Austin & Baker, supra note 38, at 1757.
43. See Berenson et al., supra note 2, at 973.
44. Id. at 973–74.
For this reason, Robert Berenson argues that “antitrust policy and enforcement can only be one—and not the primary—approach to addressing provider pricing power.” He contends “that the source of hospital and physician pricing power . . . lies . . . in its leverage negotiating contracts with health insurers,” which is not the same as market concentration.

An essential element of health plan-provider negotiations over price and other contractual terms and conditions is the willingness of consumers to accept narrow or tiered network products that effectively limit their choice of provider to those willing to accept the health plan’s pricing. Without a credible threat of either excluding or disadvantaging high-cost providers by placing them in a higher consumer cost-sharing tier, health plans lack an important bargaining chip.

Another factor is that it has become common health care parlance to refer to “must-have” providers—especially hospitals—that must be included in a plan’s provider network to make the plan marketable to customers. Must-have hospitals, by definition, have pricing leverage over insurers because the plans cannot plausibly threaten to exclude or limit their participation in the insurer’s provider networks.

C. Out-of-Network Hospital-Based Providers and Surprise Billing

Recent years have seen what Berenson calls an “epidemic of physicians and hospitals in some cases purposefully remaining out of network to charge either the insurer or the unsuspecting consumer outrageously high amounts.” The movement toward integration and accountable care has been met with stubborn resistance from hospital-based physicians at the many community hospitals that outsource their emergency rooms and other hospital-based specialties to large physician staffing corporations. With their economy of scale, these companies have the capacity to bill both insurers and patients, and to pursue collection action against consumers for unpaid bills. By setting up shop in hospitals that are

45. Berenson, supra note 1, at 714.
46. Id.
47. Id.
48. Id. at 720.
49. Id.
50. See Berenson, supra note 1, at 727.
51. See Joseph Burns, Health Plans Seek Leverage When Physicians Submit Extremely High Bills, MANAGED CARE (Aug. 2011),
in-network, they gain access to a captive clientele of consumers who need care.\textsuperscript{52} As such, these companies see little advantage to signing network contracts with insurers that would discount prices.\textsuperscript{53} Instead, they bill their charges, obtaining payments for the “usual, customary, and reasonable” (“UCR”) amounts from insurers and send surprise bills to consumers for the difference.\textsuperscript{54}

When physicians refuse to contract, the midpoint of the range of payments used to determine a UCR amount will shift rightward. Ordinarily, one would expect the distribution to be dominated by Medicare and Medicaid prices, and network rates discounted for the volume an insurer can offer, skewing the distribution to the left, with only a few data points at the right representing self-pay patients paying the full charges.

A distribution of reimbursements for services delivered by non-participating providers will be dominated by amounts representing a UCR payment tendered by an insurer plus any balance between that amount and the charge that is paid by the consumer. These data points will be higher dollar amounts, and as they proliferate within a specialty, such as emergency medicine, the UCR midpoint will ratchet upward. This means higher overall costs of care, and in making hospital-based specialties more lucrative, making those careers more attractive to medical graduates. This, in turn, could increase the supply and utilization of expensive emergency room care, at the expense of access to primary care.

In addition to the higher costs, there are two other consequences when hospital-based physicians decline to join insurer networks. For consumers, one immediate consequence arises from the fact that out-of-network expenditures may not count toward their deductible and out-of-pocket maximum, thereby undermining the Affordable Care Act’s limitations on medical debt. But the refusal of hospital-based physicians to participate in networks also has far-reaching implications for the payment and delivery system reforms that many policymakers and stakeholders hope will improve quality and efficiency. This is particularly true of emergency medicine physicians.

Generally speaking, current payment and delivery system reforms are aimed at giving a group of providers accountability for the total cost of

\textsuperscript{52} See Burns, supra note 51.
\textsuperscript{53} See id.
care of a population’s health needs or for the cost of an individual’s episode of care. In such circumstances, providers will be more mindful of opportunities to avert a potentially avoidable hospitalization and to use resources efficiently. In global budget models—whether a staff-model Health Maintenance Organization (“HMO”), an Accountable Care Organization, or Maryland’s unique Global Budget Revenue program—providers must deliver care to covered persons within fixed financial benchmarks. Providers’ incentives are to manage patients’ chronic conditions through primary care and care coordination, so they are not hospitalized and, when patients do appear at a hospital, to avoid unnecessary resource utilization. Unless a global budget or episode payment system is imposed by the state—as in Maryland—insurers are the only entity capable of sponsoring such payment reforms.

The Emergency Department (“ED”) is at the fulcrum of any efforts to integrate care, so a refusal of emergency medicine physicians to contract with insurers will undermine reform activities. According to a recent Rand Corporation study, the ED now accounts for more than one half of hospital admissions, up from only about one third of admissions in the early 1990s. While inpatient admissions overall have declined relative to population growth in the United States, there has been a 17% increase in admissions from the ED, offsetting the decrease in admissions from physician offices and other outpatient settings.

Meanwhile, a study recently published in the Annals of Internal Medicine indicates that nearly one in twelve patients who visit an ED return to an “acute care setting within three days,” with the thirty day re-visit rate being nearly one in five patients.

Yet even as there is consensus on the need to reduce avoidable hospitalizations and ED use, ED physicians increasingly position themselves outside the insurance system. Their only bonds are to the physician staffing corporations that employ them and the hospital that contracts with

56. Id. at 24.
them—two entities that generally have financial incentives to *increase* admissions and *increase* emergency room traffic.  

IV. **POLICY OPTIONS TO ADDRESS PROVIDER PRICING PROBLEMS**

A. **All-Payer Rate Setting for Providers as a Policy Option**

A key distinction between America’s pluralistic system of multiple payers and those of peer nations, according to Anderson and colleagues, is that “the government-controlled health systems of Canada, Europe, and Japan allocate considerably more market power to the buy side.”  

In essence, the health insurance plans overseas are more monopsonistic.  

Anderson argues that while a monopsonistic purchaser is ultimately constrained by market forces on the supply side—that is, by the reservation—minimally acceptable—prices of the providers of health care below which they will not supply their goods or services. . . . [W]ithin that limit, monopsonistic buyers enjoy enough market clout to drive down the prices paid for health care, and health care inputs fairly close to those reservation prices.

For this reason, a number of prominent United States health-policy thought leaders endorse some type of all-payer rate setting regime.  

[A] model of self-regulation, [under which] public and private payers would negotiate payment rates with providers, and these rates would be binding on all payers and providers in a state. Providers could still offer rates below the negotiated rates. The privately negotiated rates would have to adhere to a global spending target for both public and private payers in the state. After a transition, this target should limit growth in health spending per capita to the average growth in wages, which would combat wage stagnation and resonate with the public. We recommend that an independent council composed of providers,

---

60. Anderson et al., *supra* note 20, at 102.
61. *Id.*
62. *Id.*
payers, businesses, consumers, and economists set and enforce the spending target.\(^{64}\)

Robert Berenson endorses a regulatory approach that would place price ceilings on negotiated rates that come out of insurer-provider negotiations and upper limits on billing to consumers, beyond the negotiated rates insurers agree to pay, set as a percentage above the Medicare yardstick. Setting upper limits would bound the prices, while permitting market negotiations to focus on selected networks with discounting and with new payment models—market approaches that can be difficult to preserve in a full-fledged all-payer rate-setting environment.\(^{65}\)

While many health policy analysts would like to see all-payer rate setting for providers, there are two major political barriers to this option.\(^{66}\) First, it is contrary to the American preference for a light regulatory touch.\(^{67}\) As seen in the continuing battles over state certificate-of-need laws, conservatives remain unconvinced that “health care is different” and merits restrictions on prices or supply that remain unthinkable in other areas of the economy.\(^{68}\)

Second, providers are vehemently opposed to restrictions on the prices they can charge, as seen in the opposition to the Massachusetts proposal for a luxury tax on expensive hospitals,\(^{69}\) and to the proposed mergers of four large insurers announced in 2015.\(^{70}\)

\(^{64}\) Emanuel et al., supra note 63, at 950.

\(^{65}\) Berenson, supra note 1, at 738.

\(^{66}\) See id. at 725–26, 738; Berenson et al., supra note 2, at 979.

\(^{67}\) See Berenson, supra note 1, at 712, 729–30; Berenson et al., supra note 2, at 975.

\(^{68}\) See Berenson, supra note 1, at 726–27, 733; Berenson et al., supra note 2, at 975.

\(^{69}\) See H.R. 4070, 187th Gen. Court, Reg. Sess. (Mass. 2012); Chris Camire, Reps Eye ‘Luxury Tax’ on Massachusetts Hospitals, LOWELL SUN, http://www.lowellsun.com/news/ci_20618865/reps-eye-luxury-tax-massachusetts-hospitals (last updated May 14, 2012, 6:35 AM). The hospital luxury tax proposal was a provision of a Massachusetts House bill that would have imposed a 10% tax on hospitals charging more than 20% above the state median price for a specific service if they could not “prove they offer[ed] higher-quality service than [other] facilities.” H.R. 4070; Camire, supra. The funds were to have been redistributed to hospitals serving poor communities. Camire, supra; see also H.R. 4070. The provision was stripped from the final version of the legislation, but a variation on the concept has been revived for a current ballot initiative in Massachusetts. S.B. 2260, 187th Gen. Court, Reg. Sess. (Mass. 2012); Camire, supra.

\(^{70}\) Hancock, supra note 14.
But while health care provider rates are regulated in only one state, Maryland, there is a long-standing tradition of regulating insurer rates. This Article will argue in the next section that this regulatory structure can be marshaled to put downward pressure on provider prices.

B. Insurance Regulation as an Alternative to Rate-Setting for Providers

Robert Berenson notes that, to date, “the market response to the increase in prices resulting from growing provider leverage in rate negotiations has been limited and largely ineffective.” McKinsey Global Institute argues that this is because of a health care supply chain in which “stakeholders are either unwilling or unable to resist cost increases that are passed along to them.” In its view, cost increases from physicians and hospitals are “pass[ed] on . . . to the next player in the chain. . . . Unless the [United States] health system addresses this dynamic, medical inflation cannot help but continue.”

The consensus of a 2004 panel discussion on the health care industry was that employers are “missing in action” on health care prices:

[Most employers have not pushed back at providers and insurers to lower cost and premium trends, relying instead on shifting costs to workers through higher patient cost sharing—higher deductibles and co-insurance, for example. The panelists agreed that in the near term employers will continue to shift costs to workers but that cost sharing as a long-term cost-containment strategy [will not] work.

“We [have not] seen the employers kick in because their first line of defense has been cost shifting, which has been an effective strategy in the short run, but you can only raise the deductible to $1000 one time. So, [there is] a cliff here that [we are] coming to,” said Robert Laszewski, President of Health Policy and Strategy Associates.

[The] exception to the lack of purchaser pushback against higher cost and premium trends is the California Public Employees Retirement System, or (“CalPERS”), analysts agreed, but they

71. Berenson, supra note 1, at 712, 725 n.8, 738.
72. Berenson et al., supra note 2, at 979; infra Section IV.B.
73. Berenson, supra note 1, at 713.
74. FARRELL ET AL., supra note 9, at 30.
75. Id.
76. CTR. FOR STUDYING HEALTH SYS. CHANGE, supra note 2, at 2.
77. Id.
78. Id.
were skeptical that CalPERS’ decision to exclude several dozen hospitals from its health maintenance organization—HMO—networks would prompt other purchasers to take a harder line.\footnote{79}{Id.} One of CalPERS’ strategies is described infra.\footnote{80}{See Ann Boynton & James C. Robinson, Appropriate Use of Reference Pricing Can Increase Value, HEALTH AFF.: BLOG (July 7, 2015), http://www.healthaffairs.org/blog/2015/07/07/appropriate-use-of-reference-pricing-can-increase-value/; infra Section IV.B.2.} Employers and insurers could have good reason to be reluctant to apply pressure to providers.\footnote{81}{See CTR. FOR STUDYING HEALTH SYS. CHANGE, supra note 2, at 2–3.} Purchasers must maintain a good working relationship with the doctors and hospitals to which they entrust enrollees’ care.\footnote{82}{Burns, supra note 51.} Further, the only recourse if a provider’s price is too high is to walk away from negotiations and accept a narrower network that may be less attractive to employees and consumers.\footnote{83}{See CTR. FOR STUDYING HEALTH SYS. CHANGE, supra note 2, at 2; Berenson et al., supra note 2, at 974–75.} The thesis of this Article is that purchasers might be emboldened if they are backed up by an insurance regulator who is leading and facilitating a coordinated pushback campaign. In the Author’s view, many commissioners have two major legal tools available for deployment, but much of their role would be hortatory as public figures having a central role in the health care system oversight.

Insurance laws in at least three states already direct commissioners to inquire into underlying health care costs, specifically calling attention to provider prices.\footnote{84}{See e.g., 42 R.I. GEN. LAWS § 42-14.5-2. With respect to health insurance as defined in Title 42, Section 14.5-2 of the Rhode Island Health Care Reform Act, “the health insurance commissioner shall discharge the powers and duties of office to:” (1) [g]uard the solvency of health insurers; (2) [p]rotect the interests of consumers; (3) [e]ncourage fair treatment of health care providers; (4) [e]ncourage policies and developments that improve the quality and efficiency of health care service delivery and outcomes; and (5) [v]iew the health care system as a comprehensive entity and encourage and direct insurers towards policies that advance the welfare of the public through overall efficiency, improved health care quality, and appropriate access. 42 R.I. GEN. LAWS § 42-14.5-2. “Changes in the insurer’s health care cost containment and quality improvement efforts included, as an appendix to the filing and labeled, ‘Appendix II: Cost Containment and Quality Improvement Efforts.’” OR. ADMIN. R. 836-053-0473 (2016). The cost containment and quality improvement efforts must: (A) [e]xplain any changes the insurer has made in its health care cost containment efforts and quality improvement efforts since the insurer’s last rate filing for the same category of health benefit plan; (B) [d]escribe significant new health care cost containment initiatives and quality improvement efforts; (C) [i]nclude an estimate...}
To be sure, a commissioner cannot succeed in this project without the support of the payer community, including the insurers themselves. Insurers would have to embrace the role of price-cutter, even though, as explained infra, their financial incentive to do so can be ambiguous. One assumption is that industry rhetoric-deploring high prices is sincere and the regulatory path would be welcomed. Another assumption is that norms promulgated in the state-regulated insurance sphere would spill over into the larger employer-sponsored insurance sphere.

This effort would therefore also require the support of self-insured employers that retain insurance companies on an administrative services only basis. Employers have perhaps the greatest financial interest in obtaining lower prices from insurers, although the insurance commissioner’s authority is at low ebb—if not absent altogether—when an insurer acts solely as a third party administrator.

Thus, to a great extent, the regime envisioned is one in which the commissioner is acting as much as a convener and coordinator as he is a regulator. An advisory committee of purchaser representatives and consumer advocates would give the project added heft. A commissioner who is a gubernatorial appointee—and most are—would also need the political support of a governor who believes its state is competitively disadvantaged by high health care costs. Success would also be greatly aided by the cooperation of the state’s Attorney General. Attorneys General have traditionally wielded some oversight of health care as enforcers of antitrust law and as interpreters of laws governing non-profit corporations such as Blue plans and hospitals.

1. Use of Rate-Setting Authority to Require Pushback on Prices

According to a Kaiser Family Foundation analysis of state statutory authority to review health insurance rates, “[thirty-five jurisdictions]—including the District of Columbia—ha[ve] prior approval authority over . . . [premiums in] some portion of the individual and small group market,” with “[twenty-two] ha[ving] prior approval authority over all major medical expenses.”

Id. Section 1385.03(c)(3) of the California Health and Safety Code requires plans to detail “significant new health care cost containment and quality improvement efforts and provide an estimate of potential savings together with an estimated cost or savings for the projection period.” CAL. HEALTH & SAFETY CODE § 1385.03(c)(3) (West 2015).

of the potential savings from the initiatives and efforts described in subsection (2)(g)(B) of this section together with an estimate of the cost or savings for the projection period; and (D) [i]nclude information about whether the cost containment initiatives reduce costs by eliminating waste, improving efficiency, by improving health outcomes through incentives, by elimination or reduction of covered services or reduction in the fees paid to providers for services.
health insurance products in both the individual and small group markets;” and in the remaining “states, prior approval authority [is] limited” to subgroups of products. Additionally, the analysis noted “some states with little to no authority to regulate rates,” including some file and use states, have negotiated rate reductions. The typical statutory grant of regulatory authority over premiums provides that “[r]ates shall not be excessive, inadequate, or unfairly discriminatory.”

Insurance regulators could withhold permission to increase premiums that reflect provider market power due to inappropriate consolidation and order insurers to pursue antitrust litigation when prices and HHI exceed a certain threshold. Rates could be set so that an insurer’s profits are reduced in proportion to excessive prices that are deemed to be within the insurer’s power to reduce. In other words, the regulator would prescribe upper limits on medical expenditures representing quantity times a target price in line with national averages. The target price could be lowered in increments annually to give time for insurers to act.

In this scenario, the commissioner would put insurers on notice that they need to push back on prices and levy a tentative, but avoidable, fine payable in the event that they do not act. This fine is meant to be borne collectively, not individually, to reflect provider market power only, and not any differential market power of insurers of varying size. The fine should be set to promote cooperation among insurers in preparing antitrust litigation and to have an in terrorem effect on providers that softens their negotiating stance. The commissioner, as a state actor with antitrust immunity, could lawfully coordinate insurers’ actions toward target price levels.

Suppose insurers file rates that assume a medical cost trend of 5%, based upon current provider prices, and a 3.5% profit margin. The commissioner could decree a lower cost trend based upon a target price and set rates so that if the target were not met, the insurer profit margin would be one or two percentage points lower.

It is worth noting that federal law mandating a minimum medical loss ratio using a percentage of gross revenues may have a perverse effect making insurers less likely to push back on prices. For instance, a health plan with 10,000 enrollees, which has annual medical reimbursements at the United States per-enrollee average in 2009, would spend $33,140,000,
permitting it to keep $5,000,000 for administrative costs and profits. Meanwhile a plan with 10,000 enrollees in Rochester, New York—where prices and utilization are relatively low—would expect just $23,190,000 in medical reimbursements, and would be allowed to keep only $3,500,000 for administrative costs and profits. Presumably, insurance executives prefer operating in markets where higher provider prices give insurers additional cushions for administrative costs and profits.

The concept envisioned here is intended to be deployed in regions where costs are excessive and those costs are attributable to high prices. A commissioner can look to benchmarks to make a determination as to whether prices are excessive. National data is available from various sources, which can be used to compare a region’s prices for hospitals and physicians.

Prices beyond a certain threshold could be the triggering mechanism for the pushback process. For example, the HCCI has promulgated a set of economic metrics they have dubbed the Healthy Marketplace Index (“HMI”), “intended to provide baseline measurements of health care market performance related price, productivity, and competition.”

An HMI measures a “basket of health care services allowing for consistent comparisons” across regions at the Core-Based Statistical Area (“CBSA”) level, permitting “differences between markets [to] be attributed to prices rather than the types or amounts of services used.” An “index value of 1.00 indicates that, on average for a basket of services, the prices in the CBSA were equal to those of the total population.” A CBSA with an index value of 1.05 would have prices 5% higher.

Suffice it to say, there is no obvious threshold for a price index trigger. The Dayton, Ohio inpatient price index of 1.18 would seem to qualify as a true outlier, but the Milwaukee level of 1.09 would also justify taking action if it is causing insurance premiums to be unaffordable for consumers or businesses.

The triggering mechanism could have multiple parts. An HHI measurement exceeding 2500, or an even higher threshold, would verify that market concentration is the principal culprit in high prices. A third triggering benchmark could look to hospital financial indicators. High levels of hospital reserves, profit margins, or executive compensation could be viewed as markers of excessive prices.

90. Id. at 2.
91. Id.
92. Id. at 3.
While the substance of antitrust law relating to health care providers is beyond the scope of this Article, one can point to a template for private antitrust enforcement by an insurer against a provider: Litigation mounted in the 1990s by *Blue Cross and Blue Shield United of Wisconsin v. Marshfield Clinic*.*93* The case was hardly straightforward in either its atypical fact pattern—the insurer eventually prevailed because it proved the defendant had divided territories with a potential competitor but no damages were awarded; and judgment on a monopolization charge under Section 2 of the Sherman Act was reversed—or in its procedural journey—two trials and two trips to the Seventh Circuit Court of Appeals.*94* Rather, it illustrates the ideal envisioned: An insurer serving a high-cost region taking on a large health system that had stifled competition, bearing great expense to painstakingly assemble a complex case and pursue it aggressively.*95* Warren Greenberg, who served as an expert witness for the plaintiff, noted that this expense was borne entirely by one insurer, even though a successful outcome would have benefited competing insurers, consumers, and employers who did not contribute.*96* A multi-payer mandate from a commissioner to pursue such litigation would more fairly apportion costs.

To be sure, a rate ruling that effectively orders insurers to file antitrust litigation would represent a heavy lift.*97* First, there are legal hurdles.*98* As Robert Berenson wrote, “[t]he [h]orse [h]as [a]lready [l]eft the [b]arn”*99* in the sense that “monopolies lawfully acquired or, in the case of consummated mergers, fully entwined entities . . . are impractical to successfully unwind.”*100*

In such instances, plaintiffs could request *conduct remedies* that would “regulate the conduct of the monopolist, for example, by providing for binding arbitration to resolve payer-provider price disputes or requiring maintenance of open medical staffs.”*101*

Second, litigation would be expensive. It would be helpful if one of the many philanthropies dedicated to health care policy could fund a forensic resource center to marshal legal and economic thinking relevant to modern

---

93. 152 F.3d 588, 590 (7th Cir. 1998); see also 65 F.3d 1406, 1408 (7th Cir. 1995).
94. *Blue Cross & Blue Shield United of Wis.,* 152 F.3d at 588, 590–96; *Blue Cross & Blue Shield United of Wis.,* 65 F.3d at 1416–17.
95. *See Blue Cross & Blue Shield United of Wis.,* 152 F.3d at 590–91.
96. Greenberg, supra note 6, at 118 n.1, 122, 123; *see also Blue Cross & Blue Shield United of Wis.,* 152 F.3d at 590–91.
97. *See Berenson, supra note 1,* at 713–14.
99. *Id.* at 725.
100. *Id.* at 726 (citation omitted).
101. *Id.* (citation omitted).
understanding of health care organizations, formulate principles and guidelines for applying antitrust and non-profit law, and collect evidence for and testify in adversarial proceedings.

2. Commissioners’ Catchall Authority to Declare Insurance Acts and Practices Unfair

A commissioner’s plenary authority to prohibit unfair practices could be used to prohibit insurers from capitulating to contracting terms that reflect inappropriate provider market leverage, particularly in the sphere of the must-have provider. Many states’ insurance codes include a grant of authority similar to this:

If the [c]ommissioner believes that any person engaged in the insurance business is in the conduct of such business engaging in this state in any method of competition or in any act or practice not defined in NRS 686A.010 to 686A.310, inclusive, which is unfair or deceptive and that a proceeding by the Commissioner in respect thereto would be in the public interest, the Commissioner shall, after a hearing of which notice and of the charges against such person are given to the person, make a written report of the findings of fact relative to such charges and serve a copy thereof upon such person and any intervener at the hearing.

Melnick and Fonkych urge policymakers to limit:

“all-or-none” contracting by multi-hospital systems and prohibiting other anti-competitive contract language that flows from market power achieved by large multi-hospital systems. Such pro-competitive regulation would allow for hospital systems to integrate to improve efficiencies without the deleterious side effects of increased market power which can result in reduced price competition and higher costs to consumers.

A commissioner’s catchall authority might be invoked to accomplish this. Rhode Island’s Health Insurance Commissioner has promulgated “Hospital Contracting Conditions, [and] [t]hese conditions support

102. NEV. REV. STAT. § 686A.170(1) (2016); see also CAL. INS. CODE § 790.06(a) (West 2016); KY. REV. STAT. ANN. § 304.12-130(1) (West 2016); MONT. CODE ANN. § 33-18-1003(1) (2015); N.C. GEN. STAT. § 58-63-40(a) (2016).
103. Melnick & Fonkych, supra note 31, at 6 (footnote omitted).
affordable health insurance by making the approval of insurer rate filings contingent on the health insurer’s agreement to abide by contracting standards with hospitals that limit service price inflation, improve the quality of care, and work towards increased administrative efficiencies.”

The Hospital Contracting Conditions have two main provisions. One limits annual rates of price increases for inpatient and outpatient services to increases in the CMS Hospital Input Price Index plus 1% for each year covered by the contract. The second “require[s] that insurer contracts with hospitals include a quality incentive program, [in which] at least 50% of the annual price increase for hospitals must be” tied to performance on quality measures.

According to Christopher F. Koller, the former Rhode Island Health Insurance Commissioner, legal authority for promulgating the conditions was implied by the combination of the statutory mandate to improve health care quality and efficiency and the power to approve rates. The fact that no explicit oversight of hospital rates was granted to the Commissioner suggests that regulators in other states could also take an expansive view of catchall authorities to pursue this option.

Tools used by government agencies as active purchasers are not closely analogous to those available to the insurance regulator, but could conceivably be adapted. Covered California, the insurance exchange established in that state to implement the Affordable Care Act, has conditioned participation in its marketplace on an insurer’s efforts to obtain low prices from providers. Beginning in 2018, an insurer that wants to sell in the California exchange must “report on its strategy to assure that contracted providers are not charging unduly high prices, which may include but are not limited to: Telemedicine [and] use of Centers of Excellence.”

While the intent is not explicitly stated, the mention of teledmedicine and Centers of Excellence suggests that the state might encourage insurers to substitute providers who are outside the region for overpriced providers.

105. Id. at 12.
106. Id.
107. Id.
108. Id. at 12–13.
112. PLAN MGMT. ADVISORY GRP., supra note 111, at 18.
113. Id.
within its service area. An insurer might be able to find academic medical centers outside its geographic market that have prestige equal to local must-have providers but are willing to treat patients at a lower cost. Covered California has also indicated that by 2019, insurers “will be expected to exclude hospitals and other facilities that demonstrate outlier high cost.”

It is surely easier to tell insurers that they must exclude overpriced outliers from their networks in the exchange market than in the small group market because: (1) insurer participation in the exchanges is voluntary, and it is now presumed that it will constitute less than 100% of companies and (2) employer-sponsored insurance is a fringe benefit used to attract employees, so there is greater pressure to have a robust network. It might be easier to facilitate or mandate reference pricing, which preserves access to the high priced provider, than to ban the high-priced provider altogether.

With reference pricing, a payer includes expensive, must-have providers in its network but requires the patient to pay the difference between what a lower-cost provider charges and the higher price.

The payment limit typically is the median or some other mid-point in the distribution of prices in the local market. Consumers who select a provider that charges less than the purchaser’s limit receive standard coverage, with minimal cost sharing. Consumers who select a provider charging above the contribution limit must pay the entire difference.

The technique was pioneered by CalPERS, and it is unclear whether it has migrated from self-insured plans to fully-insured plans. Insurance regulators cannot set administered prices like Medicare or Maryland’s all-payer rate setting board; however, they could create safe harbors for reference prices by approving, in advance, acceptable price levels for a given procedure in a market. This could pressure high-cost providers to lower their prices. A commissioner might go a step further by declaring payments beyond a set luxury level to constitute an unfair insurance practice, having the effect of imposing a reference price requirement.

114. See id.
115. See id. at 18, 24.
116. Id. at 18.
117. See id. at 7, 13, 18, 22.
118. See Boynton & Robinson, supra note 80.
119. Id.
120. Id.
3. Convening Insurers to Fight Balance Billing

Under the *quantum meruit* doctrine, which governs medical billing in the absence of agreed-to price terms, out-of-network physicians are entitled only to UCR-based reimbursement.\(^1\)\(^{121}\) As such, an insurer’s payment of the UCR amount should suffice to make the physician whole—at least two courts have held that balance billing is restricted under such circumstances.\(^1\)\(^{122}\) But, because most consumers do not have the savvy or resources to fight these bills, which may have an adverse effect on credit scores, this plainly illegal business model has succeeded.\(^1\)\(^{123}\) Insurance regulators could spur insurers to pledge to defend collection lawsuits, which would likely bring an end to the out-of-network business model and bring these physicians into networks at lower prices.\(^1\)\(^{124}\)

Under common law principles, when a consumer obtains a service without an express agreement as to price, the legal doctrine of *quantum meruit* applies.\(^1\)\(^{125}\) The classic example of this, as explained by Judge Richard Posner in *Confold Pacific, Inc. v. Polaris Industries, Inc.*,\(^1\)\(^{126}\) is the patient who comes to the emergency room with no ability to inquire into or negotiate over prices.\(^1\)\(^{127}\) In such circumstances,

the plaintiff [doctor] is entitled to the market value of his services rather than to the benefit that he conferred on the defendant, which might be much greater—for example, if the plaintiff physician had saved the defendant’s life. The court tries to simulate a competitive market; and in such a market, price is based on the cost to the seller rather than on the subjective value to the buyer, which often is much greater.\(^1\)\(^{128}\)

The Pennsylvania Superior Court applied this doctrine in its decision in *Temple University Hospital, Inc. v. Healthcare Management Alternatives, Inc.*\(^1\)\(^{129}\) That case involved the amount the hospital was owed by a health insurer for services rendered after the network contract between the parties

\(^{123}\) See Dennis, 2016 WL 4717657, at *7.
\(^{124}\) See 42 R.I. GEN. LAWS § 42-14.5-2(5).
\(^{125}\) Confold Pac., Inc. v. Polaris Indus., 433 F.3d 952, 958 (7th Cir. 2006).
\(^{126}\) 433 F.3d 952 (7th Cir. 2006).
\(^{127}\) Id. at 958.
\(^{128}\) Id.
The superior court of Pennsylvania explained that in the absence of agreement on price terms, Pennsylvania “law implies a quasi-contract, which requires the defendant to pay to plaintiff the value of the benefit conferred,” or “a reasonable fee for a health provider’s services.” “Thus, in a situation such as this, the defendant should pay for what the services are ordinarily worth in the community.”

Since the relevant question is “what health care providers actually receive for those services,” if a provider rarely recovers its billed charges, those charges “cannot be considered the value of the benefit conferred because that is not what people in the community ordinarily pay for medical services.” The purpose of quantum meruit is to place the provider in the position he would have been had services been delivered in the ordinary course of business, not in a “better position than [he] would have been had the services been performed for the majority of [his] other patients.”

Therefore, in instances where the insurer has tendered a UCR amount, the doctor has been compensated in full. As such, there ordinarily

---

130. Id. at 505.
131. Id.
132. Id. at 506.
133. Id.
135. Id. at 508 (citing Eagle v. Snyder, 604 A.2d 253, 254 (Pa. Super. Ct. 1992)).
136. Id. (citing Eagle, 604 A.2d at 254).
137. Id. (citing Eagle, 604 A.2d at 254, 256).
138. Id.
should remain no lawful balance to collect from the patient. A Connecticut case, Gianetti v. Riether, has so held. 

Gianetti was a plastic surgeon on call in an emergency room. He treated the defendant and was reimbursed $349.54, on an out-of-network basis, by the defendant’s insurance company; he then billed the patient for the balance of his $425 charge, $75.46.

The court held that the doctor did not meet his burden of proving “that $425 was the reasonable value of such service.” “The plaintiff provided no evidence as to what similar doctors or physicians charge for similar work.” “The plaintiff provided no evidence concerning his usual and customary charges for similar work.” But the court went on:

Additionally, there is evidence from which the court can and does find that the reasonable value of the first item was only $349.54. The court takes judicial notice that health insurance companies typically reimburse physicians for the usual and customary charges for similar medical services by area physicians. The amount reimbursed is prima facie evidence of the reasonableness of such charges. The plaintiff has failed to rebut such evidence. Consequently, the court finds that the plaintiff was fully compensated therefor.

Similarly, the court in Dennis v. PHC-Martinsville, Inc., rejected a hospital’s billed charges of $111,115.37 and looked to “the reasonable value of . . . services rendered to” the patient. The court determined that it would be “the amount the hospital would have received had Dennis pre-paid his bill as an uninsured patient.” The hospital’s policy was to grant a 75% discount from its chargemaster amount in such circumstances. This amount was $27,778.84, which was $523.89 more than Dennis’s insurer had

---

142. See id.
144. See id. at *5.
145. Id. at *1.
146. Id. at *5.
147. Id.
148. Gianetti, 2011 WL 4347211, at *5,
149. Id.
150. Id.
152. Id. at *7.
153. Id.
154. Id.
paid.\textsuperscript{155} As such, unlike Gianetti’s patient, Dennis was ordered to pay a relatively small balance.\textsuperscript{156}

The hospital has appealed the ruling to the Virginia Supreme Court.\textsuperscript{157} Three Virginia health care lawyers commented that “the \textit{Dennis} decision is a shot across the bow for all hospitals” and “may have significant implications for the current rate-setting and debt collection process for hospitals.”\textsuperscript{158}

A third decision is worth mentioning here, although it does not involve interpretation of the common law.\textsuperscript{159} Texas’ workers compensation statute sets forth several criteria for fixing the compensation of out-of-network providers, one of which is a \textit{fair and reasonable} amount, which appears to be congruent with the standard for \textit{quantum meruit} awards.\textsuperscript{160}

\textit{Reimbursement of Air Ambulance Services Provided by PHI Air Medical}\textsuperscript{161} presented the question of whether an air ambulance service could collect its \textit{full billed charges} that were “typically at least two to three times the Medicare rate” when 72\% of the provider’s patients received 125\% of the Medicare rate or less.\textsuperscript{162} The insurance carriers involved had tendered reimbursement at 125\% of Medicare.\textsuperscript{163} An Administrative Law Judge, analyzing the facts under the \textit{fair and reasonable} criterion, found that the billed charges did not meet the standard because “patients should not be required to pay two or three times the rates paid by 72\% of PHI’s patients.”\textsuperscript{164}

In determining the appropriate reimbursement amount, the Administrative Law Judge looked to the provider’s operating costs.\textsuperscript{165} The judge settled upon 149\% of Medicare as fair and reasonable because it

\begin{flushright}
\textsuperscript{155} Id.
\textsuperscript{158} Id.
\textsuperscript{161} Decision and Order, \textit{supra} note 217.
\textsuperscript{162} Id.
\textsuperscript{163} Id.
\textsuperscript{164} Id.
\textsuperscript{165} Id.
\end{flushright}
reflects PHI’s average cost to provide service to each patient and to attain the profit it has earned the past few years. . . . [T]his is the amount that, if paid by every PHI patient, would allow PHI to operate exactly as it did during the time period at issue, making a profit that Carriers’ expert conceded is adequate. 166

When state common “law caps out-of-network physician fees at the market price, . . . legislation is not necessary to prohibit balance billing.” 167 The cases cited here indicate that balance billing is essentially a bluff that is not being called due to a collective action problem. 168 What is needed is a coordinated effort to enforce current law. While [a] commissioner may not have jurisdiction over providers, she does have jurisdiction over insurers, and can therefore convene insurers and consumer advocates to act cooperatively. Patients pay balance bills because: (1) they [do not] know their rights; (2) they are afraid of unpaid bills affecting their credit scores; and (3) they would be unable to defend a collection lawsuit if the physician staffing company filed one. All three of these barriers can be overcome through sub-regulatory action by [a] commissioner and cooperation by insurers. This has been done before.

. . . . [I]n the 1990s, no-fault auto insurers in Michigan were involved in a similar dispute with providers over the legality of balance billing. The insurers banded together, and with the approval of the insurance commissioner, did the following: (1) advised their insureds [not] to pay the balance bill; (2) told the insureds that if they were sued by the provider, the insurer would defend them and indemnify them if they lost the suit; (3) warned the credit reporting agencies [not] to report the balance on the consumer’s credit report. The providers did not file collection suits but instead filed two class action lawsuits—one in state court, one in federal—seeking a declaratory judgment of their right to collect balances. Both suits were quickly dismissed, and the problem was resolved.

. . . . [T]he favorable case law can be leveraged to protect . . . consumers . . . who are balance-billed [through] a collaboration in which stakeholders undertake the following activities: . . . Insurance Commissioner: respond to consumer complaints about balance billing by telling consumers they are free to disregard bills

166. Decision and Order, supra note 217 (footnote omitted).
167. Williams, supra note 160; see also Confold Pac., Inc. v. Polaris Indus., 433 F.3d 952, 958 (7th Cir. 2006).
168. See Confold Pac., Inc., 433 F.3d at 958; Williams, supra note 160.
if the insurer has paid the UCR amount—the commissioner may have to verify that insurers are using a legitimate method of determining UCR; confirm that the Temple [rationale] applies to all hospital-based out-of-network providers; admonish credit reporting agencies that they must not report balance-bill debts furnished by these providers because they are inaccurate; promulgate an official [Explanation of Benefits notification (“EOB”)]; . . . Insurers: commit to defending and indemnifying their insureds in the unlikely event of a physician’s collection lawsuit; notify consumers of their rights on EOB forms; . . . Consumer Advocates: coordinate activities; publicize the project; disseminate the project to other states; find consumer attorneys willing to sue under the Fair Credit Reporting Act if credit reporting agencies do not cooperate.

I would not anticipate a need for insurers to actually defend individual lawsuits. The staffing companies would need to pull physicians away from their hospital shifts to testify in court if collection cases were defended. [F]urther, these companies operate across states and could not afford the risk of making bad law—generating a direct unfavorable legal precedent—that could immediately force changes to their business model in other states. . . .

. . . [One suspects] that the simple fact of a joint announcement by [a] [c]ommissioner and insurers to pursue the Michigan option, communicated to consumers on the EOB, would suffice to end balance billing in [a state where it is a problem].169

If not, however, the [c]ommissioner could help facilitate bellwether trials.170 In the context of federal multi-district litigation, bellwether trials are arranged for cases deemed typical of the multiple claims consolidated before the multi-district litigation court.171 The outcomes of such trials give litigants a sense of the settlement value of claims, expediting compromise of all the litigation.172 In the context of out-of-network providers, bellwether trials could fix the quantum meruit value of services, ideally as a percentage

171. Advocacy Org. for Patients & Providers, 176 F.3d at 318, 328.
172. See id. at 318; Burns, supra note 51.
of Medicare rates. The commissioner could play a coordinating role in getting payers to share the costs of such trials.

V. CONCLUSION

The problem of excessive provider prices is well understood, well documented, and one for which several existing legal and practical remedies are available. In the Author’s view, the principal hurdle to alleviating the problem is one of will. The same multiplicity of purchasers that causes them disadvantage relative to providers in negotiating prices also deters individual purchasers from taking action upon which other purchasers could free-ride.

If lower health care prices are truly a public good, the solution is for government to marshal cooperative efforts among purchasers. The Insurance Commissioner’s authority and stature as a representative of consumer interests make that office a natural locus for coordination.


174. See Advocacy Org. for Patients & Providers, 176 F.3d at 328 n.9. Commissioners may also have a regulatory option: Mandating, as part of their enforcement of network adequacy regulations, that an insurer have at least one fully participating hospital in their network. See HEALTH BENEFIT PLAN NETWORK ACCESS AND ADEQUACY MODEL ACT § 5 (Nat’l Ass’n Ins. Comm’rs 2015). A fully participating hospital would be one that guarantees either that its hospital-based physicians will be in that insurer’s network, or that the hospital will hold patients harmless for any balance billing. See Burns, supra note 51; Gold et al., supra note 26. This concept, first suggested by a regulator participating in a National Association of Insurance Commissioners workgroup, draws inspiration from the Blue Cross Blue Shield Association’s Blue Distinction program. See Blue Distinction Centers of Excellence, EXCELLUS BLUECROSS BLUESHIELD, http://www.excellusbcbs.com/wps/portal/xl/prv/pc/coe (last visited May 8, 2017); Gold et al., supra note 26. That program lists Centers of Excellence for various procedures that have been vetted by BCBSA. See Blue Distinction Centers of Excellence, supra; Gold et al., supra note 26. The hospitals have the option of certifying that any hospital-based physicians delivering ancillary care during or in consequence of the procedure are also in-network, and presumably these hospitals will be more attractive to consumers worried about surprise bills. See Gold et al., supra note 26. The fully participating hospital proposal assumes two premises: First, that consumers would prefer such a hospital, even for emergency care, and consult their insurer’s provider directory—or heed a fully-participating hospital’s advertising—to learn which nearby hospital has that status; second, that hospitals would perceive a competitive advantage from the status and that one or more would require that the staffing agency granted the physician franchise in their facility agree to terms with insurers or submit their rates to binding arbitration. See id. To date, hospitals have been unwilling to impose such a requirement. Id.
STATE LAW GOVERNANCE OF HEALTH INFORMATION TECHNOLOGY

CASON SCHMIT*

Howdy! So I am new to Texas A&M and that is the official Texas A&M greeting. It is a little awkward for a former California boy to say. Thank you very much to NSU for welcoming me. Thank you to the faculty and staff. It is really an honor to be here.

So I am a recent transplant from the U.S. Centers for Disease Control and Prevention, and I have to acknowledge that a lot of what I am going to be talking about today is work that I did while I was there. I worked with a truly fantastic team of attorneys, including Gregory Sunshine, Dawn Pepin, Tara Ramanathan, Akshara Menon, and, of course, our director Matthew Penn, and they put a lot of work into what I am going to be presenting today.

Of course, as a former government attorney, we have to have our disclaimer. Believe me, these are not CDC official determinations or policies. This is [for] educational purposes only. I am an attorney, but I am not your attorney—[this is] not legal advice. So, let’s dive into this here.

[The] US Health system is in the middle of a digital revolution. It has already transformed the health systems efficiency, capacity, and function. Health information, in all shapes and sizes in all sectors of healthcare and public health systems, is being created and shared electronically. Electronic health information is incredibly diverse: it includes electronic medical records, laboratory reports, syndromic surveillance data, electronic prescriptions, vital records, and epidemiological reports. Digitization of health information allows for a single piece of health information to be used for multiple purposes simultaneously, and law plays a critical roll in this health information technology revolution. Every data type, every data use is governed by law. Consequently, the future of health information technology is heavily dependent on this legal framework. While some of the laws have changed to adapt to this new technology, in many cases, it is the technology that has been forced to adapt to the law.

Thirty years ago, the Office of Technology Assessment made the claim that “technological change is now outpacing the legal structure that governs the system, and [it] is creating pressures on Congress to adjust the

---

* This is a transcribed talk given by Cason Schmit, J.D. Schmit is a Research Assistant Professor in the Department of Health Policy and Management at Texas A&M University. He serves as the HIPAA Privacy Officer of the Texas A&M School of Public Health, and is a licensed attorney in the state of Arizona.
law to accommodate these changes.\textsuperscript{1} Now, given the pace of technological change, the age of this statement should be really alarming. Since then, the pace of information technology development has only increased, and I thought it would be interesting to put things in perspective for you. If we were to assume that the speed of legal adaptation has not changed—and knowing our current Congress, that is probably a little generous—if we assume that information technology remains consistent with Moore’s law by doubling about every two years, and if we assume that 1986 was the first time that the pace of technology passes or sped past the pace of legal adaptation, then we find a staggering difference in the rates of that change for technology and law. Under this methodology, legal adaptation is estimated to have changed by a factor of eleven, whereas pace of technology is estimated to have changed by a factor of 32,768. Obviously, this is a pretty crude estimation, but it is helpful to put things into perspective, the relative change between law and technology. These significant technological advances are not taking place in a regulatory vacuum. There are many preexisting laws that might apply to these new technologies; however, these existing laws are designed to handle the technology that was in place when those laws were enacted, and they often do not account for future technology developments. Thus, these laws can become quickly outdated, and this puts an incredible amount of stress on existing laws to compensate.\textsuperscript{2}

As technology advances, both the benefits and risks of technology are apparent. Society places rules on technology to attempt to balance the potential benefits with the potential risks. These rules come in many forms: They can be laws, they can be policies, they can be industry standards, but all of these rules collectively form the governance framework for that technology. Ideally, we would hope that a governance framework maximizes the potential benefits [and] minimizes the potential risks.

When I was with the CDC Public Health Law Program, we conducted a study of state laws on electronic health information. This study provides evidence that the current state law component of health information technology might be poorly suited to appropriately balance the risks and benefits of this rapidly evolving technology. Now, if true, the current governance framework for health information technology could leave us vulnerable to consequences of mismatches between technology and the law. Commentators note two significant consequences for these types of

\begin{footnotes}
\item[1.] U.S. CONG., OFFICE OF TECH. ASSESSMENT, OTA-CIT-302, INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION 3 (1986).
\item[2.] Gregory N. Mandel, Regulating Emerging Technologies, 1 L. INNOVATION & TECH. 75, 75 (2009).
\end{footnotes}
On one hand, outpaced laws could impede and stall technological development, and this would ultimately delay the potential benefits of that technology. On the other hand, outpaced laws might leave regulatory gaps that allow technology to develop unchecked, ultimately exposing society to the potential risks of the technology, potential and preventable in many cases.

Given this staggering estimated difference in health information technology that we just went through, health information technology is probably vulnerable to these two consequences. It is possible that state law frameworks are contributing to a stalled health information technology sector, delaying the true potential benefits of health information technology, and, conversely, there are probably some applications of health information technology that are not being regulated and that are exposing society to some potential risks.

Now, understanding the legal framework is critical to identifying strategies to improve health information technology governance. Commentators note that the dynamics between law and technology are similar to the tortoise and the hare allegory. So, in this allegory, the hare outpaces the tortoise, but then stops and rests while the tortoise eventually catches up. Once caught up, the hare eventually wakes up and continues the race. Technology, like the hare, moves very swiftly, but it can only progress so far before the laws become mismatched.

We see those mismatches, and users of health information technology start to experience more uncertainty, risk, or experience laws that are otherwise impeding the development of the technology. The law must catch up to technology to provide innovators with clarity to move forward. Health information technology is really a story of two hares. The first hare is information technology more generally, and this hare has taken off and introduced society to radical new applications and uses for health information generally. The second hare is health information technology specifically. This hare has been remarkably slow. In 2005, the chairman of the Center for Information Technology Leadership noticed the slow rate, and noted that the “healthcare information technology market [was] broken.”

Since then, the tortoise has made some progress. In 2009, the HITECH Act was passed, which is a federal law that incentivized the adoption and meaningful use of electronic health records, so this incentivized widespread

advances in health information technology. At CDC, we are interested in incentives that HITECH provided to health public health uses of health information technology, including case reporting, syndromic surveillance, and many new public health registries.

However, these new improvements to the health information technology infrastructure supported by HITECH enabled more uses of health information technology, including bidirectional communication between providers and public health, including the ability to have increased situational awareness tools in emergencies. In some cases, it has revolutionized the way that we investigate disease outbreaks. Many of these new health information technologies were initiated by state governments under new statutes and new regulations.

At the CDC Public Health Law Program, we investigated these laws to better understand this state legal landscape. So here is what we did: We used Westlaw to identify relevant laws using standardized search streams and systematic searches. Our search scope was limited to laws that related to electronic health information, and that is an incredibly broad net. We included only those laws that were in effect January 2014. We used two or three legal researchers to categorize each legal provision on the nature of the described use of the prescribed use within the law, and we did this blind to each other. We independently coded each legal provision, and then held meetings to discuss any inconsistencies to determine final consensus codes. Our coding scheme involved two types of codes—main-codes [and] cross-reference codes. We assigned every single law a main-code relating to the general purpose of health information within the law, or the general activity that comprised the focus of the law.

Now, some laws related to more than one use of health information technology or health information, so we assigned those laws cross-reference codes for whenever the law related primarily to one use but also referenced other uses in health information technology. Consequently, every law contained a main-code, but not every law had a cross-reference. This study identified 2364 state statutes and regulations relating to health information technology. State law frameworks varied qualitatively and quantitatively. Jurisdictions averaged just over forty-three laws. Texas, Oregon, and California were the states with the most laws—Texas had 145, Oregon had 104, [and] California had 103. We only found three territories with laws with health information technology—Guam, Virgin Islands, [and] Puerto

5. Cason Schmit et al., Assessing the Impact of State Laws Related to Electronic Health Information in the Centers for Medicare & Medicaid Services State Innovation Models Initiative, Presentation at the National Association of County and City Health Officials Annual Conference (Jul. 8, 2015).
Rico. Each of those had fewer than ten laws. Hawaii, South Carolina, Delaware, and South Dakota were the states with the fewest health information technology laws, and each of them had fewer than twenty laws. We identified three primary use categories relating to patient treatment: This is treatment in traditional settings, treatment in correctional settings, and treatment in educational settings. We also identified forty-six use categories that relate to other uses of health information apart from patient treatment. These secondary use categories are incredibly diverse, covering traditional public health functions, such as case reporting [and] vital records, to new public health registries, voter registration, and medical marijuana among many, many others. In total, we found 228 different main-code/cross-reference code combinations, suggesting that the landscape is not only big, it is incredibly complex, and states are approaching health information technology governance in very different ways.

It follows then that the race between law and technology does not involve one tortoise and a hare, it involves fifty tortoises running fifty very different races. This then begs the question: Is it good to have more laws? A number of scholars that have examined other emerging technology, such as bio-technology, nanotechnology, and genomics, have placed some pretty hard criticism on complex governance frameworks. Some have suggested the quality oversight can suffer without sufficient coordination, or that the multiplicity of statutes and agencies involved could create confusion among the regulated industry, reduce the clarity, or otherwise slow technological development. Others have argued that when there are multiple entities managing the risks, there is a chance they might neglect some risks by relying on other risk managers, or they can make decisions that have unintended consequences without sufficient coordination, or otherwise slow technological development here. [The] International Risk Governance Council has warned that whenever a governance system involves multiple entities [or] multiple responsibilities, there is a real danger that the risk response is not going to be coordinated. This can be duplicated efforts. We see this in HIT with health information exchanges and wasted resources, reinventing the wheel over and over again.

All these critiques aside, it might be the case this complex health information technology governance framework is inevitable. Many health

7. Mandel, supra note 2, at 82.
9. Id. at 16.
information technology applications are undertaken or at least supported by government entities. These government entities need legal authority to do these things. In many cases, this means new statutes and new regulations to authorize these new technological applications. Now, fortunately, this study does not conclude that more health information technology laws are necessarily bad for health information technology.\textsuperscript{10} It is undeniable that the federal HITECH incentives have been a driving force in health information technology adoption. Moreover, at the 2015 National Association for County and City Health Officials Annual Meeting, we reported that there are some important healthcare and public health objectives that are associated with jurisdictions with more health information technology laws. For example, using data from this assessment, we found that the number of laws relating to health information exchange among those states that are innovating—the state innovation model states—were positively correlated and significantly correlated with the percentage change and information sharing among federal acute care hospitals.\textsuperscript{11}

Similarly, we found that the number of laws relating to health information technology oversight was positively and significantly correlated with the percentage of non-federal acute care hospitals that are sharing public health data with local and state health authorities. Consequently, we have evidence that some types of laws could be enabling health information technology uses rather than stifling the development.

To kind of wrap things up with some key points here: This Public Health Law Program state law study revealed the governance framework for health information technology is incredibly complex and could pose a significant risk to health information technology development. However, given that many health information technology uses involve state actors, some of this complexity might be inevitable. Additionally, we do have evidence that at least some laws could be authorizing governments and enabling entities to engage in new and innovative health information technology uses.

So, moving forward, experience from other emerging technologies, such as biotechnology, genomics, and information technology more generally, these different approaches and different thoughts about governance with relation to these technologies might point to different innovative governance models for health information technology. Some people argue for the use and increase in soft law mechanisms. We have seen some industries rely on leveraging legal requirements for contracts between entities to impose a governance framework. We have also seen some

\begin{itemize}
\item \textsuperscript{10} Schmit, supra note 5.
\item \textsuperscript{11} See id.
\end{itemize}
proposals for adding and coordinating a governing entity among the different industries. We hope that this public health law program study can provide a strong foundation to analyze new approaches if people are so interested. With that, there is my contact information. Thank you very much. [applause]
KEEPING INTERNET PIRATES AT BAY: RANSOMWARE NEGOTIATION IN THE HEALTHCARE INDUSTRY

PAUL R. DEMURO*

I. INTRODUCTION.............................................................................. 350
II. THE BASICS OF RANSOMWARE ........................................... 352
   A. The History of Ransomware............................................. 353
   B. How Does Ransomware Infect Computers? .................... 354
   C. Ransomware and the Black-Market Economy............... 356
   D. The Threat of Ransomware in the Healthcare Setting..... 357
   E. Using a Negotiation Theory Approach to Solving the
      Ransomware Problem....................................................... 360
III. NEGOTIATING WITH PIRATES............................................. 361
    A. Piracy in the Modern Age............................................. 361
    B. The Piracy Ransom Negotiation Context...................... 362
    C. Arguments Against Paying Ransoms to Pirates............. 364
    D. Arguments in Favor of Paying Ransoms to Pirates........ 365
    E. Negotiation Solutions to the Ransom Problem: The Piracy
       Context.............................................................................. 365
IV. NEGOTIATING WITH TERRORISTS ....................................... 368
    A. The Heightened Interest of International Terrorism....... 369
    B. The International Law of Paying Ransoms to Terrorists.. 370
    C. The U.S. Approach to Paying Ransoms to Terrorists..... 371
    D. Insurance Policies Covering Ransom Payments to
       Terrorists ........................................................................... 372
    E. Solutions to the Ransom Problem: The Terrorism
       Context.............................................................................. 373
V. NEGOTIATING WITH RANSOMWARE HACKERS....................... 374
    A. The Existing Legal Framework for Ransomware
       Negotiations: The Health Insurance Portability and
       Accountability Act (“HIPAA”)............................................. 374

* Paul R. DeMuro, PhD, JD, MBA, CPA is an Associate Professor, Department of Sociobehavioral and Administrative Pharmacy, College of Pharmacy, Nova Southeastern University, Fort Lauderdale, FL, and Of Counsel, Broad and Cassel, Fort Lauderdale, FL. He can be reached at pdemuro@nova.edu or pdemuro@broadandcassel.com. The author wishes to thank Henry Norwood, a student at Nova Southeastern University, Shepard Broad College of Law, for his extensive research and writing contribution to this article.
1. Who Is Covered by HIPAA? ............................... 375
2. The HIPAA Privacy Rule .................................... 375
3. The HIPAA Security Rule ................................... 377
4. The HIPAA Breach Notification Rule.................. 380

B. Best Practices for Healthcare Organizations to Avoid Ransomware Attacks........................................................ 382
1. Backup—and Then Backup Your Backup........... 382
2. Controlling Access to Operating Systems .......... 383
3. Monitoring Inbound and Outbound Emails ........ 383
4. Human Error Is the Greatest Risk...................... 384
5. Cyber-Defensive Measures............................... 384
6. How HIPAA Helps ........................................... 384
7. Dealing with a Ransomware Attack ................... 385
8. The Role of Law Enforcement............................ 386

C. Negotiation Solutions to the Ransom Problem: The Ransomware Context .......................................................... 386
1. Arguments in Favor of Paying Ransoms to Ransomware Hackers .......................................... 390
2. Arguments Opposed to Paying Ransoms to Ransomware Hackers .......................................... 390

D. Alternative Solutions to the Ransomware Problem .......... 391
1. A Heightened Terrorist-esque Interest for Ransomware Negotiations ............................................. 391
2. Imposing a Tax on Ransomware Payments to Be Used for Anti-Hacking Efforts............................. 391
3. Prohibiting Insurance Coverage for Ransomware Attacks .......................................................... 392
4. Requiring Healthcare Organizations to Pass Annual Cyber-Inspections and Employ Cyber-Guards .................................. 393

VI. CONCLUSION .......................................................... 395

I. INTRODUCTION

The law plays a significant role in all negotiations, regardless of the context.¹ The law can determine the who, what, when, where, and why of all

¹ See Lucas V.M. Bento, Preserving Negotiation Whilst Promoting Global Order: Should We Bargain with Salt-Water Devils?, 19 HARV. NEGOT. L. REV. 285, 297
negotiations. Given the importance and power of law in the negotiation context, adopting clear legal principles tailored to negotiations in specific contexts will help willing and unwilling negotiators reach their desired outcomes. Negotiation comes into play in a number of different areas, both legal and otherwise.

One venue where the negotiation principles used in legal and non-legal areas coincide is the venue of ransom negotiations. Like other negotiations, ransom negotiations feature adverse parties with competing interests struggling to promote their own ends. With ransom negotiations, however, the stakes are often much higher than a standard negotiation and the party demanding the ransom payment has the opposing party at a distinct disadvantage.

Ransom negotiations take place fairly often in the contexts of piracy and terrorism. Several laws and a wealth of experience have shaped how negotiations in these contexts are able to progress. Insights into negotiations in these contexts can be used to shape negotiations in favor of the party facing a ransom demand in a different ransom context—the context of cybercrime. Cybercriminals continue to develop new inventive means of extorting valuable assets from computer users, including holding computer systems hostage. Cybercriminals are employing viruses that lock a computer user out of their own system and demand payment in return for

2. See Bento, supra note 1, at 297; Gifford, supra note 1, at 46; Hurder, supra note 1, at 253–54.
3. See Bento, supra note 1, at 297; Gifford, supra note 1, at 46; Hurder, supra note 1, at 253–54.
4. See Bento, supra note 1, at 297; Gifford, supra note 1, at 46; Hurder, supra note 1, at 253–54.
6. See Bento, supra note 1, at 307–08.
7. Id. at 308, 311; see also 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
8. See Bento, supra note 1, at 299; Rivka Weill, Exodus: Structuring Redemption of Captives, 36 CARDOZO L. REV. 177, 180 (2014).
regained control of the system.\textsuperscript{12} To make matters worse, these viruses are often capable of stealing private information from the captive computer as the virus locks down the system.\textsuperscript{13} The healthcare industry, with its endless amount of electronic private patient information and high-demand environment, is especially at risk from the virus.\textsuperscript{14}

This Article discusses the history, composition, and value of the ransomware virus, as well as its impact on the healthcare industry.\textsuperscript{15} The Article then moves to a discussion of negotiation and legal theories applied to the contexts of piracy and terrorism.\textsuperscript{16} After analyzing the existing legal framework of electronic private patient information in the healthcare industry, along with the best practices to avoid cyberattacks in the first place, negotiation theory is applied to the ransomware context to shed light on whether healthcare organizations should be permitted to engage in ransom negotiations with cybercriminals.\textsuperscript{17}

\section{The Basics of Ransomware}

Ransomware, as its name suggests, is a type of computer malware designed to extort ransom payments from its targets.\textsuperscript{18} Ransomware acts by infecting a computer, disabling the entire computer or disabling specific programs or functions of the computer, and presenting a message on the computer demanding a ransom payment in exchange for regaining the

\begin{itemize}
\item[13.] CCIPS WHITE PAPER, supra note 12, at 2.
\item[15.] See infra Part II.
\item[16.] See infra Parts II, III.
\item[17.] See infra Section IV.
\item[18.] CCIPS WHITE PAPER, supra note 12, at 2; Alexandre Gazet, \textit{Comparative Analysis of Various Ransomware Virii}, 6 J. COMPUTER Virology & Hacking Tech. 77, 77 (2010).
\end{itemize}
computer’s functionality. Ransomware has taken on many different forms and has evolved since its birth many years ago.

A. The History of Ransomware

The original ransomware would infect a computer, encrypt certain files in the computer so that the user could not open them without an decryption key, and demand a ransom payment in exchange for the decryption key. The modern day ransomware is capable of locking an infected computer’s screen, rendering the computer useless to the user. The virus will then display a message demanding payment in exchange for regained access to the computer. This modern form of ransomware is believed to have originated near Russia. Instead of simply demanding a ransom payment and disclosing the criminal nature of the screen lock, some early forms of ransomware would instead display a message on the infected computer purporting to be from Microsoft and claiming that in order to activate the computer, the user must send a text message to a phone number which would charge the user a premium charge for the text. The user would thus be sending what he or she thought was a simple activation text to Microsoft, but in reality his or her computer had been infected with ransomware and the premium charge from the text message was being collected by the hacker. Another early variant of the virus did not bother with concealing the criminal nature of the ransom and instead of posing as a representative of Microsoft, the hacker would simply display a pornographic image on the user’s screen and lock the screen with the image on display. The hacker would then send a message demanding payment through a similar premium charge phone call or text message as the Microsoft variant, in exchange for removal of the pornographic image and regained computer function. This version of ransomware was successful by shaming the

21. Id. at 3; see also CCIPS WHITE PAPER, supra note 12, at 2.
25. Id. at 4.
26. Id.
27. Id.
28. Id.
computer’s user into paying the ransom and this version lasted for quite some time.29

Starting around 2011, a new ransomware variant was introduced.30 The virus is similar to its predecessor in that the virus still locks the user’s computer screen or locks the user out of specific computer files.31 The major difference is in the content of the ransom message displayed on the computer user’s screen.32 The new displayed messages claim to be from a government agency, such as the Federal Bureau of Investigation (“FBI”), or from a local law enforcement agency.33 The fake message would inform the user that his or her computer had been locked because the user had committed a crime and the only way to regain access would be to pay a fine for the crime.34 Interestingly, some forms of the virus use accessible location services in order to determine where the infected computer is located geographically.35 Determining where the computer is located allows the hacker to tailor the ransom message to appear more legitimate, such as by ensuring the message is written in the predominant language where the computer is located and by displaying law enforcement images portraying the agencies existing in that country.36 This new ransomware also abandoned the premium charge text and phone method of collecting its ransoms.37 Modern ransomware hackers now take advantage of online pre-payment methods, which act similarly to online pre-paid visas.38 The computer user loads funds into an online account, which the hacker has access to using his or her own credit card.39 The hacker then retrieves the funds and decides whether to unlock the victim’s computer or dishonor their agreement.40

B. How Does Ransomware Infect Computers?

Of course, in order to ever succeed in their goal of extorting a ransom from their victims, hackers must first infect computers with the

30. Id.
31. Id.; Gazet, supra note 18, at 77; Zimmerman, supra note 5, at 16.
32. See O’GORMAN & MCDONALD, supra note 10, at 4.
33. Id. at 2.
34. Id. at 4; see also Gazet, supra note 18, at 77; Zimmerman, supra note 5, at 16.
35. O’GORMAN & MCDONALD, supra note 10, at 5.
36. Id.
37. Id. at 4–5.
38. Id. at 5.
39. Id.
40. O’GORMAN & MCDONALD, supra note 10, at 6; see also 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
ransomware virus. There are many different techniques used by hackers to infect computers with the ransomware virus. One of the most common methods used is referred to as a drive-by download. A drive-by download occurs when the hacker has already gone through the process of hacking into a website. The hacker then inserts hidden malware onto the website. An unsuspecting person visiting the website will automatically be redirected to a second website operated by the hacker, which installs the ransomware onto the person’s computer. In order to hack into a website in the first place, the website must have some type of vulnerability that the hacker can exploit.

To avoid the hassle of exploiting an already existing weakness in a website, some hackers legitimately buy advertising space on a website. The advertisement may purport to be promoting anything, but once the user clicks on the advertisement, the user is directed to the hacker’s website containing the ransomware virus.

A different tactic used by hackers is referred to as spear phishing. Spear phishing is a hacking technique where the hacker sends a false email to an employee of a company. The email may claim to be from the employee’s coworker or supervisor and may instruct the employee to follow a series of tasks, which would actually result in the employee infecting his or her system with a virus, such as ransomware.

Other means of infecting computers with the ransomware virus include piggybacking the virus onto a different form of malware already infecting a computer, or by sending out emails containing spam along with the virus. Ransomware will often be paired with another form of malware designed specifically to steal data and other information located on the infected computer. Thus, while the ransomware virus locks the computer

41. O’GORMAN & MCDONALD, supra note 10, at 2; Hagland, supra note 14.
42. O’GORMAN & MCDONALD, supra note 10, at 2.
43. Id. at 4; see also DUNBRACK, supra note 19, at 1.
44. O’GORMAN & MCDONALD, supra note 10, at 4.
45. Id.
46. Id.
47. Id.
48. Id.
50. DUNBRACK, supra note 19, at 1–2; Hagland, supra note 14; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
51. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; see also DUNBRACK, supra note 19, at 2.
52. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; see also DUNBRACK, supra note 19, at 2.
53. DUNBRACK, supra note 19, at 10; see also O’GORMAN & MCDONALD, supra note 10, at 4.
54. CCIPS WHITE PAPER, supra note 12, at 8.
and demands ransom from the victims, the additional malware is stealing data from the hostage computer.  

While the version of ransomware which requires a computer user to click on a certain advertisement or email is still commonly used, newer versions of the virus are being developed that rely on vulnerabilities in an organization’s web server. If a healthcare organization’s web server is unprotected or unpatched, hackers are able to exploit this weakness and infiltrate the organization’s online network. Once inside the network, the virus is able to move from the initial hacked computer to other computers using the same network, collect login data and credentials from employee staff, steal private stored data, and infect multiple systems with the ransomware virus.

C. Ransomware and the Black-Market Economy

The earning prospects for cybercriminals using the ransomware virus vary by country and by virus. In one study, a variant of the virus was discovered to have infected 5700 computers in approximately one day. Of this number, 168 users appear to have tried to free their computers by entering a pin number, which is given to the user by the hacker after the user pays the demanded ransom. The study demonstrated that the number of users who potentially paid the ransom was approximately 2.9% of those infected, the average amount demanded was $200, and that this would result in the hackers extorting $33,600 in ransom payments in a single month using this variant of the ransomware virus. Expanding this finding to an entire year, the researchers concluded that an estimated $394,400 could be transferred in ransom in an entire year with this virus if only 2.9% of the yearly targets pay. As of the beginning of 2016, over 4000 cyberattacks using the ransomware virus have occurred every single day on average. This number marks an increase of 300% when compared to the number of attacks that occurred in 2015. While these numbers alone are sufficiently

55. Id.
56. See DUNBRACK, supra note 19, at 2; O’GORMAN & MCDONALD, supra note 10, at 4.
57. DUNBRACK, supra note 19, at 2.
58. Id.
60. Id.
61. Id.
62. Id.
63. Id.
64. CCIPS WHITE PAPER, supra note 12, at 2.
65. Id.
significant to demonstrate the growing threat of ransomware, they may represent only a fraction of the total sums extorted from organizations, as many organizations do not report being attacked by ransomware hackers, nor do they report paying the hacker a ransom.66

The ransomware virus is being used by hackers moderately to aggressively target computers in the United States.67 Just as the virus itself has evolved over time, so has its targets.68

D. The Threat of Ransomware in the Healthcare Setting

Healthcare organizations are appealing targets to hackers.69 In 2015, healthcare organizations were targeted by cybercriminals more than most other industries.70 Some research suggests that on average, healthcare organizations experience a cyberattack almost every single month.71 The same research also suggests that nearly half of the healthcare organizations involved in the study had experienced a cyberattack within the past twelve months in which private patient information was at risk.72

66. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5. There are a number of reasons why an organization may choose not to report an attack. CCIPS WHITE PAPER, supra note 12, at 5. If word gets out that the organization was successfully attacked or, even worse, that the organization paid a hacker’s ransom demands, other cybercriminals may be encouraged to attack the organization upon seeing its willingness to pay or upon discovering its cyber-vulnerability. Id. The organization that pays a ransomware hacker may also be met with a negative reputation if word of the payment gets out because the organization has indirectly financed criminal activity. Id.

67. O’GORMAN & MCDONALD, supra note 10, at 9; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5. In May of 2017, a series of ransomware attacks worldwide resulted in hundreds of thousands of computer systems being infected from over one-hundred countries. Ross Koppel & Harold Thimbleby, Lessons from the 100 Nation Ransomware Attack, THE HEALTH CARE BLOG (May 14, 2017), http://thehealthcareblog.com/blog/2017/05/14/lessons-from-the-100-nation-ransomware-attack/.. The variant of the ransomware virus employed in these attacks has been labeled “WannaCry” and is believed to have been developed based on vulnerabilities in Microsoft operating systems, which were originally discovered by the U.S. National Security Agency. Id.; David Goldman, Global Cyberattack: A Super-Simple Explanation of What’s Going on, CNN (May 15, 2017), http://money.cnn.com/2017/05/14/technology/global-cyberattack-explanation/index.html.

68. Hagland, supra note 14.

69. Id.

70. Id.


72. Id.
The ransomware virus has been very effective at infecting healthcare organizations.\textsuperscript{73} Between 2005 and 2014, $57.6 million in ransom payments were made by healthcare organizations to ransomware hackers.\textsuperscript{74} During these years, ransom payments to hackers ranged from $200 to $10,000.\textsuperscript{75} However, in the year of 2015 alone, approximately $24 million in ransom payments were made by healthcare organizations to ransomware hackers.\textsuperscript{76} On February 12th, the Hollywood Presbyterian Medical Center in Hollywood, California fell prey to a ransomware attack.\textsuperscript{77} A doctor of the medical center claimed that the medical center’s system “was being held for ransom.”\textsuperscript{78} Later reports indicated that the health center had lost control of its electronic health record system for longer than a week and that those responsible demanded over $3 million in order to bring the medical center’s system back online.\textsuperscript{79} The CEO for the hospital later revealed that the medical center had paid approximately $17,000 to the hackers and the hackers had honored their word and restored the medical center’s access to their system.\textsuperscript{80} A March 28th incident revealed that integrated systems storing health data were also at risk when a Columbia-based integrated healthcare system was targeted by a ransomware virus.\textsuperscript{81} The system stored information for ten hospitals and the information systems reportedly took several weeks to restore while the hospitals attempted to function and care for patients as best as possible.\textsuperscript{82} A single attack on a Maryland-based hospital led to an $18,500 ransom payment.\textsuperscript{83}

Healthcare organizations are an appealing target to data hackers.\textsuperscript{84} Patients’ electronic health records are worth far more than a victim’s credit or debit card number.\textsuperscript{85} In fact, data indicates that electronic health records

\begin{flushleft}
\textsuperscript{73.} 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
\textsuperscript{74.} Id.
\textsuperscript{75.} Id.
\textsuperscript{76.} Id.
\textsuperscript{77.} Hagland, supra note 14.
\textsuperscript{78.} Id.
\textsuperscript{79.} Id.
\textsuperscript{80.} Id.
\textsuperscript{81.} Id.
\textsuperscript{82.} Hagland, supra note 14.
\textsuperscript{83.} DUNBRACK, supra note 19, at 2.
\textsuperscript{84.} See 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; Beek, supra note 14; William Maruca, Hacked Health Records Prized for their Black Market Value, FOX ROTHISCHILD LLP: HIPPA, HITECH & HIT (Mar. 16, 2015), http://hipaalegal.foxrothschild.com/2015/03/articles/articles/hacked-health-records-prized-for-their-black-market-value/.
\textsuperscript{85.} 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; Kevin Lonergan, Why the Healthcare Industry Badly Needs a Cyber Security Health Check,
may be worth ten times more to data hackers than a credit or debit card number. \(^{86}\) In 2015, there was a larger volume of U.S. based ransomware attacks than previously, specifically focusing on the healthcare industry. \(^{87}\) Healthcare organizations may be so appealing to hackers because every minute could literally be a matter of life and death, and every minute the organization does not have full access to its electronic information, each patient is at risk. \(^{88}\)

As noted above, electronic health records are extremely valuable to cyber hackers. \(^{89}\) Healthcare organizations are using and creating more electronic healthcare data than ever before. \(^{90}\) Electronic healthcare data allows healthcare providers different advantages to providing patients with quality care; however, with more data being stored in an online format, hackers have more targets and far more incentive to target the healthcare industry. \(^{91}\) Healthcare organizations are storing “valuable financial, insurance, and demographic data” which can be used, or sold to be used, to commit identity theft. \(^{92}\)

As an additional threat, hospital employees and medical staff are now using their personal or organization-provided mobile devices in order to access private patient health records stored on the organization’s servers. \(^{93}\) Alerts are sent to the mobile devices of healthcare staff to keep them informed of patients’ vital statistics. \(^{94}\) Medical imaging machines are connected to healthcare servers using the Internet. \(^{95}\) New technologies are being developed that allow constant health monitoring of patients by healthcare professionals, such as smart glasses. \(^{96}\) This constant stream of private health information is recorded and digitally sent to the healthcare organization’s servers where it becomes accessible to the monitoring healthcare professional. \(^{97}\) Older technology, such as copy machines, are also

---

\(^{86}\) 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; Lonergan, supra note 85; Maruca, supra note 84.

\(^{87}\) 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.

\(^{88}\) See DUNBRACK, supra note 19, at 1–3.

\(^{89}\) See 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; Lonergan, supra note 85; Maruca, supra note 84.

\(^{90}\) DUNBRACK, supra note 19, at 2–3.

\(^{91}\) Id.

\(^{92}\) Id. at 2.

\(^{93}\) Id. at 3.

\(^{94}\) Id.

\(^{95}\) DUNBRACK, supra note 19, at 3.

\(^{96}\) Id.

\(^{97}\) See id.
connected to the organization’s servers. Unfortunately, these technologies are very vulnerable to cyberattacks. It seems that as the technology itself boldly strides forward, the efforts to secure and protect the information being sent by the technologies are left behind.

E. Using a Negotiation Theory Approach to Solving the Ransomware Problem

Intelligent negotiation can aid in dispute-resolution without having to deal with lengthy and costly conflicts. Negotiators employing what is referred to as the problem-solving approach to negotiations appreciate the costs and benefits of each side of the negotiation and seek to reach a resolution beneficial to both sides. The problem-solving negotiator seeks creative solutions to disputes that will satisfy, at least in part, the goals of each party. Negotiation theory is an ideal framework from which to analyze negotiations with ransomware hackers, as it takes into account the costs and benefits of ransom negotiations, as well as considering other external factors, such as the legal landscape surrounding the negotiation and the human costs of ransom negotiations, which can aid negotiators dealing

98. Id.
99. Id. at 4. Hackers are already using these new technologies to breach healthcare organization’s networks. See Dunbrack, supra note 19, at 4. Connected technologies including “insulin pumps, heart monitors, and picture archiving and communication systems” have already been hacked in order to gain access to the connected healthcare organization’s network. Id.
100. Id. Ransomware hackers are able to use these new technologies as back doors to gain access to a healthcare network. Id. The hacker no longer needs to find vulnerabilities in the organization’s network itself, but instead hackers can breach the more vulnerable healthcare technologies that are connected and transmitting information to the network. Id. This type of back door hacking is known as medjacking. Dunbrack, supra note 19, at 4. After breaching the single, connected device, the hacker can use the virus to infiltrate the organization’s network and move from system to system on the network, infecting devices, and stealing information. See id. Once infected, cybercriminals could “take . . . control of the [specific] device itself, but this is uncommon, and hackers normally use these devices as a means of gaining access to the more lucrative prize of the connected organization’s network. Id. Healthcare organizations are woefully unprepared for this type of threat as most organizations have not integrated these new technologies into their existing security framework. See id.
101. Hurder, supra note 1, at 254.
102. Id. at 254, 273.
103. Charles B. Craver, Effective Legal Negotiation and Settlement 11–12 (7th ed. 2012); see also Spencer Punnett, Representing Clients in Mediation: A Guide to Optimal Results Based on Insights from Counsel, Mediators, and Program Administrators 412 (2013); Gifford, supra note 1, at 46.
with ransomware hackers and other criminal hostage-takers to achieve optimal results.\textsuperscript{104}

III. NEGOTIATING WITH PIRATES

Piracy poses a major threat across the globe to human life, the global economy, and the environment.\textsuperscript{105} Pirates who engage in hostage-taking for ransom payments put ransom negotiators in the position to save lives, while trying not to financially benefit the pirates.\textsuperscript{106} Effective negotiation can reduce these costs and creative legal strategies can reduce the incidence of piracy worldwide.\textsuperscript{107}

A. Piracy in the Modern Age

Piracy has become an increasing problem over the past decade.\textsuperscript{108} In 2008, pirates committed or attempted roughly 293 attacks.\textsuperscript{109} In 2012, the number of attacks increased to roughly 300.\textsuperscript{110} Pirates long ago realized that simply to pillage and plunder a seized vessel was a wasted opportunity when the vessel’s crew could be ransomed off for far more lucrative bounties.\textsuperscript{111} In fact, the ransoming of crewmembers has largely become the primary motivation for modern-day pirates seizing maritime vessels.\textsuperscript{112} Between 2008 and early 2014, ransom payments exceeding $300 million had been paid to pirates.\textsuperscript{113} In 2011, more than 1200 people were held for ransom by pirates.\textsuperscript{114} Of this number, 35 of the hostages and 111 pirates died during the process.\textsuperscript{115} Further, many piracy attacks never go reported at all, as ship owners try to keep the attacks quiet in order to avoid increased insurance

\textsuperscript{104} See CRAVER, supra note 103, at 11–12; PUNNETT, supra note 103, at 412; Bento, supra note 1, at 305; Gifford, supra note 1, at 46.
\textsuperscript{106} See Bento, supra note 1, at 313–14, 321–22.
\textsuperscript{107} See id. at 287–88, 292, 326; Hurder, supra note 1, at 254.
\textsuperscript{108} See Bento, supra note 1, at 294.
\textsuperscript{110} Id.
\textsuperscript{111} Bento, supra note 1, at 287, 304.
\textsuperscript{112} Id. at 287.
\textsuperscript{114} ICC IMB, supra note 109, at 24.
\textsuperscript{115} Id.
While the costs of human life and ransom payments may be the most prominent costs of piracy, there are also secondary costs involved in piracy situations, such as the costs to deliver the ransom, to repair damaged vessels, to replace stolen cargo, to pay for legal services, etc.\textsuperscript{117} The pirates’ course is simple: Seize the vessel while ensuring its continued navigability and seize the crew in order to maximize the pirates’ expected return for their efforts.\textsuperscript{118} The negotiation phase begins here and the stakes could not be higher: The lives of the sailors.\textsuperscript{119}

B. \textit{The Piracy Ransom Negotiation Context}

Recent history is replete with graphic examples of negotiations with pirates gone bad for many of the same reasons negotiations in the business or legal setting turn sour—miscommunication, refusal to cooperate, delayed payments, an aggressive negotiation style, technical difficulties, etc.\textsuperscript{120} In 2011, Somali pirates seized and killed four American sailors when negotiations fell apart between the pirates and the U.S. Navy.\textsuperscript{121} The next year, Somali pirates killed a sailor over the delay of a ransom payment.\textsuperscript{122}

Grisly illustrations of negotiations with pirates gone south tend to cloud the public’s perception of how pirates view these transactions: It is only business.\textsuperscript{123} From a pirate’s perspective, ransoming sailors is nothing more than a matter of financial gain.\textsuperscript{124} This is one of the major details separating the pirate from the terrorist.\textsuperscript{125} Although ransom situations may result in harm or death to the hostage crew, such situations may also conclude with the successful release of the hostages after the ransom is paid.\textsuperscript{126} In 2012, pirates attacked a Greek vessel and held its crew for

\begin{enumerate}
\item Bento, supra note 1, at 293.
\item Id. at 291.
\item See Bento, supra note 1, at 291.
\item See id. at 287–88.
\item Id.
\item Id. at 288; see also Dutton & Bellish, supra note 118, at 301.
\item See Pines, supra note 105, at 73–74, 78.
\item See id. at 78.
\item See Bento, supra note 1, at 303–04.
\end{enumerate}
ransom. If pirates never intend to make good on their ransom deals, they would eventually cease to exist because ransoms would no longer be paid.

The ransoms negotiated by pirates provide a means of financial support to both the pirate and to the local economy of the pirate’s community. The correlation between dismal local economic conditions and piracy provides insight into a pirate’s motivations. While the pirates’ actions are certainly deplorable, ignoring their motivations is a critical mistake for the negotiator on the other side of the table.

Attorney Lucas V.M. Bento distinguishes between three different interests at play in ransom negotiations with pirates. Non-pecuniary interests are those involving “the well-being of hostages during captivity, their safe release and post-incident care.” Pecuniary interests are those involved in recovering the vessel and its cargo. Lastly, hybrid interests are a combination of the first two interests. Bento explains that, although the majority of ransom negotiations involve hybrid interests, non-pecuniary interests tend to be more concerning.

Beyond the financial and non-financial interests at stake in pirate ransom negotiations, understanding the nature and complexity of pirate organizations is vital to reaching desired outcomes. Pirate organizations can vary in their sophistication just like other criminal syndicates. The pirates physically present and boarding their target vessels may not have the clout in a negotiation to make decisions on behalf of the pirate

sailors were held as hostages by pirates. Dubner & Chavers, supra, at 300. Of this total number, the pirates killed six of the sailors, leaving the remaining sailors alive. Id.

109. Dubber & Chavers, supra, at 300. Of this total number, the pirates killed six of the sailors, leaving the remaining sailors alive. Id.
127. Bento, supra note 1, at 295.
128. Id.
129. Dutton & Bellish, supra note 118, at 301.
130. See id. at 305–06.
131. See Dubner & Chavers, supra note 126, at 298–99; Lennox-Gentle, supra note 126, at 205; Pines, supra note 105, at 77–78.
133. Bento, supra note 1, at 291. Lucas V.M. Bento is an attorney based in New York specializing in international disputes and arbitration. Id. at 285 n.*.
134. Id. at 291.
135. Id.
136. Id.
137. Bento, supra note 1, at 291.
138. See Lennox-Gentle, supra note 126, at 205.
139. Dutton & Bellish, supra note 118, at 306; Lennox-Gentle, supra note 126, at 205–06.
organization.\(^{140}\) For the negotiator opposing the pirates, it is paramount to discover whether the pirates involved in the discussion have the authority to make flexible decisions or whether they are strictly following a preconceived plan with no option to deviate.\(^{141}\) Shedding light on all of the inner workings of a pirate organization is often impossible, but by putting in the effort to learn as much about the organization as possible, the opposing negotiator can increase the chances of arriving at a desired outcome.\(^{142}\)

C. Arguments Against Paying Ransoms to Pirates

International state actors differ in their approaches to addressing the problem of negotiating with and paying ransoms to pirates.\(^{143}\) Many nations, including the United States, France, Britain, Columbia, and Italy, as a matter of policy, oppose paying ransoms to pirates to free hostages, however these countries do not make the payment of pirate ransoms illegal.\(^{144}\) Somalia has illegalized the payment of ransoms to pirates.\(^{145}\) The opponents of paying ransoms to pirates contend that giving in to ransom demands only emboldens the pirates and encourages them to commit similar acts in the future because the pirates know their demands will be met.\(^{146}\) Further, opponents believe that paying ransoms indirectly funds the enterprise of piracy, thus giving the same pirates the means to conduct additional operations.\(^{147}\) An argument against paying a pirate’s ransom demands, often employed by the United States, is that piracy is commonly intertwined with other international crimes, such as terrorism.\(^{148}\) While international terrorism is a separate international crime from piracy, paying a ransom demand in response to one crime may end up resulting in the other.\(^{149}\)

In 2010, former President of the United States, Barack Obama, issued an executive order banning any financial transactions with certain

\(^{140}\) See Dutton & Bellish, supra note 118, at 305–06.
\(^{141}\) See id. at 301, 306; Pines, supra note 105, at 78.
\(^{142}\) See Lennox-Gentle, supra note 126, at 205.
\(^{143}\) See Bento, supra note 1, at 288–89; Dubner & Chavers, supra note 126, at 317–22; Lennox-Gentle, supra note 126, at 206–07.
\(^{144}\) Bento, supra note 1, at 288–89; Dubner & Chavers, supra note 126, at 320–22; Lennox-Gentle, supra note 126, at 206.
\(^{145}\) Somalia: Six Jailed for ‘Pirate Ransom’ Cash, BBC (June 20, 2011), http://www.bbc.co.uk/news/world-africa-13826050; see also Bento, supra note 1, at 288–89.
\(^{146}\) Bento, supra note 1, at 288–89; Dutton & Bellish, supra note 118, at 309–10.
\(^{147}\) Bento, supra note 1, at 289; Dutton & Bellish, supra note 118, at 309–310.
\(^{148}\) Bento, supra note 1, at 290; Lennox-Gentle, supra note 126, at 215.
\(^{149}\) Bento, supra note 1, at 290; Lennox-Gentle, supra note 126, at 214–15.
Somali organizations, some of which had ties to pirate gangs. The United Kingdom (“U.K.”) similarly criminalizes ransom payments made to pirate gangs with sufficient links to terrorist organizations. Thus, although very few state actors go as far as to illegalize ransom payments to pirates, some states ban these payments if there is a threat that the funds may end up in terrorist hands. The economic success of piracy has led to a pirate stock exchange, through which individual or corporate investors are actually investing in and receiving a cut of ransom payments given to pirates. Paying ransoms to pirates may encourage the growth of and continued investments to the industry of piracy globally.

D. Arguments in Favor of Paying Ransoms to Pirates

The maritime industry, however, has expressed concern that an outright ban on ransom payments would put sailors’ lives at risk and significantly hamper the industry as a whole. After all, what sailor would be interested in traversing pirate-infested waters with the knowledge that, if taken for ransom, nobody would be answering the call? Proponents of paying ransoms to spare the lives of hostages also note that, even if ransom payments are made illegal, pirates may simply amplify their violence toward hostages in order to compel the sailors’ family members—as well as ship owners—to make the illegal ransom payments.

E. Negotiation Solutions to the Ransom Problem: The Piracy Context

Many scholars argue against an absolute ban on negotiations with pirates. The varying interests of all parties involved should be weighed in

---

150. Bento, supra note 1, at 290.
152. See Dutton & Bellish, supra note 118, at 320, 322; Lennox-Gentle, supra note 126, at 214–15.
155. Id. at 313–14; Dubner & Chavers, supra note 126, at 319.
156. See Dubner & Chavers, supra note 126, at 319.
157. See ADJOA ANYIMADU, CHATHAM HOUSE, COORDINATING AN INTERNATIONAL APPROACH TO THE PAYMENT OF RANSOMS: POLICY OPTIONS FOR REDUCING RANSOM PAYMENTS 8 (2012); Dubner & Chavers, supra note 126, at 319.
158. Bento, supra note 1, at 326, 330; Dubner & Chavers, supra note 126, at 327.
order to assess the potential payoffs of each approach to the problem. The options available to governments and private parties or corporations facing ransom demands are either to pay the ransom or not to pay the ransom. The options available to pirates demanding ransom are either to release the hostages or not to release the hostages. Of these potential options, there is only one possible solution that benefits both parties: Where the government or private party pays the ransom and the pirates release the hostages. If the private party chooses not to pay the ransom and, by some miracle, the pirates choose to release the hostages unharmed, the private party will have achieved its goal in the negotiation, whereas the pirates’ goal will have been thwarted. If the private party pays the ransom, but the pirates do not release the hostages, or if the pirates kill the hostages, then the private party will have been thwarted, and the pirates will have achieved their goal. Lastly, if the private party chooses not to pay the ransom and the pirates choose not to release the crew—a scenario seen often—then neither party will have achieved their goals.

While this framework provides a view of the competing interest of the parties, it is insufficient on its own to shed light on an appropriate policy regarding paying ransoms to pirates. First, each option cannot be given equal weight, since the outcome in which the private party does not pay the ransom and the pirates release the hostages is unlikely; the outcome in which the private party pays the ransom and the pirates do not release the hostages is, at least, somewhat likely; and the situation where the private party pays the ransom and the pirates release the hostages can hardly be said to be an absolute win for the private party. The private party is already at a loss for having to negotiate with pirates to begin with, and thus, the parties are on unequal footing going into the negotiation. A key argument against paying ransoms is to prevent the funding of future criminal activity, a

159. See Bento, supra note 1, at 326, 330.
160. Id.
161. Id.
162. Id.
163. Id.
164. Bento, supra note 1, at 326, 330.
165. Id. In 2010, seven crewmembers were held hostage by pirates aboard the vessel, the Iceberg 1, for 800 days while the pirates’ demands for ransom went ignored. See Why David Cameron Will Not Stop Somali Pirates Getting Their Pieces of Eight, COLINFREEMANSITE (Sept. 6, 2012), http://www.colinfreemansite.wordpress.com/2012/09/06/why-david-cameron-will-not-stop-somali-pirates-getting-their-pieces-of-eight/. During this time, one of the crewmembers committed suicide. Id. The situation was resolved by military intervention. Id.
166. See Bento, supra note 1, at 326, 330.
167. See id.
168. See id.
response to which this analysis does not provide. However, completely banning private parties from paying ransoms to pirates could likely result in loss of life and remove that important option from the private party negotiator.

This struggle between two options, which many perceive as unacceptable, has led scholars to propose more creative solutions to the problem. A starting proposal argues that while private parties should be permitted to negotiate with and pay ransoms to pirates, state actors, such as the United States and the U.K., should have an absolute non-negotiation policy. That approach ensures state actors take a stance against the actions of pirates and, ideally, will work toward reducing and eliminating the source of the problem, piracy itself. Another solution is to permit private parties to pay ransoms to pirates, but to tax the ransom payments. The benefits of this solution are twofold: First, additional funds are raised which can be applied toward combatting piracy; and second, those in charge of the ships at risk will be incentivized to take extra care to prevent these situations from occurring and protecting their vessels as best as possible. The detriment of this solution is that victims of piracy are essentially being taxed for paying to spare the lives of their crew. A further solution proposes holding ship-owners liable to their crew for failing to properly safeguard them from pirates. The United States already permits sailors to sue ship-owners for negligence in situations involving pirate raids and for sending sailors into areas the owners know are plagued by pirate attacks. Another solution would be to require ship-owners to employ guards on voyages through

169. See id. at 327; Dutton & Bellish, supra note 118, at 313.
171. Bento, supra note 1, at 330–33; Dutton & Bellish, supra note 118, at 324–27.
172. See Bento, supra note 1, at 330 n.278.
173. Id.
174. Id. at 331.
175. Id. This solution also provides a silver lining to those opponents of paying any type of ransom to criminal pirates, in that the pirates who hold sailors for ransom are indirectly supporting the efforts to end piracy. Id. at 332. When private parties pay ransoms to pirates—in a sense rewarding pirates for their criminal activity—these ransom payments will then be taxed, and the proceeds will contribute to government efforts aimed at stopping piracy. Bento, supra note 1, at 332.
176. Id. at 331. An additional downside of this approach is that private companies paying ransoms for the release of their crew will be faced with an incentive not to report the incident at all in order to avoid being taxed on the ransom payment. Id. at 332.
177. Id. at 331.
178. Id. at 331–32.
pirate-infested waters.\(^{179}\) In 2009, the U.S. Coast Guard required ships traveling in dangerous areas near Africa to employ guards.\(^{180}\)

Negotiating with pirates need not feature an all-or-nothing outlook, in which a party either closes off from negotiations or where a party pays every ransom.\(^{181}\) A cost-benefit analysis should be conducted during every negotiation to ensure that the negotiator is able to maximize its benefits, minimize its losses, and weigh context-based factors accordingly.\(^{182}\) The ransom negotiator must also consider governmental efforts to curb piracy, such as taxes on ransom payments and ship-owner liability.\(^{183}\)

**IV. NEGOTIATING WITH TERRORISTS**

Terrorists frequently participate in kidnapping to bankroll their other terrorist activities.\(^{184}\) Ransoming off victims of terrorist kidnappings is highly lucrative and reports in recent years indicate that terrorists are receiving higher ransom rewards than in the past.\(^{185}\) Newer terrorist organizations, such as the Islamic State of Iraq and the Levant (“ISIL”), have used the tactic with great success and have shed light on the different approaches taken by various countries in dealing with ransom negotiations with terrorists.\(^{186}\)

---

179. See Bento, *supra* note 1, at 331.
180. *Id.*
181. See *id.* at 326; Gifford, *supra* note 1, at 60–62; Reynolds, *supra* note 132, at 612.
183. Bento, *supra* note 1, at 331; *see also* Dutton & Bellish, *supra* note 118, at 325–27.
185. Kazmir, *supra* note 184, at 326. The New York Times conducted a 2014 study demonstrating the growth in terrorist ransom payments. Rukmini Callimachi, *Paying Ransoms, Europe Bankrolls Qaeda Terror*, N.Y. TIMES (July 29, 2014), http://www.nytimes.com/2014/07/30/world/africa/ransoming-citizens-europe-becomes-al-qaedas-patron.html?_r=0. In 2003, Al Qaeda was ransoming hostages at an average of $200,000 per hostage. *Id.* Compare this with 2008 where two Canadian hostages were ransomed for $1 million, and with 2013 where four French hostages were ransomed for $40 million. *Id.* The New York Times study concluded that between 2008 and 2015 Al Qaeda, and its supporting organizations, have made approximately $125 million through hostage negotiations and ransom payments. *Id.*
A. The Heightened Interest of International Terrorism

When it comes to making ransom payments to terrorist organizations, there seems to be a heightened interest at play compared to paying ransoms to other brands of criminal organizations.\textsuperscript{187} This could be due to the intense hostility toward terrorism and the heightened threat communities tend to perceive when confronted with terrorism.\textsuperscript{188} In recent years, questions surrounding the wisdom of paying ransoms to terrorists have been thrust to the forefront of public attention, given the rise of ISIL.\textsuperscript{189} ISIL is known to have taken hostages from at least twelve different countries, including the United States, England, Italy, Russia, France, Denmark, Sweden, Switzerland, Spain, and Belgium.\textsuperscript{190} Many of these hostages have been ransomed and returned to their respective countries, while others are still being held by the organization.\textsuperscript{191} The threat posed by international terrorism has led to it generally being treated as a heightened interest in terms of ransom and other laws.\textsuperscript{192} The heightened interest is utilized as a policy argument in support of an outright ban on ransom payments to terrorist organizations, whereas, in other criminal enterprises, an outright ban on cooperative efforts is typically shied away from.\textsuperscript{193}

Countries have taken different approaches to the problem of negotiating with and paying ransoms to terrorist organizations.\textsuperscript{194} This patchwork of differing laws and policies is complicated further by international legal entities, such as the United Nations ("U.N.")\textsuperscript{195}, which also has set forth extensive resolutions on the issue.\textsuperscript{195}

\begin{itemize}
\item \textsuperscript{187} Weill, supra note 8, at 184–85.
\item \textsuperscript{188} Id.
\item \textsuperscript{189} Kazmir, supra note 184, at 327.
\item \textsuperscript{191} See Mullen, supra note 190; Yourish, supra note 190.
\item \textsuperscript{192} Bento, supra note 1, at 301–04; Dutton & Bellish, supra note 118, at 319–20.
\item \textsuperscript{193} Bento, supra note 1, at 301–04; Dutton & Bellish, supra note 118, at 319–20.
\item \textsuperscript{194} See Kazmir, supra note 184, at 328, 337–40.
\item \textsuperscript{195} See id. at 329.
\end{itemize}
B. The International Law of Paying Ransoms to Terrorists

The U.N. and other international legal entities have taken the broad, outward position that ransom payments should generally be banned. However, this position, along with the resolutions passed by U.N. member-states, are not binding under international law. In 2009, the U.N. passed Security Council Resolution 1904, which mandates that U.N. member-states freeze funds and assets in order to prevent ransom payments, but the resolution did not explicitly ban paying ransoms to terrorists. Security Council Resolution 2133, which was passed in 2014, required states to prohibit terrorist organizations from “benefiting directly or indirectly from ransom payments.” Finally, in 2015, the U.N. passed Security Council Resolution 2199, which prohibits member-states from paying ransoms to terrorist organizations. Security Council Resolution 2199 is surprisingly broad in its scope, in that the resolution prohibits the payment of any ransom payment by anyone, “regardless of how or by whom the ransom is paid,” to a terrorist organization listed on a designated list of sanctioned terrorist organizations. Despite the seemingly clear stance the U.N. has taken in its approach to paying ransoms to terrorists, its resolutions have not resulted in any prosecutions of either state-members or private individuals who have made ransom payments to prohibited terrorist organizations. The laws and policies supported by individual countries regarding ransom payments are far more complicated than the U.N.’s approach and send an inconsistent international approach to ransom payments. Some countries, including the United States and the U.K. strongly oppose the practice of paying ransoms to terrorists. On the other hand, there are countries, including Germany and France, which publicly take a stance against paying terrorist ransom demands, but have allegedly made such payments.

196. Id. at 329–30.
197. Id. at 329.
201. Id.
202. Kazmir, supra note 184, at 337.
203. Id.
204. Id. at 337–38.
205. Id. at 338; Yourish, supra note 190. France has actually made it illegal to provide financial, or other support, to terrorist organizations and it is unclear if French citizens
C. The U.S. Approach to Paying Ransoms to Terrorists

The United States takes the approach of banning ransom payments to terrorists and has tried to dissuade individual citizens from making such payments. Families of U.S. hostages have accused the U.S. government of threatening them with legal prosecution if the families attempted to pay terrorists’ ransom demands to secure the return of their family members. In response to such accusations, the U.S. government has stated that it does not engage in threatening the families of hostages being held by terrorist groups, but claims it has a policy of informing such families of the laws in place that prevent the government or private U.S. citizens from making ransom payments to terrorist groups. This dissuasion has led to some controversy between the U.S. government and U.S. citizens who want the government to support the release of their family members being held hostage.

The Patriot Act is the legal instrument through which paying ransoms to terrorist organizations may be deemed illegal in the United States. Section 2339B of the Patriot Act makes it unlawful for any person to knowingly provide material support to terrorist organizations. This section imposes a prison sentence of between fifteen years to life for

would be prosecuted for paying terrorists’ ransom demands in order to secure the release of their hostage family members. CODE PENAL [C. PÉN.] [PENAL CODE] art. 421-2-2 (Fr.).


Michael Isikoff, Sotloff’s Parents Told They Could Be Prosecuted for Paying Ransom to IS, YAHOO NEWS (Sept. 12, 2014), http://www.yahoo.com/news/sotloff-s-parents-were-told-they-could-be-prosecuted-for-paying-ransom-to-is-234329991.html?ref=gs; Paula Mejia, U.S. Threatened James Foley’s Family Over ISIS Ransom Demand, His Mother Says, NEWSWEEK (Sept. 12, 2014, 5:16 PM), http://www.newsweek.com/us-threatened-james-foleys-family-over-isis-ransom-demand-270151. The families of two U.S. citizens, James Foley and Steven Sotloff, held hostage by ISIL, both reported being threatened with criminal prosecution by the U.S. government if they attempted to pay ISIL’s ransom demands in exchange for their family members. Isikoff, supra; Mejia, supra.

Kazmir, supra note 184, at 339–40; Mejia, supra note 207.

Family Releases Statement on Death of Warren Weinstein in U.S. Operation, WASH. POST (Apr. 23, 2015), http://www.washingtonpost.com/news/postnation/wp/2015/04/23/family-releases-statement-on-death-of-warren-weinstein-in-u-s-operation/?utm_term=.7a897b402cf9. Warren Weinstein was a U.S. citizen taken hostage by al-Qaeda. Id. Weinstein was killed by a drone strike conducted by the United States, while Weinstein was being held by the terrorist group. Id. Weinstein’s wife would later express her desire for a more consistent approach by the U.S. government in aiding hostages and supporting their families. Id.


Id. § 2339B(a)(1).
violations, depending on whether any loss of life results from the violation.\footnote{212} To violate section 2339B of the Act, the person providing material support must do so knowing that he or she is providing support to a terrorist organization.\footnote{213} Further, the violator must provide material support, which can be monetary support, training, advice, etc.\footnote{214} While there is nothing illegal under this section with the U.S. government or a private citizen having a conversation, or even negotiating with a terrorist organization, providing support—such as through a ransom payment—would violate this section of the Patriot Act.\footnote{215} However, section 2339C of the Patriot Act prohibits financing terrorism, attempting to finance terrorism, or conspiring to finance terrorism.\footnote{216} Thus, under section 2339C, the U.S. government or the family of a hostage may violate the Patriot Act by negotiating with terrorists under the Attempts and Conspiracy provisions of section 2339C.\footnote{217} This section, however, does include a heightened intent requirement, mandating that a violator of the section must intend that his or her support be used for terrorist activities.\footnote{218} If negotiations are permitted by section 2339C, the payment of ransoms to terrorist organizations would be a violation of both sections 2339B and 2339C.\footnote{219}

D. Insurance Policies Covering Ransom Payments to Terrorists

To offset the high prices of negotiation and ransom payments, some insurance companies offer kidnapping and ransom (“K&R”) insurance.\footnote{220} These policies can cover a number of aspects in ransom negotiations, including fees necessary for consultations, any money lost while actually recovering the hostage, and the ransom payment itself.\footnote{221} While it is unclear how various countries will treat K&R insurance policies that seemingly flout
laws by illegally providing financial support to terrorists, such as the Patriot Act, the U.K. has designed legislation intended to criminalize such policies.\textsuperscript{222}

E. \textit{Solutions to the Ransom Problem: The Terrorism Context}

The United States’ rationale for banning ransom payments to terrorists is that doing so would place U.S. citizens at an even higher risk of being targeted as hostages by terrorist organizations.\textsuperscript{223} The idea behind the argument in favor of an outright ban on paying ransoms to terrorists is that making such payments would only incentivize and legitimize the practice of hostage-taking and indirectly fund the terrorists’ operations.\textsuperscript{224} The downside to this argument is that placing a blanket ban on ransom payments reduces a ransom negotiator’s flexibility to employ that option, which tends to result, as we often see, in a state actor or international entity paying the ransom anyway in direct violation of its own policy.\textsuperscript{225} Closing the door entirely on negotiations cuts off any possibility of engaging in conversations that may prove beneficial from a \textit{cost-benefit} perspective for the ransom negotiator.\textsuperscript{226}

An approach that attempts to remedy this issue is referred to as a \textit{process-structural approach}.\textsuperscript{227} This approach is designed to “take the specific individual into consideration, while bolstering his or her bargaining power and reducing terrorists’ incentives to kidnap.”\textsuperscript{228} First, this approach to dealing with terrorists’ ransom demands is to be set out by statute to ensure the public understands their government’s approach to dealing with the issue.\textsuperscript{229} Next, any decision to accept or decline a ransom demand must be met with the approval of the Executive Branch and a majority of the Legislative Branch.\textsuperscript{230} Deliberations over whether or not to accept the demand are to be conducted in private and the government will simply

\begin{footnotesize}
\begin{enumerate}
224. Weill, \textit{supra} note 8, at 192, 196.
225. \textit{See id.} at 202–05.
226. \textit{Id.} at 205.
227. \textit{See id.} at 217.
228. \textit{Id.}
229. Weill, \textit{supra} note 8, at 211, 217.
230. \textit{Id.} at 218. The theory is designed to aid democratic governments in addressing the issue of ransom demands by terrorists. \textit{Id.}
\end{enumerate}
\end{footnotesize}
answer whether they accept or decline the ransom demand.\textsuperscript{231} The families of the hostages are to be given a hearing on the matter, during which the families can make their own case for paying or not paying the ransom.\textsuperscript{232} The goal of this approach is to maximize a government’s bargaining power by conducting closed-door discussions over whether the ransom deal would be to the country’s advantage, while at the same time giving the entire ransom negotiation process uniformity, structure, and fairness to the hostages and their families.\textsuperscript{233} Such a policy may give ransom negotiators enough flexibility to maximize the return for their party’s interests, minimize their costs, and save lives.\textsuperscript{234}

V. \ \textsc{Negotiating with Ransomware Hackers}

Although never having to engage with a ransomware hacker is the best-case scenario, many healthcare organizations find themselves having to do so following a successful attack.\textsuperscript{235} Ransom negotiators working on behalf of healthcare organizations in the face of a ransomware attack must deal with the same principles as ransom negotiators in other contexts: Maximizing benefits while minimizing costs, accounting for victim-based factors, and remaining in compliance with existing legal boundaries.\textsuperscript{236}

A. \textit{The Existing Legal Framework for Ransomware Negotiations: The Health Insurance Portability and Accountability Act ("HIPAA")}

HIPAA has become synonymous with private patient healthcare information.\textsuperscript{237} HIPAA is intertwined with the threat posed by ransomware because the virus may steal electronic private patient information from healthcare providers.\textsuperscript{238} A ransomware attack may rise to the level of a breach under HIPAA if the hacker actually obtains the protected patient

\begin{footnotes}
\footnote{231. \textit{Id.} at 220.}
\footnote{232. \textit{Id.} at 225.}
\footnote{233. \textit{See Weill, supra} note 8, at 220, 225, 230.}
\footnote{234. \textit{See id.} at 217.}
\footnote{235. \textit{See CCIPS WHITE PAPER, supra} note 12, at 2, 7.}
\footnote{236. \textit{Id.} at 5, 7; Weill, \textit{supra} note 8, at 217, 225.}
\footnote{237. \textit{See U.S. DEP’T OF HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA} 1, 3 (2016).}
\footnote{238. \textit{See CCIPS WHITE PAPER, supra} note 12, at 2; Zimmerman, \textit{supra} note 5, at 16.}
\end{footnotes}
information, which would be an unpermitted disclosure “which compromises the security or privacy of the protected [personal] health information.”

1. Who Is Covered by HIPAA?

As a starting point, HIPAA only governs “covered entities and business associates.” Covered entities include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that transmit electronic information. Covered entities also include health insurance companies, HMOs, employment-based health plans, Medicare, Medicaid, other government health insurance programs, and healthcare clearinghouses. These covered entities must abide by HIPAA’s numerous provisions and they may also be held liable under certain HIPAA provisions.

2. The HIPAA Privacy Rule

The HIPAA Privacy Rule creates national standards designed to protect private health information. The Privacy Rule applies to a certain type of information, known as protected health information. Protected health information, also referred to as individually identifiable health information, is information relating to: “[T]he individual’s past, present, or future physical or mental health or condition; the provision of healthcare to the individual; or the past, present, or future payment for the provision of healthcare to the individual,” which either identifies the specific person or which can reasonably identify that person.

Individually identifiable health information cannot be used by covered entities for any reason other than reasons allowed in the Privacy Rule or if the individual, whose information is at issue authorizes, in writing, the information to be used for specific purposes. The information cannot

---

239. 45 C.F.R. § 164.402 (2015); see also CCIPS WHITE PAPER, supra note 12, at 2; Zimmerman, supra note 5, at 16.
241. Id.
242. Id.
243. Id.
245. Id.
246. Id. at 3–4; see also 45 C.F.R. § 160.103 (2005).
be disclosed by covered entities unless it is disclosed to the actual individuals, upon request, or to certain government agencies if there is an ongoing investigation.\textsuperscript{248} Covered entities also may use or disclose this information for the organization to treat, pay, and conduct other healthcare activities.\textsuperscript{249} Treatment includes “the provision, coordination, or management of healthcare and related services for an individual by one or more healthcare providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.”\textsuperscript{250} Payment includes activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for healthcare delivered to an individual and activities of a healthcare provider to obtain payment or be reimbursed for the provision of healthcare to an individual.\textsuperscript{251}

Healthcare operations include several actions, such as:

\begin{itemize}
  \item [(a)] quality assessment and improvement activities, including case management and care coordination;
  \item [(b)] competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation;
  \item [(c)] conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs;
  \item [(d)] specified insurance functions, such as underwriting, risk rating, and reinsuring risk;
  \item [(e)] business planning, development, management, and administration;
  \item [(f)] business management and general administrative activities of the entity, including but not limited to: \textsuperscript{D}e-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.\textsuperscript{252}
\end{itemize}

Further, the Privacy Rule requires covered entities to implement safeguards designed to ensure individually identifiable health information

\begin{itemize}
  \item \textsuperscript{248} 45 C.F.R. § 164.502(a)(2) (2005); U.S. Dep’t Health & Human. Servs., supra note 244, at 4.
  \item \textsuperscript{249} 45 C.F.R. § 164.506(c)(1)(i)–(ii) (2005); U.S. Dep’t Health & Human. Servs., supra note 244, at 4–5.
  \item \textsuperscript{250} U.S. Dep’t Health & Human. Servs., supra note 244, at 5; see also 45 C.F.R. § 164.501 (2005).
  \item \textsuperscript{251} U.S. Dep’t Health & Human. Servs., supra note 244, at 5; see also 45 C.F.R. § 164.501.
  \item \textsuperscript{252} U.S. Dep’t Health & Human. Servs., supra note 244, at 5; see also 45 C.F.R. § 164.501.
\end{itemize}
remains private and is not made public intentionally or unintentionally.\textsuperscript{253} Individuals also can request that covered entities restrict access to their individually identifiable health information strictly for the purposes of treatment, payment, and other healthcare activities.\textsuperscript{254} If a covered entity fails to abide by HIPAA’s Privacy Rule, it may be subject to civil monetary penalties.\textsuperscript{255} Penalties can range from $100 to over $50,000, with an annual cap on the amount an organization may be penalized of $1,500,000.\textsuperscript{256} The penalty imposed depends on the circumstances of the privacy breach, including any possible intent or negligence on the part of the covered entity in regard to the privacy breach.\textsuperscript{257} If the organization was not willfully negligent in regard to the privacy breach and the organization remedied the breach within thirty days of the organization discovering the breach or within thirty days of the day the organization should have known of the breach, then a civil penalty will not be imposed.\textsuperscript{258} Criminal penalties also may be imposed for intentional breaches of the HIPAA Privacy Rule, which ranges depending upon the circumstances of the breach, with more egregious violations, such as violations committed with commercial motives, often resulting in penalties.\textsuperscript{259}

3. The HIPAA Security Rule

The HIPAA Security Rule mandates that entities covered by the Act implement measures that can work to lower an entity’s risk of any cyberattack.\textsuperscript{260} The Security Rule applies to a specific type of protected health information, referred to as “electronic protected health information.”\textsuperscript{261} Electronic protected health information is protected health information transmitted by the organization using some electronic means.\textsuperscript{262}

The Security Rule requires organizations to conduct regular risk analyses to detect potential vulnerabilities to the electronic protected health

\begin{footnotesize}
253. 45 C.F.R. § 164.530(c)(1) (2005); U.S. Dep’t of Health & Human Servs., \textit{supra} note 244, at 1, 3.
254. 45 C.F.R. § 164.522(a)(1) (2005); U.S. Dep’t of Health & Human Servs., \textit{supra} note 244, at 4.
255. \textit{See} U.S. Dep’t of Health & Human Servs., \textit{supra} note 244, at 17.
256. \textit{Id.} at 17–18.
257. \textit{See id.}
258. \textit{Id.} at 17.
259. \textit{Id.} at 18.
261. \textit{Id.}
262. \textit{Id.}
\end{footnotesize}
The organization then must work to minimize these vulnerabilities. Organizations must have protocol in place to detect and prevent malicious software from infecting their computer systems. Users of healthcare organization computer systems must be trained on how to protect their systems against malicious software, as well as reporting any suspicions that malicious software has infected one of the organization’s systems. The Security Rule also requires healthcare organizations to use access controls, allowing only necessary users to have access to electronic protected health information. The Security Rule requires organizations to conduct a risk analysis of all threats to any electronic protected health information generated by the organization or its affiliates to determine if any electronic protected health information is in jeopardy of theft, exposure, or loss. Covered entities must also ensure that their entire workforce is in compliance with the Security Rule.

Although the Security Rule is somewhat similar to the Privacy Rule, in its application to electronic protected health information, the Security Rule does require two additional broad measures regarding health information. First, organizations must maintain the integrity of electronic private health information under the Security Rule. Integrity is defined by the Security Rule as ensuring that the electronic protected health information is not destroyed or altered without authorization. The Security Rule also requires organizations to maintain electronic protected health information’s availability. Availability is defined by the Security Rule as maintaining the accessibility and usability of electronic protected health information.

The Security Rule further requires covered entities to conduct a risk analysis, which must include several components. The analysis must identify possible threats to electronic protected health information and assess

263.  Id.
265.  See 45 C.F.R. § 164.306(a)(2), (e); Summary of the HIPAA Security Rule, supra note 260.
266.  See Summary of the HIPAA Security Rule, supra note 260.
267.  Id.
268.  45 C.F.R. § 164.306(a); Summary of the HIPAA Security Rule, supra note 260.
269.  Summary of the HIPAA Security Rule, supra note 260.
270.  Id.
271.  45 C.F.R. § 164.304 (2015); Summary of the HIPAA Security Rule, supra note 260.
273.  Id.
274.  Id.; 45 C.F.R. § 164.304.
the impact of such threats, as well as the likelihood that they will occur.\textsuperscript{276} The organization must develop measures to deal with the risks identified.\textsuperscript{277} The measures taken to deal with security threats must be recorded.\textsuperscript{278} Finally, the organization must maintain the security measures implemented.\textsuperscript{279}

In order to ensure that these provisions are applied and upheld, healthcare organizations are required to name a security official whose role is to ensure that their organization is following through on these procedures.\textsuperscript{280} Covered organizations are required to implement policies authorizing only certain staff members to have access to electronic protected health information.\textsuperscript{281} Organizations must train and supervise all personnel handling electronic protected health information.\textsuperscript{282} If a member of an organization’s staff violates the organization’s internal safeguards, the organization must issue appropriate sanctions.\textsuperscript{283} Organizations must periodically review their procedures and ensure their staff is in compliance.\textsuperscript{284}

The Security Rule also provides for a number of provisions designed to ensure the physical safety of electronic protected health information.\textsuperscript{285} Organizations must ensure their physical facilities, where they keep the equipment storing their electronic protected health information, are secure.\textsuperscript{286} Covered entities must also ensure that only authorized personnel are able to

\begin{itemize}
\item \textsuperscript{276} 45 C.F.R. § 164.306(b)(2)(iv) (2015); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{277} 45 C.F.R. § 164.308(a)(1)(ii)(B) (2015); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{279} 45 C.F.R. § 164.306(e); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{280} 45 C.F.R. § 164.308(a)(2) (2015); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{281} 45 C.F.R. § 164.308(a)(4)(i); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{282} 45 C.F.R. § 164.308(a)(5)(i); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{283} 45 C.F.R. § 164.308(a)(1)(ii)(C); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{284} 45 C.F.R. § 164.308(a)(8); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{285} 45 C.F.R. § 164.310(a)–(d) (2015); \textit{Summary of the HIPAA Security Rule, supra} note 260.
\item \textsuperscript{286} 45 C.F.R. § 164.310(a); \textit{Summary of the HIPAA Security Rule, supra} note
access devices storing electronic protected health information.\textsuperscript{287} Further, the entity must have policies in place designed to protect its electronic protected health information during its “transfer, removal, disposal, and re-use.”\textsuperscript{288}

The HIPAA Security Rule imposes a number of technical safety measures, including access controls, which allow only certain users to access systems containing electronic protected health information and only for certain purposes.\textsuperscript{289} Organizations also must install hardware, software, or other methods designed to record how the information is being used and accessed by the organization.\textsuperscript{290} Steps must be taken to ensure that the information is not destroyed or modified without authorization, as well as steps taken to ensure the information is monitored to ensure it is not destroyed or modified.\textsuperscript{291} Finally, the Security Rule requires organizations to take steps to ensure that electronic protected health information is secured and protected when being transmitted electronically.\textsuperscript{292}

4. The HIPAA Breach Notification Rule

As an additional incentive to avoid putting electronic protected health information at risk, and to put those negatively affected on alert, HIPAA provides for a number of rules requiring healthcare organizations to notify different parties in the case of a breach.\textsuperscript{293} These provisions make up HIPAA’s Breach Notification Rule.\textsuperscript{294} The Breach Notification Rule applies to all protected health information, not only electronic protected health information.\textsuperscript{295} Under title 45, section 164.402 of the Code of Federal Regulations, a breach is defined as: “[T]he acquisition, access, use, or disclosure of protected health information in a manner not permitted, . . . which compromises the security or privacy of the protected health information.”\textsuperscript{296} Any impermissible use of protected health information is

\begin{flushleft}
\textsuperscript{287} 45 C.F.R. § 164.310(b)–(c); \textit{Summary of the HIPAA Security Rule}, supra note 260.
\textsuperscript{288} \textit{Summary of the HIPAA Security Rule}, supra note 260; see also 45 C.F.R. § 164.310(d)(i)–(iv).
\textsuperscript{289} 45 C.F.R. § 164.312(a)–(e) (2015); \textit{Summary of the HIPAA Security Rule}, supra note 260.
\textsuperscript{290} 45 C.F.R. § 164.312(b); \textit{Summary of the HIPAA Security Rule}, supra note 260.
\textsuperscript{291} 45 C.F.R. § 164.312(c); \textit{Summary of the HIPAA Security Rule}, supra note 260.
\textsuperscript{292} \textit{Summary of the HIPAA Security Rule}, supra note 260.
\textsuperscript{293} \textit{See} 45 C.F.R. §§ 164.400–414 (2015).
\textsuperscript{295} \textit{See} 45 C.F.R. § 164.400.
\textsuperscript{296} 45 C.F.R. § 164.402.
\end{flushleft}
presumptively a breach requiring notification, unless the covered entity is able to demonstrate that there is a low likelihood the protected health information was actually compromised based on several factors. Not included as a breach under the rule are:

(i) [a]ny unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted [by the rule];
(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted [by the rule]; [and] (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

If a covered entity commits a breach that involves unsecured protected health information, the entity is required to make disclosures to the U.S. Department of Health and Human Services, any individuals who may be affected by the breach, and, depending on the circumstances, to the public through the media. Unsecured protected health information is defined as “protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology [as] specified” by the Department of Health and Human

297. 45 C.F.R. § 164.402(2).

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) [t]he unauthorized person who used the protected health information or to whom the disclosure was made; (3) [w]hether the protected health information was actually acquired or viewed; and (4) [t]he extent to which the risk to the protected health information has been mitigated.

298. 45 C.F.R. § 164.402(1)(i)–(iii).

Covered entities must only disclose to the media if over 500 residents of a certain jurisdiction are affected by an entity’s breach.\textsuperscript{301}

B. \textit{Best Practices for Healthcare Organizations to Avoid Ransomware Attacks}

Of course, never ending up in a situation where one has to negotiate with a ransomware hacker is the most effective means of protecting a healthcare organization's information and resources.\textsuperscript{302} The U.S. government has encouraged that systems administrators and computer users take certain preventive steps to lower the risk of a successful ransomware attack.\textsuperscript{303}

1. Backup—and Then Backup Your Backup

Backing up all electronic data to a secured backup location can prevent a terrible situation from becoming a nightmare.\textsuperscript{304} A healthcare organization with a secured, isolated backup at an isolated location can restore its computer system in approximately four hours.\textsuperscript{305} These backups should be tested and assessed annually to ensure they can deal specifically with a ransomware threat.\textsuperscript{306} Once a computer is infected with ransomware, the virus can move between computers using the same network, which is why it is imperative to store backup data outside of the original network to ensure it also would not be exposed to the virus.\textsuperscript{307} External backups can be stored in a cloud-based system or stored in physical form.\textsuperscript{308}

\begin{itemize}
\item \textsuperscript{300} 45 C.F.R. § 164.402(2)(iv).
\item \textsuperscript{301} 45 C.F.R. § 164.406(a).
\item \textsuperscript{302} See CCIPS WHITE PAPER, supra note 12, at 3, 5.
\item \textsuperscript{303} Id. at 3–4.
\item \textsuperscript{304} See 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
\item \textsuperscript{305} Id.
\item \textsuperscript{306} CCIPS WHITE PAPER, supra note 12, at 4.
\item \textsuperscript{307} DUNBRACK, supra note 19, at 2; CCIPS WHITE PAPER, supra note 12, at 4.
\item \textsuperscript{308} CCIPS WHITE PAPER, supra note 12, at 4. Although, there are variants of the ransomware virus that are capable of infecting backups located on cloud-based storage systems if those systems regularly back up the original system automatically. Id. at 6. This method of automatic back up from a cloud-based system is referred to as \textit{persistent synchronization}. Id. at 4. Healthcare organizations with a persistent synchronization back up network may want to consider utilizing a separate back up network as well. See id.
\end{itemize}
2. Controlling Access to Operating Systems

Perhaps not every healthcare organization staff member requires access to the organization’s shared network to perform their tasks and, therefore, access to the network can be limited based on priority. Administrative access to shared networks should only be granted if necessary and limiting the use of access can reduce the window of opportunity that a ransomware hacker has to infiltrate the network. Access controls can also be used to limit the files a user is able to access, thus controlling the potential danger zones a user can access.

3. Monitoring Inbound and Outbound Emails

Although newer versions of the ransomware virus no longer require an employee to open a dangerous email, the older virus is still being used and other viruses are also dispatched in this manner. Known as phishing emails, these treacherous emails only pose a threat if they are opened by an employee. While training and awareness programs can be effective at reducing the risk of an employee opening these false emails, some hackers are very skilled at making the emails appear authentic and important. Along with a prevention training program, healthcare organizations should take efforts to ensure these emails never reach their employees in the first place. Spam filters can be enabled to detect these malicious emails, and authentication technologies are available to detect emails being sent from unknown locations. System administrators should also monitor inbound and outbound emails for suspicious activity.

---

309. Id.
310. CCIPS WHITE PAPER, supra note 12, at 3–4.
311. Id. at 4.
312. Id. at 3.
313. Id.; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
314. See CCIPS WHITE PAPER, supra note 12, at 3. Hackers have used a virus variant that sends an authentic-appearing email to an employee, listing that employee’s employer as the sender. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5. The unsuspecting employee is more likely to open an urgent, yet spam, email from their boss than they are to open an email from an anonymous or unfamiliar sender. Id.
315. CCIPS WHITE PAPER, supra note 12, at 3.
316. Id. Among these different verification programs are “Sender Policy Framework (“SPF”), Domain Message Authentication Reporting and Conformance (“DMARC”), and DomainKeys Identified Mail (“DKIM”).” Id.
317. Id.
4. Human Error Is the Greatest Risk

Although not all versions of the ransomware virus depend on human action, many versions infect computers by deceiving computer users into clicking links or opening emails. One of the simplest preventive steps a healthcare organization can take to defend itself from ransomware attacks is to inform its personnel of the risk posed by ransomware, common methods by which the virus is used to infect computers; and actions to avoid while using a healthcare server, such as clicking on advertisements, browsing unnecessary websites, or opening emails that seem in any way suspicious. A training and awareness program specific to the threat of ransomware, along with periodic reminders, can go a long way toward preventing an attack.

5. Cyber-Defensive Measures

As mentioned previously, some variants of ransomware are able to breach an organization’s shared network due to vulnerabilities or unpatched areas in the system’s network. The risk of this type of ransomware variant being successful can be mitigated by employing a patch management system to detect and prevent holes in the system’s network. Other more common methods of defending computer systems include setting up firewalls that block unknown IP addresses and ensuring anti-virus and anti-malware settings are set to scan for threats.

6. How HIPAA Helps

If complied with, HIPAA’s numerous provisions can aid a healthcare organization in protecting itself from ransomware and all other cyberattacks. HIPAA’s Security Rule requires organizations covered by the law to implement a risk assessment plan and to actively minimize the cybersecurity risks identified in the plan. The Security Rule also requires covered organizations to train personnel with access to electronic protected health information and to designate a security official in charge of managing

318. DUNBRACK, supra note 19, at 2; CCIPS WHITE PAPER, supra note 12, at 3.
319. CCIPS WHITE PAPER, supra note 12, at 3.
320. Id.
321. DUNBRACK, supra note 19, at 2.
322. CCIPS WHITE PAPER, supra note 12, at 3.
323. Id.
324. See U.S. DEP’T OF HEALTH & HUMAN SERVS., supra note 244, at 4.
access to electronic protected health information. Further, the Security Rule requires covered organizations to impose access controls regarding which employees may access this information.

HIPAA’s Enforcement Rule gives the law teeth by imposing disclosure requirements on organizations which experience certain types of breaches pertaining to their stored protected health information. The Enforcement Rule requires healthcare organizations to disclose breaches of certain magnitudes to the individuals affected, the press, or the government. These penalties encourage healthcare organizations to abide by HIPAA’s Privacy and Security Rule provisions, which can minimize the risk of a ransomware attack in the first place. These disclosure requirements will also help to inform individuals affected by a data breach to enable them to take steps to protect themselves.

7. Dealing with a Ransomware Attack

If a computer or operating system is infected with the ransomware virus, the U.S. Government further suggests the organization take certain steps to deal with the attack. If the virus is detected early enough that it has only infected one or a small number of computers, those computers should be disconnected from the organization’s network to prevent the virus from spreading further. If there are computers that have been infected, but not entirely disabled, these computers should also be disconnected from the network and shut down. If the organization has a backup system, this should be monitored to ensure it has not been infected by the virus, and if the backup is connected to the same network as the original system, the backup should be disconnected from the network. The U.S. Government also recommends that organizations contact the FBI or the Secret Service if they fall victim to a ransomware attack. The organization should then secure as

---

326. See 45 C.F.R. § 164.306(e), .308(a)(2) (2015); Summary of the HIPAA Security Rule, supra note 260.
327. 45 C.F.R. § 164.306(a); Summary of the HIPAA Security Rule, supra note 260.
328. 45 C.F.R. § 164.402 (2015); Breach Notification Rule, supra note 294.
329. 45 C.F.R. § 164.402; Breach Notification Rule, supra note 294.
330. See Breach Notification Rule, supra note 294.
331. See 45 C.F.R. § 164.402; Breach Notification Rule, supra note 294.
332. CCIPS WHITE PAPER, supra note 12, at 4–5.
333. Id.; see also DUNBRACK, supra note 19, at 10.
334. CCIPS WHITE PAPER, supra note 12, at 4; see also DUNBRACK, supra note 19, at 10.
335. CCIPS WHITE PAPER, supra note 12, at 5; see also DUNBRACK, supra note 19, at 11; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
336. CCIPS WHITE PAPER, supra note 12, at 5.
much of its uninfected system as possible and change any passwords associated with the network, if possible. Finally, the U.S. Government does not recommend paying ransoms to ransomware hackers.

8. The Role of Law Enforcement

The U.S. Government recommends that organizations infected with ransomware make contact with law enforcement. Law enforcement, such as the Secret Service or the FBI, may be able to tap into resources able to help the organization, to which the organization—acting alone—would not have access. One such resource would be the international law enforcement community, which can aid in tracking down international hackers or foreign variants of the virus. While notifying law enforcement may seem futile or embarrassing in ransomware cases, law enforcement officials have been successful in several ransomware cases.

Despite these best practices, all organizations face a strong possibility of being attacked successfully by a ransomware hacker. Healthcare organizations, along with each and every one of their users, must be vigilant at all times to prevent these attacks, whereas, a ransomware hacker only has to get lucky once. This state of constant defense does not bode well for healthcare organizations with the result being that sooner or later many organizations will find themselves negotiating with ransomware hackers.

C. Negotiation Solutions to the Ransom Problem: The Ransomware Context

If ransomware hackers are able to infect a healthcare organization’s system with the virus, the organization is faced with two options: (1) pay the

337. Id.
339. CCIPS WHITE PAPER, supra note 12, at 5.
340. Id.
341. Id.
342. Zimmerman, supra note 5, at 16. For example, in mid-2014 the U.S. Department of Justice was able to takedown an entire malware system being used to launch ransomware attacks. Id. This system was known as Gameover ZeuS. Id.
343. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
ransom or (2) do not pay the ransom.\textsuperscript{346} Paying the ransom is the only realistic hope of having the virus removed from the system.\textsuperscript{347} However, paying the ransom with the hope that the virus will be lifted rests on a number of assumptions.\textsuperscript{348} First, if the virus depends on a decryption key to unlock the infected computer, the organization is assuming that if its pays, the hacker will give it the decryption key.\textsuperscript{349} Second, the organization assumes that if it is given the decryption key, it will actually work and remove the virus.\textsuperscript{350} Third, the organization assumes that if the decryption key is provided and effectively removes the virus, that the virus will be removed from all of its systems and not just some of its systems.\textsuperscript{351} Fourth, the organization assumes that the ransomware hacker will not simply hack it again after seeing their efforts rewarded.\textsuperscript{352} On the other hand, refusing to pay the ransom would result in practically zero chance of lifting the virus, which, when dealing with healthcare organizations, can result in lost time, resources, and patient information, all of which can be especially critical in the healthcare context.\textsuperscript{353} However, this may be an acceptable loss if the proper protocols have been adhered to.\textsuperscript{354}

As discussed in the context of piracy above, the various interests of the opposing parties in the ransomware context must also be considered and each outcome predicted when deciding whether or not to pay ransom demands.\textsuperscript{355} The successfully hacked healthcare organization may either pay the ransom or refuse to pay the ransom.\textsuperscript{356} The successful hacker may either release the hostage computer system, along with all of its data, or refuse to release the system, leaving it infected and unusable.\textsuperscript{357} The only win-win situation here occurs where the healthcare organization pays the ransom and the ransomware hacker releases the computer system.\textsuperscript{358} The healthcare organization will regain its ability to function and provide healthcare services
and the ransomware hacker will have realized his or her financial goal. A second resolution arises where the healthcare organization decides to pay the ransom demand, but the ransomware hacker refuses to release the computer system from the virus, despite the payment. This resolution plays out fairly often, unfortunately, since ransomware hackers are not the most honest of criminals, making payment of ransom demands a less-than-appealing option. This is a lose-win situation for the hospital and the hacker, respectively. The next outcome, in which the healthcare organization decides not to pay the ransom demand and the ransomware hacker chooses to release the hostage computer system, is a win-lose outcome favoring the healthcare organization and will almost never occur because the ransomware hacker has already succeeded in attacking the organization’s computer system and, therefore is in a superior bargaining position in which he or she unlikely would act contrary to his or her own interest. The final outcome—in which the healthcare organization chooses not to pay the demanded ransom, and the hacker chooses not to release the hostage computer system—is a lose-lose scenario in which the organization will not recover its lost system functioning, and the hacker will not realize his or her financial goal.

359. See Bento, supra note 1, at 326, 330; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
360. See Bento, supra note 1, at 326, 330; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
361. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5. This was the case where a ransomware hacker successfully infected a Kansas-based hospital with the ransomware virus. Id. The hospital chose to pay the ransom, likely hoping that the first outcome would occur where the hospital regains functioning of its computer systems and the hacker is satisfied with their reward. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; see also Bento, supra note 1, at 326, 330. However, instead of honoring their agreement, upon receiving the ransom sum, the hacker released only part of the hospital’s operating system. 10-Minute Guide to Ransomware Protection, supra note 5. The hacker then demanded further ransom payments to release the rest of the system—a significant portion of the system—from the ransomware virus. Id. Thus, while hoping to achieve the first outcome of the possible resolutions to a ransom negotiation, this negotiation ended up reaching the second outcome, in which the hospital pays the ransom and the ransomware hacker refuses to release the computer system from the virus. See Bento, supra note 1, at 326, 330; 10-Minute Guide to Ransomware Protection, supra note 5. This is a lose-win situation for the hospital and the hacker, respectively. See Bento, supra note 1, at 326, 330; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
Similar to the context of piracy, this outcome-based framework for analyzing ransomware negotiations is insufficient on its own for several reasons. As in the piracy context, each option cannot be given equal weight because the outcome in which the healthcare organization does not pay the ransom, and the ransomware hacker releases the computer system will almost certainly not occur—the outcome in which the healthcare organization pays the ransom and the hacker does not release the parts of, or the entire computer system, is a possibility and has occurred in the past—and the situation where the healthcare organization pays the ransom, and the hacker releases the computer system, is actually not a win at all for the healthcare organization; in fact, it is a serious loss. The healthcare organization will have lost resources for the amount used to pay the hacker for the downtime suffered during the negotiation and—worst of all—for any stolen protected patient information. However, if the healthcare organization has adhered to the best practices for preventing a ransomware attack prior to being attacked, it will have backed up all of its electronic information onto a separate server, safe from the ransomware attack. This action would mitigate the potential damage if the organization chooses not to pay the ransom and does not recover the system controlled by the hacker. A system backup would further allow the organization to recommence operation much faster than would be possible if the organization engages in negotiations with the hacker. This scenario makes the lose-lose outcome more appealing, especially considering that at any point after a ransomware hacker takes control of a computer system, a hacker could steal protected patient data. Thus, under any of the four outcomes, protected patient data could be stolen, resulting in a significant loss for the healthcare organization and its patients.

365. See Bento, supra note 1, at 326, 330; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; supra Section III.E.
366. See Bento, supra note 1, at 326, 330; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; supra Section III.E.
367. Beek, supra note 14.
368. DUNBRACK, supra note 19, at 11; Zimmerman, supra note 5, at 16; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
370. See DUNBRACK, supra note 19, at 11; Zimmerman, supra note 5, at 16; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5. In fact, if the organization engages with and pays a ransomware hacker, the organization may never regain control over its stolen computer system. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
1. Arguments in Favor of Paying Ransoms to Ransomware Hackers

The arguments in favor of paying ransoms to pirates and terrorists are similar to the arguments in favor of paying ransoms to ransomware hackers, including: The possibility of recovering the hostage data and the notion that ransom negotiators should not limit their options by removing the possibility of paying ransoms. However, the digital nature of the hacker ransom demand transaction can allow hackers to back out on their side of the agreement with greater ease than a pirate, or terrorist, who takes people hostage. Where both sides of a ransom negotiation are entirely digital, the possibility of recovering the hostage data decreases substantially.

2. Arguments Opposed to Paying Ransoms to Ransomware Hackers

Once again, the arguments in the contexts of piracy and terrorism are similar to the arguments opposed to paying ransoms to ransomware hackers, including: The idea that ransom payments will only further the ransomware hacking enterprise; the argument that paying a ransomware ransom may expose the organization as vulnerable and willing to pay out, which encourages future ransomware attacks; and the argument that ransomware hackers may simply accept the ransom payment and sell off the ransomed data on the black market. These arguments are compelling in greater part because they have been proven accurate based on ransomware attacks on healthcare organizations in the past. However, imposing an outright ban on healthcare organizations paying ransom payments to ransomware hackers would unnecessarily deprive negotiators of a valuable option in the negotiation. Further, there may be nothing to be gained by depriving healthcare organizations of the right to pay ransom to ransomware hackers because these hackers will have an incentive to use the virus and demand ransom, even if they are fully aware that healthcare organizations are banned from paying them. The hackers still have an incentive to hack the

373. See Bento, supra note 1, at 326, 330; Dubner & Chavers, supra note 126, at 317–19, 327; Weill, supra note 8, at 200, 204–05.
375. See Bento, supra note 1, at 289; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
378. See Gifford, supra note 1, at 60–62; Reynolds, supra note 132, at 612; CCIPS WHITE PAPER, supra note 12, at 5.
organizations to steal their valuable, protected patient data and they still may demand ransom payments, hoping that the organizations will pay regardless of the ban, perhaps in order to make the problem go away quietly.\(^{380}\)

D. **Alternative Solutions to the Ransomware Problem**

Although an outright ban on ransom payments to ransomware hackers may be too restrictive of an option for negotiators, other alternative solutions can be employed to help combat the issue using the legal landscape.\(^{381}\)

1. **A Heightened Terrorist--esque Interest for Ransomware Negotiations**

As mentioned above, the problem of terrorism has been accorded a heightened interest, which is used by many countries to justify an all-out ban on ransom payments to terrorists, as well as enabling several other practices considered too extreme to use in response to other crimes.\(^{382}\) The idea behind this heightened interest is that terrorism is a uniquely difficult problem that cannot be solved using conventional methods alone.\(^{383}\) Whether the threat posed by ransomware necessarily rises to the level where it would warrant an all-out ban on ransom payments need not be answered because of the unique electronic nature of the entire ransomware transaction, and the incentive of ransomware hackers to use the virus in order to steal protected patient data resulting in no beneficial purpose to be gained by an all-out ban on ransom payments.\(^{384}\)

2. **Imposing a Tax on Ransomware Payments to Be Used for Anti-Hacking Efforts**

An alternative method of reducing the incentives of ransom negotiators to pay the ransom—and of hostage takers to take hostages to begin with—is to impose a tax on ransom payments made, with the proceeds being used to combat the ransomware problem.\(^{385}\) This solution has been discussed in the context of piracy ransom negotiations.\(^{386}\) In the ransomware

\[\text{\^{380}}\text{ Zimmerman, supra note 5, at 16; Hagland, supra note 14.}\]
\[\text{\^{381}}\text{ See Gifford, supra note 1, at 60–62; Reynolds, supra note 132, at 612; CCIPS \text{\^{382}}}\text{ White Paper, supra note 12, at 5.}\]
\[\text{\^{383}}\text{ Weill, supra note 8, at 180–81.}\]
\[\text{\^{384}}\text{ Id. at 181.}\]
\[\text{\^{385}}\text{ See Gifford, supra note 1, at 60–62; Reynolds, supra note 132, at 612–13; CCIPS \text{\^{386}}}\text{ White Paper, supra note 12, at 5.}\]
\[\text{\^{385}}\text{ See Bento, supra note 1, at 332.}\]
\[\text{\^{386}}\text{ Id.}\]
context, a federal tax could be imposed on all ransom payments made to ransomware hackers and the proceeds could be used to fund federal efforts to prevent cyberattacks. 387 Such a tax reduces the incentive of healthcare organizations to pay ransoms to ransomware hackers because doing so would result in them having to pay an additional sum on top of the ransom payment. 388 The tax also reduces the incentive of ransomware hackers to demand ransom from these organizations because doing so will indirectly fund government efforts aimed at preventing cyberattacks in the first place. 389 The major shortfall of this alternative approach is that healthcare organizations may become even less likely to report ransomware incidents to avoid the imposed tax. 390

3. Prohibiting Insurance Coverage for Ransomware Attacks

Insurance companies have been offering coverage to companies and individuals facing ransom situations, such as K&R policies in the terrorism context. 391 Noting the rising threat of cyber-hacking in today’s world, many different forms of cyber insurance are now available. 392 Cyber-insurance seeks to cover insured entities for the cost of digital loss and repair following a cyberattack on the insured’s computer network. 393 Healthcare organizations have an incentive to purchase cyber insurance as coverage can aid an organization financially in recovering from a debilitating attack. 394

387. See id. at 332–33.
388. See id. Reducing the incentive of healthcare organizations to pay ransoms to hackers, hoping to ensure that their lost network will be functioning, is an important goal considering how often healthcare organizations pay the ransom demand and the ransomware hackers refuse to restore the organization’s network or make additional ransom demands. See id.; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5. Further, once a healthcare organization pays a ransom demand, it may be seen by other hackers as vulnerable, increasing the likelihood that they will be attacked again. 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
389. Bento, supra note 1, at 332.
390. See Bento, supra note 1, at 332; CCIPS WHITE PAPER, supra note 12, at 5; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
391. Clendenin, supra note 220, at 750.
393. See Bolot & Lelarge, supra note 392, at 270–71; MAJUCA ET AL., supra note 392, at 3; Richards, supra note 392.
394. See Bolot & Lelarge, supra note 392, at 270–71; MAJUCA ET AL., supra note 392, at 2–3; Richards, supra note 392.
However, many organizations choose not to purchase cyber-insurance because, among other reasons, the organizations do not want to disclose that its system has been compromised following an attack, because doing so may expose the organization as vulnerable to future attacks.  

Although some would argue that ransom-based insurance policies promote security, since the occurrence of successful cyberattacks are nearly inevitable, others argue that this type of coverage only lulls covered organizations into a false sense of security and results in the organization failing to implement other appropriate safeguards to prevent ransom situations from arising. The major difference here between the ransomware context and the contexts of terrorism and piracy is that ransomware hackers may obtain something of value from healthcare organizations merely by taking the organization’s system hostage: Protected patient information. Unlike human hostage situations, where the criminals are only successful if their ransom demands are met, ransomware hackers are still successful even if their demands are not met. 

Cyber-insurance can help a healthcare organization regain a functioning network in the face of an attack, but the organization still has every incentive to take other steps to protect its system because cyber-insurance typically does not help the organization with respect to HIPAA claims and other liability due to lost patient data.

4. Requiring Healthcare Organizations to Pass Annual Cyber-Inspections and Employ Cyber-Guards

HIPAA already places several requirements on healthcare organizations pertaining to its electronic protected health information, including a requirement that the organization conduct regular risk analyses on its electronic security measures. This requirement could be expanded to require healthcare organizations to pass an annual cyber-inspection every year.

395. See Richards, supra note 392.
396. See Bolot & Lelarge, supra note 392, at 277; MAJUCA ET AL., supra note 392, at 2–3; Clendenin, supra note 220, at 750–51; Richards, supra note 392.
397. See CCIPS WHITE PAPER, supra note 12, at 8; Zimmerman, supra note 5, at 16.
398. See Weill, supra note 8, at 205–07, 217; Zimmerman, supra note 5, at 16; CCIPS WHITE PAPER, supra note 12, at 8.
399. Bolot & Lelarge, supra note 392, at 270–71; MAJUCA ET AL., supra note 392, at 2–3; Breach Notification Rule, supra note 294; Richards, supra note 392; Summary of HIPAA Security Rule, supra note 260.
400. 45 C.F.R. § 164.306(a)(1) (2015); see also Breach Notification Rule, supra note 294; Summary of HIPAA Security Rule, supra note 260.
Such a requirement would push healthcare organizations to ensure its electronic protected health information is protected to clear inspection.402

Further, an alternative solution raised by some in the piracy context is to require ship-owners to employ guards on their vessels when they know their crew is being sent into pirate-infested waters.403 This solution could be applied to the ransomware context by requiring healthcare organizations to employ electronic data protection experts to conduct regular performance reviews of a healthcare organization’s security measures.404

5. A Process-Structural Approach to Ransomware Ransom Payment Decision-Making

An alternative solution proposed in the terrorism context, as opposed to an outright ban on ransom payments to terrorists, is what is described as a process-structural approach.405 The process-structural approach to ransom payments requires a clear legal standard determining when, and how the decision to pay a ransom demand will be reached.406 The approach requires a distinct group of decision-makers to reach a consensus privately as to whether or not they will agree to the ransom demand.407 Finally, the human and personal factors involved are taken into account, with those who will be affected by the decision being given the opportunity to be heard by the decision-makers.408 The process-structural approach is ideal in the terrorism or even the piracy context because it allows an existing decision-making body, a democratic government, to reach a contemplated consensus while promoting both transparency behind its approach, as well as a private means of reaching a decision.409 Unfortunately, this approach would be inapplicable to the context of ransomware because the approach requires decision-makers to engage in a lengthy process of discussion in order to

401. See 45 C.F.R. § 164.306(b)(1); Breach Notification Rule, supra note 294; Summary of HIPAA Security Rule, supra note 260.
402. See 45 C.F.R. § 164.306(c); Breach Notification Rule, supra note 294; Summary of HIPAA Security Rule, supra note 260.
403. Bento, supra note 1, at 331–32.
404. See 45 C.F.R. § 164.308(a)(2) (2015); Summary of HIPAA Security Rule, supra note 260. HIPAA already requires covered organizations to designate an individual in charge of ensuring the organization complies with HIPAA-required safeguards pertaining to protected patient information. 45 C.F.R. § 164.308(a)(2); Summary of HIPAA Security Rule, supra note 260.
405. Weill, supra note 8, at 217–18.
406. Id. at 218.
407. Id. at 217.
408. Id. at 217–18.
409. Id.
VI. CONCLUSION

The threat of ransomware likely will only increase as the virus is modified to overcome cyber-defenses in the healthcare industry, which seems to continually struggle to keep up with technological advancements. Despite the persistence of ransomware hackers, understanding the preemptive steps healthcare organizations can take to protect their electronic-protected patient information and complying with HIPAA’s other, numerous requirements will ideally protect healthcare organizations from many ransomware attacks. If and when, however, these defenses fail and a hacker is successful at infecting a healthcare system with the ransomware virus, understanding the advantages and disadvantages of various negotiation-based approaches can help the organization manage the crisis as best as possible. Further, there are ways that the legal landscape can be changed to better fight the ransomware problem. Alternative methods such as taxing ransom payments, imposing stricter cyber testing requirements, and requiring inspections by experts in the cyber security field can be helpful legal tools to curb the ransomware problem without depriving negotiators of the option to pay the ransomware hacker’s demands or, at least, allow the hacker to believe the organization may pay his or her demands. These options demonstrate how different approaches, such as the negotiation theory approach, can be utilized to better understand and fight the growing ransomware menace.

410. See Weill, supra note 8, at 217–18; CCIPS WHITE PAPER, supra note 12, at 2.
411. DUNBRACK, supra note 19, at 2; O’GORMAN & MCDONALD, supra note 10, at 10; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5.
412. U.S. DEP’T OF HEALTH & HUMAN SERVS., supra note 244, at 1; see also DUNBRACK, supra note 19, at 2; O’GORMAN & MCDONALD, supra note 10, at 10; 10-Minute Guide to Healthcare Ransomware Protection, supra note 5; Breach Notification Rule, supra note 294; Summary of the HIPAA Security Rule, supra note 260.
413. See CRAVER, supra note 103, at 11–12; PUNNETT, supra note 103, at 412; Gifford, supra note 1, at 46.
414. See 45 C.F.R. § 164.306(a) (2015); Bento, supra note 1, at 332; Breach Notification Rule, supra note 294; Summary of the HIPAA Security Rule, supra note 260.
415. 45 C.F.R. § 164.306(a); Bento, supra note 1, at 332; Breach Notification Rule, supra note 294; Summary of the HIPAA Security Rule, supra note 260.
416. CRAVER, supra note 103, at 11–12; see also PUNNETT, supra note 103, at 412; Gifford, supra note 1, at 46.
PATIENT SAFETY SHOULD INCLUDE PATIENT PRIVACY: THE SHORTCOMINGS OF THE FDA’S RECENT DRAFT GUIDANCE REGARDING CYBERSECURITY OF MEDICAL DEVICES

CHRISTOPHER KERSBERGEN*

I. INTRODUCTION

Right now, a healthcare provider somewhere in the United States is being hacked or suffering the repercussions of a successful hack. Those healthcare providers that have not been attacked successfully likely have an individual attempting to penetrate the healthcare provider’s network. The attacker is targeting the weakest link in the healthcare provider’s network, a connected medical device. The device is a wireless infusion pump that is present in nearly every hospital room and contains a host of cybersecurity vulnerabilities. A successful attack would allow the individual to change the dose of medicine the pump provides and potentially seriously injure or kill the patient, but the attacker only wishes to use the infusion pump to pivot

* Christopher Kersbergen, M.S., J.D., is a Professor of Criminal Justice and the Program Director for the Legal Studies program at Keiser University. He is a United States Army veteran and received his law degree from Nova Southeastern University in 2015.
into the hospital’s network. Once in the network, the attacker can access every device in the hospital and every patient’s health record. The attacker then holds the hospital hostage by launching a ransomware attack. The hospital is crippled by the attack and cannot access vital patient records, nurses’ stations, test results, and monitoring equipment. The attacker holds the hospital hostage for a sum of money, which the hospital is forced to pay. The attack is over, but the repercussions to the hospital and the patients impacted last a lifetime. The hospital is fined millions of dollars for the loss of protected patient health information. The stolen patient information is sold and used.

A victim of the attack is denied a surgery by his or her health insurance carrier because a person used his or her stolen health information to have surgery a continent away. Another victim is billed for healthcare someone else received. Yet another person has private and embarrassing health information posted on the internet. All of the victims suffer in one form or another, many not realizing they have been a victim until it is too late. The frightening realization is that everyone, at one point, has been the victim of a cyberattack on a healthcare provider. The healthcare industry has become virtually dependent on medical devices, and individuals motivated by the enormous profits achievable by attacking medical devices are causing severe concerns for all stakeholders in the healthcare industry.

The regulatory agencies that are responsible for protecting healthcare critical infrastructure from cybersecurity threats have been slow and reactive to the danger. Only within the last couple of years have they made cybersecurity a top priority. The Food and Drug Administration (“FDA”) is the government agency “responsible for . . . [ensuring] that medical devices are [both] safe and effective for use.” The FDA exercises its regulatory authority with regard to cybersecurity of medical devices in the form of

1. Alert: Ransomware and Recent Variants, US-CERT (Mar. 31, 2016), http://www.us-cert.gov/ncas/alerts/TA16-091A. “Ransomware is a type of malware that infects computer systems, restricting user[] access to the . . . system[] . . . [until] a ransom is paid . . . .” Id.
2. TRAPX LABS, TRAPX SEC., INC., ANATOMY OF AN ATTACK: MEDJACK (MEDICAL DEVICE HIJACK) 7–8 (2015).
4. Laura Hagen, Coding for Health: Cybersecurity in Medical Devices, HEALTH LAW., June 2016, at 25, 25–26; see also 21 U.S.C. §§ 351, 360c(f), 360e(a) (2012); 21 C.F.R. § 806.1 (2016).
guidance documents issuing alerts about medical devices and product recalls. In May of 2015, the FDA issued one such alert regarding a vulnerability identified with an infusion system that could allow an unauthorized user to control the device and change the dosage the pump delivers. The alert came ten days after the U.S. Department of Homeland Security (“DHS”) issued warnings on the very same pump. It was the first time the FDA advised healthcare providers to discontinue use of a medical device because of cybersecurity concerns. Both agencies and the manufacturer were aware of the vulnerability for over a year before the advisory was issued. This prompted the increased focus by the FDA and other government agencies on the cybersecurity of medical devices. The increased focus led to the FDA issuing guidance documents for the industry, titled Postmarket Management of Cybersecurity in Medical Devices.

The FDA has largely been reactionary to cybersecurity threats but appears to be moving towards a proactive approach to ensure the safety of medical devices. The guidance documents are a step in the right direction because of their risk-based approach to cybersecurity. The guidance does have flaws, as it falls short on the issue of patient privacy protection, which is neither discussed nor mentioned. The regulatory function of the FDA is 5. Hagen, supra note 4, at 25–26; Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication, U.S. FOOD & DRUG ADMIN. (July 31, 2015), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm; Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication, U.S. FOOD & DRUG ADMIN. (May 13, 2015), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm.


9. See RIOS, supra note 3.


focused primarily on the safety of the devices it regulates, not privacy, and because of that focus, manufacturers are free to ignore many of the issues that are causing the cybersecurity crisis of medical devices.\(^\text{15}\)

This Article restricts the scope of the discussion of the FDA guidance documents to three key recommendations newly introduced, rather than a review of their contents.\(^\text{16}\) The newly introduced recommendations include the introduction for the manufacturer defined essential clinical performance of a medical device, the distinction between controlled and uncontrolled risks, and promotion of membership in Information Sharing and Analysis Organization (“ISAO”) for manufacturers.\(^\text{17}\) Additionally, the guidance documents focus on medical devices that are already in the market and deployed in healthcare organizations.\(^\text{18}\) Therefore, cybersecurity issues related to premarket considerations of a device are outside the scope of this Article. First, this Article addresses why medical devices have become such an attractive target for attackers and the cybersecurity challenges facing manufacturers.\(^\text{19}\) The cybersecurity challenges that are discussed include hard-coded passwords, old and outdated equipment, and the inability for devices to detect or scan for malware infections.\(^\text{20}\) Next, this Article focuses on the newly introduced definitions and recommendations found in the guidance documents.\(^\text{21}\) Finally, this Article points out key shortcomings of the guidance documents, including: the lack of attention to patient privacy due to language that could potentially allow manufacturers to leave known vulnerabilities that do not affect the safety of the device unaddressed, the vague and problematic description of ISAO, and the lack of enforceable rules in the guidance.\(^\text{22}\)

II. CHALLENGES SECURING MEDICAL DEVICES

The use of medical devices that are connected to computer networks has proliferated, as have attacks on medical devices.\(^\text{23}\) Medical devices are now part of the Internet of things, and are exposed to the same cybersecurity

\(^{15}\). *Id.* The Office of the Inspector General is currently examining whether FDA oversight of networked medical devices is sufficient to effectively protect patient health information. OFFICE OF INSPECTOR GEN., *supra* note 10, at 50.

\(^{16}\). See infra Parts II–IV.

\(^{17}\). U.S. FOOD & DRUG ADMIN., *supra* note 11.

\(^{18}\). *Id.*

\(^{19}\). See U.S. FOOD & DRUG ADMIN., *supra* note 11; infra Part II.

\(^{20}\). See infra Sections II.A–C.

\(^{21}\). See U.S. FOOD & DRUG ADMIN., *supra* note 11; infra Part III.

\(^{22}\). See U.S. FOOD & DRUG ADMIN., *supra* note 11; infra Part IV.

\(^{23}\). See U.S. FOOD & DRUG ADMIN., *supra* note 11.
threats to which anything connected to the Internet is exposed.\textsuperscript{24} While networked medical devices facilitate care, they also introduce a host of new cybersecurity risks for patients and for the hospitals that are using the devices.\textsuperscript{25}

Criminals can gain access to devices that contain little or no cybersecurity protection, and, once breached, they are able to access any personal or medical information that is stored on the device or potentially control the device itself.\textsuperscript{26} Healthcare is increasingly targeted by cybercriminals for a relatively simple reason: Crime pays.\textsuperscript{27} Patient health information is worth substantially more money on the black market than is credit card information.\textsuperscript{28} Credit card information can be sold for one or two dollars; patient health information, though, can go for as high as forty dollars per record.\textsuperscript{29} That information can be used to commit insurance fraud, identity theft for financial gain, or a specific targeted attack against an individual.\textsuperscript{30} For example, an attacker can take information obtained from patient health information to disclose embarrassing or private and sensitive information to the victim’s friends and family.\textsuperscript{31} In terms of safety, they could possibly change the coding of a medical device—controlling anything from the amount of medicine that is dispensed, to even changing health data collected by a device.\textsuperscript{32} A doctor could conceivably make wrong decisions based on altered information obtained from a medical device.\textsuperscript{33}

Multiple government agencies have been focusing on the cybersecurity of medical devices in recent years.\textsuperscript{34} Among them, the Federal Bureau of Investigation (“FBI”) investigated healthcare as a high profile risk, releasing a private industry notification, FBI Case No. 140408-009, stating there will be a likely increase in cyber intrusions due to lax cybersecurity

\textsuperscript{25} See U.S. FOOD & DRUG ADMIN., supra note 11; Internet of Things Poses Opportunities for Cyber Crime, supra note 24.
\textsuperscript{26} Internet of Things Poses Opportunities for Cyber Crime, supra note 24; see also U.S. FOOD & DRUG ADMIN., supra note 11.
\textsuperscript{27} See TAP\textsc{X} LABS, supra note 2, at 7–8.
\textsuperscript{28} See id. at 8.
\textsuperscript{30} INST. FOR CRITICAL INFRASTRUCTURE TECH., HACKING HEALTHCARE IT IN 2016: LESSONS THE HEALTHCARE INDUSTRY CAN LEARN FROM THE OPM BREACH 4, 25 (2016).
\textsuperscript{31} See id. at 3–4, 11, 16.
\textsuperscript{32} Id. at 48; see also Hagen, supra note 4, at 25.
\textsuperscript{33} See INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 30, at 48.
\textsuperscript{34} Id. at 2; Hagen, supra note 4, at 25.
standards. Clearly, the main factor driving cyberattacks on connected medical devices is that successful attacks lead to enormous profits. Compounding the problem are reports that the healthcare industry is not prepared to combat even the most basic of cyberattacks. Healthcare organizations and the medical devices they use are low hanging fruit because there are no regulations that require a medical device to meet minimum cybersecurity standards before going to the market. Over two-thirds of healthcare provider organizations have experienced a cyberattack in one form or another over the last few years, with the number of attacks possibly being much higher.

Numerous other factors contribute to the explosion of attempts to attack medical devices, but one of the largest contributors is healthcare organizations converting to electronic health records. It is frightening to consider that medical devices often run the same standard operating systems as copy machines and printers, and connect to the Internet in similar or the same way as laptops and smartphones connect through Wi-Fi or Bluetooth. Unlike many personal devices, medical devices often do not receive updates to protect security, nor are they protected from outside intrusions. Many have hard-coded passwords that can be looked up by anyone with knowledge of the device. A medical device that provides the best example of just how difficult of a challenge securing medical devices can be is an infusion pump. Infusion pumps are generally networked in nearly every hospital

35. Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, FBI CYBER DIV. (Apr. 8, 2014), http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf.
36. Id.; see also INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 30, at 11.
37. Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, supra note 35.
40. Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, supra note 35.
41. INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 30, at 44, 46, 61.
42. Id. at 3, 61.
43. See id. at 36, 70; infra Part II.B.
44. See Hagen, supra note 4, at 25.
room and have been on the market for years. The cell phone in your pocket likely has more cybersecurity protection than an infusion pump, a critically important medical device. Medical devices will never be completely secure from cybersecurity vulnerabilities. However, many of the vulnerabilities that affect medical devices are self-inflicted by design. The devices themselves do not deserve all of the blame, as healthcare organizations often do not consistently report security issues to the FDA reporting program.

A. Hard-Coded Passwords

The majority of infusion pumps have both maintenance usernames, which allow for technical support, and passwords that are hard-coded. In 2013, the DHS issued an alert stating that over 300 medical devices from forty different vendors contained hard-coded passwords that could be exploited in order to change critical settings in the device. A hard-coded password is exactly what it sounds like, a password for the device that is programmed by the manufacturer and cannot be changed. Devices affected included infusion pumps, ventilators, patient monitors, and surgical devices, among many others. The dilemma facing medical device manufacturers that choose hard-coded passwords for their devices is a complicated one to reconcile. A hard-coded password allows manufacturers to troubleshoot

47. U.S. Food & Drug Admin., supra note 11.
53. Alert: Medical Devices Hard-Coded Passwords, supra note 3; see also O’Brien, supra note 50 at 2–3.
any problems with the device remotely because, generally, only the device manufacturer can provide technical support and fixes to a malfunctioning device.\footnote{55}{Healey et al., supra note 52, at 14; see also Inst. for Critical Infrastructure Tech., supra note 30, at 36–37; Alert: Medical Devices Hard-Coded Passwords, supra note 3.}

Hard-coded passwords also allow medical personnel access to the device in case of an emergency.\footnote{56}{Healey et al., supra note 52, at 14; see also Inst. for Critical Infrastructure Tech., supra note 30, at 36–37; Alert: Medical Devices Hard-Coded Passwords, supra note 3.} For example, if a person with an embedded pacemaker collapses while on vacation, a hard-coded password allows medical personnel to quickly render assistance because they can look up the password for the device quickly.\footnote{57}{See Healey et al., supra note 52, at 14.} The downside is that anyone can obtain the password to that device with a little bit of effort and a Google search.\footnote{58}{Inst. for Critical Infrastructure Tech., supra note 30, at 73; Alert: Medical Devices Hard-Coded Passwords, supra note 3.} When medical personnel leave the hospital, there is an inability to revoke the access to the device of the former employee.\footnote{59}{See Healey et al., supra note 52, at 14; Inst. for Critical Infrastructure Tech., supra note 30, at 3–4.} The most distressing issue with hard-coded passwords is that an attacker can breach a device and actively be in a healthcare organization’s network for months without detection.\footnote{60}{See Healey et al., supra note 52, at 14; Inst. for Critical Infrastructure Tech., supra note 30, at 3, 70, 73–74; Alert: Medical Devices Hard-Coded Passwords, supra note 3.} The use of hard-coded passwords may be the easiest cybersecurity challenge to fix for manufacturers in the future, as all that would be needed is to not deploy devices with hard-coded passwords.

B. Outdated Software and Operating Systems

The FDA’s alert regarding the Hospira’s Infusion System shows the challenges of securing medical devices that have been in the market for years from attackers.\footnote{61}{See U.S. Food & Drug Admin., 510(k) No. K042081, Plum A+ Infusion System with Hospira MedNet Software and Plum A+3 Infusion System with Hospira MedNet Software (2004), http://www.accessdata.fda.gov/cdrh_docs/pdf4/K042081.pdf; Alert: Medical Devices Hard-Coded Passwords, supra note 3; Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication, supra note 5; Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication, supra note 5.} The pump was over ten years old at the time of the alert but
still widely in use. It was also in the process of being phased out for a newer model for reasons not related to cybersecurity. It is likely that the pump was using an unsupported operating system that was no longer being updated or patched to address vulnerabilities. The device had a staggering amount of vulnerabilities, the worst of which was that the pump could be accessed remotely and “allow . . . unauthorized user[s] to control the device.” The Hospira Infusion System case appears to be a common issue for medical devices. Many medical devices are “running out of date . . . operating systems such as Windows 2000, Windows XP, or Linux.” These operating systems are patched less often than other connected systems. Many manufacturers believe that changes to a device, including patches to address vulnerabilities, would require them to obtain re-approval from the FDA so they do not update and patch them. The FDA guidance documents actually state that this common misconception, held by manufacturers about patching vulnerabilities, is not the case. Even so, patching or updating a medical device to address vulnerabilities takes time. Time is not a luxury if there is a severely dangerous vulnerability in a medical device, and if a medical device is surgically implanted, patching firmware or software may


64. See id.

65. Id.; see also Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication, supra note 5.

66. See INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 30, at 73; Alert: Medical Devices Hard-Coded Passwords, supra note 3; Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication, supra note 5; Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication, supra note 5.

67. TRAPX LABS, supra note 2, at 10.

68. See id.

69. See HEALEY ET AL., supra note 52, at 14; TRAPX LABS, supra note 2, at 9–10.

70. See TRAPX LABS, supra note 2, at 9; U.S. FOOD & DRUG ADMIN., supra note 11.

71. See TRAPX LABS, supra note 2, at 9.
not be practical or feasible. The fix is to disconnect the device from the network, but this defeats the purpose of having networked medical devices.

C. Lack of Malware Scanning

The most serious cybersecurity threat to medical devices is malware. As stated previously, the motivation for the majority of attacks on medical devices is financial, and the primary way an attacker obtains profitable information is through the deployment of malware. A laptop, home computer, and a cellphone have the option to download a program that scans for malware that may be infecting those devices. Many medical devices come without antivirus or malware protection, basic encryption, or vulnerability lifecycle management. Even if there is malware scanning capabilities in a medical device, medical devices are generally unable to perform these scans because most are in use twenty-four hours a day, 365 days out of the year. They are also closed systems, not open for installation of any third party software that could scan for viruses or malware. If scanning software can be installed, it may void the warranty of the device. This means that unless a device has a malware or virus scanner built in, there would be no way to determine that the medical devices are infected until it is much too late. “Finally, even when sophisticated attacks are detected, it is still very difficult to remove the malware and blunt the attack without the full cooperation of the medical device manufacturer.”

---

72. See HEALEY ET AL., supra note 52, at 14; Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication, supra note 5; Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication, supra note 5.
73. See HEALEY ET AL., supra note 52, at 13; TrapX Labs, supra note 2, at 35; Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication, supra note 5.
74. See HEALEY ET AL., supra note 52, at 12.
75. See TrapX Labs, supra note 2, at 5–6; Alert: Ransomware and Recent Variants, supra note 1.
76. See HEALEY ET AL., supra note 52, at 13–14; TrapX Labs, supra note 2, at 10; Alert: Ransomware and Recent Variants, supra note 1.
77. See TrapX Labs, supra note 2, at 9, 16, 37–38.
78. Id. at 9–10, 35.
79. Id. at 35.
80. See id. at 10–11.
81. See HEALEY ET AL., supra note 52, at 16; TrapX Labs, supra note 2, at 11.
82. TrapX Labs, supra note 2, at 35.
III. FDA POSTMARKET GUIDANCE OVERVIEW

The FDA faces the challenge of promoting safe and secure medical devices while trying not to stifle innovation by issuing restrictive and burdensome regulations. Through the use of guidance documents, the FDA tries to recommend the best possible practices for manufacturers to protect patient safety. The guidance promotes a risk management process for manufacturers to address cybersecurity. It also reiterates that cybersecurity is a shared responsibility among stakeholders. Device manufacturers, vendors, information technology professionals, health information technology developers, and the users of medical devices are the stakeholders responsible for cybersecurity. Stakeholders are numerous and varied, but the FDA only regulates manufacturers of medical devices, which makes cybersecurity even more difficult. That is why the main goal of the FDA’s cybersecurity approach is collaboration between stakeholders, because an effective cybersecurity program is only as good as the weakest link. Often, this weakest link changes depending on the threat. For example, a device that is perfectly secure from outside attackers may still end up being compromised and affect patient safety because the patients themselves tampered with the device, or a hospital employee infects a hospital network because they clicked on a link contained in a suspicious email. What can the FDA do when a user of a medical device does not follow good cybersecurity practices and infects an entire network, putting patient safety at risk? The guidance attempts to achieve this goal of collaboration between stakeholders by issuing recommendations to manufacturers that help mitigate the various threats to medical devices.

83. See id. at 6, 9–10.
84. U.S. FOOD & DRUG ADMIN., supra note 11; see also TRAPX LABS, supra note 2, at 9–10.
85. U.S. FOOD & DRUG ADMIN., supra note 11; TRAPX LABS, supra note 2, at 9–10. “Th[e] [G]uidance applies to: (1) medical devices that contain software, including firmware, or programmable logic, and (2) software that is a medical device.” U.S. FOOD & DRUG ADMIN., supra note 11.
86. U.S. FOOD & DRUG ADMIN., supra note 11.
87. Id.; see also TRAPX LABS, supra note 2, at 35.
88. U.S. FOOD & DRUG ADMIN., supra note 11.
89. See id.; TRAPX LABS, supra note 2, at 12.
90. See TRAPX LABS, supra note 2, at 12.
91. See id. at 9.
92. U.S. FOOD & DRUG ADMIN., supra note 11.
A. **Defining Essential Clinical Performance**

The inability to be completely secure from threats is a common statement made by the FDA, as it has appeared in nearly every cybersecurity related communication released by the agency.\(^{93}\) The FDA introduces the term *essential clinical performance* as a way to compensate for the reality that a device will never be free of vulnerabilities.\(^{94}\) Essential clinical performance is thus used to gauge whether a vulnerability in a device would trigger safety concerns for patients.\(^{95}\) When a vulnerability compromises the essential clinical performance of a device, there is a situation where that vulnerability could result in severe injury or death in a patient.\(^{96}\) In that event, manufacturers would be required to intervene and remedy that vulnerability as soon as possible to prevent those situations from occurring.\(^{97}\) Manufacturers are directed to define the essential clinical performance of their device, the outcomes in terms of severity if compromised, and the level of risk that is acceptable.\(^{98}\) Vulnerabilities that do not have an impact on the essential clinical performance are supposed to be assessed in case those vulnerabilities do impact the essential clinical performance of the device in the future.\(^{99}\) Essentially, the FDA is telling manufacturers to triage cybersecurity of their devices.\(^{100}\)

Manufacturers are recommended to assess the cybersecurity risk to their device by considering the exploitability of the vulnerability and the severity of the health impact to patients if the vulnerability were to be exploited.\(^{101}\) Manufacturers are given latitude in how they assess these two considerations as long as it is industry accepted.\(^{102}\) The FDA does recommend using the Common Vulnerability Scoring System, Version 3.0, to assess exploitability and ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices—Application of Risk Management to Medical Devices to assess severity of the health impact to patients.\(^ {103}\)

\(^ {93} \) Id.

\(^ {94} \) Id.  Essential clinical performance is defined as “performance that is necessary to achieve freedom from unacceptable clinical risk.” Id.

\(^ {95} \) Id.

\(^ {96} \) U.S. FOOD & DRUG ADMIN., *supra* note 11.

\(^ {97} \) Id.

\(^ {98} \) Id.

\(^ {99} \) Id.

\(^ {100} \) Id.

\(^ {101} \) U.S. FOOD & DRUG ADMIN., *supra* note 11.

\(^ {102} \) Id.

\(^ {103} \) Id. “The Common Vulnerability Scoring System (“CVSS”) is an open framework for communicating the characteristics and severity of software vulnerabilities.” FORUM OF INCIDENT RESPONSE & SEC. TEAMS, COMMON VULNERABILITY SCORING SYSTEM
B. **Controlled and Uncontrolled Risks**

The FDA states that manufacturers determine if risks to essential clinical performance are acceptable or unacceptable. Here, the guidance documents again introduce new terms: those that are controlled and uncontrolled. If a risk is acceptable, it is labeled controlled, and unacceptable risks are labeled uncontrolled. Again, acceptable risks do not impact patient safety. Controlled risks do not affect a medical device’s essential clinical performance, meaning that there is no impact on patient safety. Here, the guidance issues its most important statement. Any change made to the medical device to address a controlled risk is considered a device enhancement. This means that a manufacturer deploying a patch or update of the device would not have to report it to the FDA. This is welcomed news, as manufacturers are free to update and patch their devices without worry that their medical devices will need to be reapproved by the FDA because of changes or updates.

An uncontrolled risk contains an unacceptable risk to the essential clinical performance of the device. Patient safety is threatened with the presence of an uncontrolled risk, and control of the medical device could be compromised. Manufacturers are recommended to remedy these risks as quickly as possible, or to at least reduce the risk to an acceptable level. All uncontrolled risks to essential clinical performance are required to be reported to the FDA according to Title 21 of the Code of Federal Regulations part 806. Interestingly, the FDA will not enforce reporting requirements if “[t]here are no known serious adverse events or deaths associated with the vulnerability.” This intent not to enforce the reporting requirements comes with the caveat that “[w]ithin [thirty] days of learning of the

---


105. Id.
106. Id.
107. See id.
108. See id.
110. Id.
113. Id.
114. Id.
115. Id.
116. 21 C.F.R. § 806.1; U.S. FOOD & DRUG ADMIN., *supra* note 11.
vulnerability, the manufacturer identifies and implements device changes . . . or compensating controls to bring the . . . risk to an acceptable level.”

Manufacturers must also notify users and be a participant in an ISAO to avoid reporting requirements. If a manufacturer cannot remedy the uncontrolled risk, the FDA would then consider that there is a reasonable probability that the device will cause serious injury or death, and the device would then “be considered [to be] in violation of the [Federal Food, Drug, and Cosmetic] Act . . . subject[ing it] to enforcement or other action.”

C. Information Sharing and Analysis Organizations

The guidance documents state that the sharing of risk information and intelligence within the medical device community is of critical importance in the adoption of a risk-based approach to cybersecurity, and ISAOs fulfill that critically important role. These ISAOs are intended to serve as focal points for information and collaboration of cybersecurity issues between the private sector and government. The stated purpose of an ISAO is to develop a shared understanding of risks to medical devices so stakeholders can efficiently assess patient health risks. Participation in an ISAO is voluntary for manufacturers; however, the FDA considers participation a critical component of an effective cybersecurity risk management program. The guidance stresses the importance of participation by calling it “a significant step toward assuring the . . . safety and effectiveness of . . . medical devices.” The FDA further incentivizes participation by indicating that it “does not intend to enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act.” Participation in an ISAO and following the other recommendations in the guidance are prerequisites to the FDA using discretion in enforcement of reporting requirements.

ISAOs are intended by the FDA to include groups from any sector, not just healthcare, and participation is inclusive and open to any that wish to join. The FDA states that ISAOs would also allow participating members

118. Id.
119. Id.
120. Id.
121. Id.
122. U.S. Food & Drug Admin., supra note 11.
123. Id.
124. Id.
125. Id.
126. Id.
128. Id.
to receive “[a]ctionable . . . useful, and practical cybersecurity [information] . . . and incident information [through] automated, real-time mechanisms,” although it does not elaborate on how that will be accomplished.\textsuperscript{129} The FDA envisions ISAOs as transparent in terms of providing information to potential members on how the ISAO operates because they are intended to be trusted.\textsuperscript{130} The information shared will be safeguarded to preserve business confidentiality.\textsuperscript{131} “[P]articipants in an ISAO can request that . . . information [provided] be treated as Protected Critical Infrastructure Information.”\textsuperscript{132} This “information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is [also] exempt from regulatory . . . and civil litigation” use.\textsuperscript{133}

IV. SHORTCOMINGS OF THE FDA GUIDANCE

The guidance can essentially be broken down into two components, both of which fall short of addressing the severe cybersecurity challenges facing medical devices.\textsuperscript{134} The FDA recommends that manufacturers adopt risk management programs consistent with, and incorporating elements of, the “[National Institute of Standards and Technology] Framework for Improving Critical Infrastructure Cybersecurity.”\textsuperscript{135} The basic elements of which are “[i]dentify, [p]rotect, [d]etect, [r]espond, and [r]ecover.”\textsuperscript{136} The framework is risk based, designed to manage risk, and intended to complement an organization’s already existing cybersecurity program.\textsuperscript{137} The framework is a good recommendation, however, it should be tailored to fit the healthcare industry, as the framework is not industry specific and is intended to complement existing cybersecurity management programs.\textsuperscript{138} Where the recommendations in the guidance fall short is incorporating the newly introduced “essential clinical performance” and “controlled and uncontrolled risk” into the risk management process.\textsuperscript{139} The second component that is problematic is the pressure to join “information sharing and analysis organizations” without providing any detail on how they will

\begin{itemize}
\item[129.] Id.
\item[130.] Id.
\item[131.] Id.
\item[132.] U.S. FOOD & DRUG ADMIN., supra note 11.
\item[133.] Id.
\item[134.] See id.
\item[135.] Id.
\item[136.] Id.
\item[137.] See U.S. FOOD & DRUG ADMIN., supra note 11.
\item[138.] Id.; see also Hagen, supra note 4, at 34–35.
\item[139.] See U.S. FOOD & DRUG ADMIN., supra note 11.
\end{itemize}
operate, what information will be available, and how information shared will be protected.140

A. Patient Privacy v. Patient Safety

The guidance, as written, fails to address privacy concerns because the distinction between controlled and uncontrolled risk will allow manufacturers to ignore cybersecurity vulnerabilities that impact patient privacy.141 Essential clinical performance is directly tied only to patient safety concerns, implying that any vulnerability that will not result in injury or death could be ignored.142 Manufacturers are free to address any vulnerability that does not impact safety at their leisure.143 The manufacturer could also ignore the vulnerability altogether, since there are usually no consequences for the manufacturer when a healthcare organization has a breach and patient health information is stolen.144 The guidance documents do not address any patient privacy concerns and reinforce a view that privacy is not a cybersecurity priority for the FDA.145 Granted, the FDA’s primary purpose is to ensure medical devices are safe for patients above anything else.146 The focus on safety is understandable, as a device that can seriously injure or even kill a patient is much more harmful than a device that has stolen the personal and financial information of perhaps every patient in a given healthcare organization.147 What is not considered is that the loss of patient privacy can also result in harm to a person’s reputation, economic situation, and mental health.148 Although patient information is covered by laws such as the Health Insurance Portability and Accountability Act (“HIPAA”), manufacturers are not usually subject to that law.149

140. See id.
142. See U.S. FOOD & DRUG ADMIN., supra note 11.
143. See id.; Hagen, supra note 4, at 28.
144. See U.S. FOOD & DRUG ADMIN., supra note 11; Comment Letter from American Association for Justice, supra note 141.
145. See U.S. FOOD & DRUG ADMIN., supra note 11; Comment Letter from American Association for Justice, supra note 141.
146. See OFFICE OF INSPECTOR GEN., supra note 10, at 47.
147. See Hagen, supra note 4, at 26.
148. INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 30, at 8–9.
149. See Hagen, supra note 4, at 30; When May a Covered Health Care Provider Disclose Protected Health Information, Without an Authorization or Business Associate Agreement, to a Medical Device Company Representative?, U.S. DEP’T HEALTH & HUM. SERVS. (Feb. 4, 2004), http://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-
HIPAA regulates either covered entities, which consist of healthcare providers or health plans, and business associates, which can be entities that either “create[], receive[], maintain[], or transmit[] [patient] health information” or perform other services on behalf of a covered entity that involve the disclosure of patient health information. A medical device manufacturer would generally not be considered a covered entity, but a medical device manufacturer is subject to HIPAA if they are business associates of a covered entity. While this means that medical device manufacturers must comply with HIPAA as business associates, manufacturers can avoid business associate classification altogether by ensuring that they merely sell or provide software or equipment to a covered entity and the manufacturer does not have access to the patient health information. Even when there is a situation where patient health information may need to be accessed by the manufacturer, the manufacturer could avoid having to comply with HIPAA by ensuring the health information is not personally identifiable. In these cases, a medical device manufacturer is not subjected to any regulation that protects patient privacy.

The College of Healthcare Information Management Executives (“CHIME”) and the Association for Executives in Healthcare Information Security (“AEHIS”), in their public comment to the FDA’s guidance, proposed a solution for addressing the patient privacy shortcomings of the guidance. They suggested inserting patient safety and patient information subcategories under both controlled and uncontrolled risk. This would ensure that uncontrolled vulnerabilities that do not cause any patient safety issues, and as such do not affect essential clinical performance, are still addressed, and any harm to patients and healthcare organizations is...

---

151. Id. § 160.103(4)(3)(i).
153. Id. at 5574.
154. See id.; When May a Covered Health Care Provider Disclose Protected Health Information, Without an Authorization or Business Associate Agreement, to a Medical Device Company Representative?, supra note 149.
156. Id.; see also U.S. FOOD & DRUG ADMIN., supra note 11.
minimized.\textsuperscript{157} The guidance as it is written now would potentially allow an attacker to access a networked medical device with a controlled vulnerability, and then once inside a healthcare organization’s network, pivot, and potentially access other devices and subsequently impact patient safety by exploiting vulnerabilities in other devices.\textsuperscript{158} Attackers are overwhelmingly focused on, and targeting, patient data.\textsuperscript{159} The disproportionate focus by the FDA on patient safety, when there has not been an event where a patient has been harmed, may send the message to those intent on stealing information that cybersecurity in devices that do have vulnerabilities that impact safety is weak.\textsuperscript{160} The perception of weak security is already driving motivations to attack, and the guidance setting aside privacy concerns could lead to a greater numbers of attacks.\textsuperscript{161}

B. ISAO Poorly Defined and Full of Risk

The guidance suggestion that manufacturers join an ISAO is problematic because the language implies any group or individual can join an ISAO and have access to the information being shared about vulnerabilities.\textsuperscript{162} Indeed, the guidance specifically states that membership is inclusive for anyone and everyone that wishes to join.\textsuperscript{163} The assumption from the language indicates that information shared with the ISAO would be publicly available, meaning good intentioned members will be participants in ISAOs with members that do not have good intentions.\textsuperscript{164} Hackers and other opportunists looking for information on exploitable vulnerabilities will no doubt be members of those very same ISAOs as well.\textsuperscript{165}

In August 2016, MedSec, a startup cybersecurity firm based in Florida, provided an example of just how badly information-sharing of

\begin{footnotesize}
\begin{enumerate}
\item Comment from CHIME & AEHIS, supra note 155; see also U.S. FOOD & DRUG ADMIN., supra note 11.
\item See U.S. FOOD & DRUG ADMIN., supra note 11; HEALEY ET AL., supra note 52, at 11; INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 30, at 10; Hagen, supra note 4, at 25.
\item INST. FOR CRITICAL INFRASTRUCTURE TECH., supra note 30, at 3–4.
\item See id.; Comment from CHIME & AEHIS, supra note 155.
\item See Comment from CHIME & AEHIS, supra note 155; U.S. FOOD & DRUG ADMIN., supra note 11.
\item See U.S. FOOD & DRUG ADMIN., supra note 11.
\item Id.
\item See id.
\item See Clarke, supra note 29; Comment from CHIME & AEHIS, supra note 155.
\end{enumerate}
\end{footnotesize}
cybersecurity vulnerabilities can go. The firm discovered alleged security flaws in pacemakers made by St. Jude Medical, a medical device manufacturer. Rather than offer to sell the information to the manufacturer, or report the information to the FDA like some researchers do, they sold the information to Muddy Waters, an investment research firm. Muddy Waters promptly announced it was shorting St. Jude stock based on the information. Based on the reported vulnerabilities, the FDA and the DHS also announced they were investigating the manufacturer’s device. The fees for MedSec were predicated on how well Muddy Waters’ short position did. If the stock tanked, which it did, the fee would be higher. St. Jude vigorously denied the allegations and cybersecurity researchers have panned the report released by MedSec as flawed. The damage had already been done though. Not only are medical devices exploitable, so too is the information about vulnerabilities affecting those devices.

The guidance documents are silent on any statutory, or regulatory, protections members of ISAOs would receive. While information-sharing is important, the value of information diminishes if it is not actionable, or, if there are large amounts of information. The guidance documents require manufacturers to report all uncontrolled vulnerabilities, even those that do not affect patient safety, possibly flooding ISAOs with information on vulnerabilities, many of them harmless. Worse, some vital information may be excluded based on the different regulatory environments of the varied stakeholders. Whether healthcare delivery organizations could

167. Id.
168. Id.
169. Id.
171. Ou, supra note 166.
173. Ou, supra note 166; Pressman, supra note 172.
174. See Finkle, supra note 170.
175. See U.S. FOOD & DRUG ADMIN., supra note 11.
176. See id.
177. Id.
178. Comment from Rapid7, Comments to FDA’s Draft Guidance for Postmarket Management of Cybersecurity in Medical Devices (Apr. 19, 2016), http://www.rapid7.com/globalassets/_pdfs/rapid7-comments/rapid7-comments-to-fda-draft-
potentially violate a regulation or law, such as HIPAA, by providing information regarding a vulnerability to an ISAO that puts patient information at risk, is a question that should be addressed by the guidance documents.\textsuperscript{179}

Without any detailed criteria about how these organizations work, the governance process, or safeguards of information, it is unlikely that manufacturers would join even though participation is greatly incentivized.\textsuperscript{180} The FDA also includes a red herring regarding the incentive to manufacturers to join an ISAO.\textsuperscript{181} Medical device manufacturers would not be required to report uncontrolled cybersecurity vulnerabilities under Title 21, section 806 of the Code of Federal Regulation if certain requirements are met.\textsuperscript{182} The most important requirement is that there are no known serious adverse events or deaths associated with the vulnerability.\textsuperscript{183} As previously stated, that means the guidance obligates manufacturers to report to an ISAO all uncontrolled vulnerabilities, increasing the burden on manufacturers that right now do not have to report those vulnerabilities.\textsuperscript{184}

C. Recommendations Not Requirements

Obligating manufacturers to report based on what is written in the guidance is a misnomer, as nothing in the guidance requires manufacturers to do anything different than what they are doing now.\textsuperscript{185} The guidance is inadequate because it is not enforceable and does not hold manufacturers “responsible for unsecured or defective [cybersecurity of] medical devices.”\textsuperscript{186} Cybersecurity threats and attacks are getting worse.\textsuperscript{187} Healthcare organizations are being subjected to ransomware attacks,
intrusions that steal patient data from millions of people. An attacker using a pacemaker to kill a patient has gone from being a once clever plot in Hollywood fiction to something that is only a matter of time from happening. The guidance is non-binding on every stakeholder to which it applies. The guidance urges collaboration, risk sharing, and risk management. Lofty outcomes can only be accomplished by making the recommendations in the guidance requirements. Nothing in the guidance places an undue burden on manufacturers of medical devices; it merely calls for cybersecurity risks to be effectively managed through a risk management program. The FDA has been providing guidance to the medical device manufacturer community for nearly two decades related to cybersecurity. Medical devices continue to be delivered to the market with either unsupported operating systems, no software maintenance plans in place, or a host of other vulnerabilities. The FDA must go from making recommendations that manufacturers should follow to making standardized requirements if it wants to seriously protect patient safety and privacy.

V. CONCLUSION

The FDA guidance as discussed is merely a draft. However, based on the generally positive reception by the medical device industry, it is very likely that the draft will be adopted unchanged in the final guidance document. The guidance proposes effective risk management ideas that should already be in use by manufacturers to prevent attackers exploiting cybersecurity vulnerabilities. Attempting to protect, or anticipate and remedy every vulnerability a medical device may have now or in the future is unrealistic. A risk based approach allows manufacturers to adapt to threats that tend to adapt quicker than those tasked with guarding against them. The guidance is a step in the right direction but should be faulted for the lack

188. Id.
189. U.S. FOOD & DRUG ADMIN., supra note 11; see also Comment from Rapid7, supra note 178.
190. U.S. FOOD & DRUG ADMIN., supra note 11.
191. See Comment from Rapid7, supra note 178.
192. See U.S. FOOD & DRUG ADMIN., supra note 11.
193. See id.; Comment from Rapid7, supra note 178.
194. See Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication, supra note 5; supra Section II.B.
195. See Comment from Rapid7, supra note 178.
196. U.S. FOOD & DRUG ADMIN., supra note 11.
197. See Comment Letter from American Association for Justice, supra note 141; Comment from Fresenius Kabi, supra note 180; Comment from Rapid7, supra note 178.
198. See supra Section IV.A.
199. See supra Section IV.
of privacy considerations.\textsuperscript{200} Patient health should be a priority alongside patient safety.\textsuperscript{201} Essential clinical performance should include patient privacy.\textsuperscript{202} Furthermore, the guidance suggests that ISAOs are critical to effective medical device cybersecurity, yet spends very little time fleshing out their vision on how exactly they will work and reassuring manufacturers that information about cybersecurity vulnerabilities will not be exploited by opportunists.\textsuperscript{203} Finally, recommendations should turn into requirements.\textsuperscript{204} Nothing in the guidance as proposed places an undue burden on manufacturers, nor does it stifle innovation.\textsuperscript{205} The FDA has a track record of issuing guidance that is ignored by those towards whom the recommendations are directed.\textsuperscript{206}

\begin{flushright}
\textsuperscript{200} See supra Section IV.A.
\textsuperscript{201} See supra Section IV.A.
\textsuperscript{202} See supra Section IV.A.
\textsuperscript{203} See supra Section IV.B.
\textsuperscript{204} See supra Section IV.C.
\textsuperscript{205} See U.S. FOOD \& DRUG ADMIN., \emph{supra} note 11; \emph{supra} Section IV.C.
\textsuperscript{206} See Comment Letter from American Association for Justice, \emph{supra} note 141.
\end{flushright}
CARDIAC DEFIBRILLATORS NEED TO HAVE A BULLETPROOF VEST: THE NATIONAL SECURITY RISK POSED BY THE LACK OF CYBERSECURITY IN IMPLANTABLE MEDICAL DEVICES

MICHAEL WOODS*

I. INTRODUCTION ........................................................................................................... 419
II. UNDERSTANDING HACKING IMPLANTABLE MEDICAL DEVICES ... 421
   A. The Lack of Cybersecurity: A Problem with the Industry ............................................. 422
   B. The Digital Vulnerabilities of Implantable Medical Devices ........................................... 424
   C. National Security Risk .................................................................................................. 427
III. CURRENT STATE OF GOVERNMENTAL AFFAIRS .............................................. 429
   A. The Power of the FDA ................................................................................................. 429
   B. Governmental Reclassifications, Power Shifts, and Executive Orders ......................... 434
IV. PROPOSED SOLUTIONS .............................................................................................. 438
   A. Governmental Solutions .............................................................................................. 439
   B. Other Solutions ........................................................................................................... 441
   C. Dangers with Governmental Regulation ........................................................................ 444
V. CONCLUSION ................................................................................................................. 446

I. INTRODUCTION

Imagine a world where a patient wearing a pacemaker or an insulin pump, just fine moments before, drops dead after his implanted medical device turns seemingly against him. 1 Worse yet, imagine that an insulin

* Michael Woods received his J.D. from Nova Southeastern University, Shepard Broad College of Law, and his LL.M. in National Security & U.S. Foreign Relations from the George Washington University Law School. He is grateful for his family and friends for their love and support throughout law school. Michael would like to thank Professors Kathy Cerminara, James Levy, Michael Richmond, and Randolph Braccialarghe for being a great influence on his legal education.
pump is giving false readings and a user relying on the readings injects too much insulin, thus being the instrument in his or her own demise. These examples can be the work of malicious actors who hack into implanted medical devices, which has been possible for years. The federal government has done little to regulate any type of cybersecurity on implantable medical devices, despite knowing that hacking these devices has been possible for almost a decade. The number of patients with implanted medical devices is not miniscule either; millions of people in the United States already have implanted medical devices, and roughly 300,000 new people are getting them each year. The implantable medical device “market is projected to be around [seventeen] [b]illion dollars by 2019,” resulting in a large population of patients with this technology in them and little to no cybersecurity attached to those devices, which is a huge security risk. Considering that “[t]he U[nited] S[tates] Department of Homeland Security has identified the . . . Public Health sector as . . . [a] critical cyber security infrastructure[]” to the United States, this lack of cybersecurity is a huge national security risk.

This Article analyzes the vulnerabilities of implantable medical devices, such as pacemakers/defibrillators and insulin pumps, to hacking by malicious actors and the national security risk that those vulnerabilities pose. Part II will explain the lack of cybersecurity of implantable medical devices, such as cardiac defibrillators and insulin pumps, and the vulnerabilities of implantable medical devices to cyberattacks that will harm
the patient. It will then emphasize how this is a national security risk by providing instances of lack of cybersecurity causing harm in the United States and abroad, which includes the research conducted in hacking implantable medical devices. Part III will analyze the current governmental legislation and regulations on implantable medical devices and how the government fails to address cybersecurity due to conflicting laws within agencies and branches of government. Part IV delves into possible solutions for this national security risk by proposing possible governmental regulations, as well as other private sector-led solutions. It will then conclude by stressing the dangers that poor regulations and laws can cause by failing to address the cybersecurity risks to the medical device industry.

II. UNDERSTANDING HACKING IMPLANTABLE MEDICAL DEVICES

Manufacturers focus, first and foremost, on functionality of implantable medical devices, and almost all manufacturers skip any type of cybersecurity due to a multitude of reasons. As devices are increasingly interconnected with the Internet and wireless functionalities, the lack of cybersecurity poses a huge security risk to patients wearing implantable medical devices from malicious actors. Part A discusses manufacturer concerns about adding cybersecurity to implantable medical devices, and explains how the Food and Drug Administration (“FDA”) echoes these fears. It also highlights the lack of focus the healthcare industry has overall in tackling cybersecurity issues. Part B examines the many ways hackers can take over and manipulate implantable medical devices. Part C provides examples of cyberattacks on medical devices across the United States and overseas, and how preventative measures, such as anti-virus software, contribute to the harm. Part C concludes by discussing laboratory simulations and public demonstrations of hacking implantable medical devices.

9. See infra Part II.
10. See infra Section II.C.
11. See infra Part III.
12. See infra Part IV.
13. See infra Parts IV–V.
14. Ransford et al., supra note 2, at 170.
16. See infra Section II.A.
17. See infra Section II.A.
18. See infra Section II.B.
19. See infra Section II.C.
devices and demonstrating the clear and present threat the lack of cybersecurity has on these devices.  

A. The Lack of Cybersecurity: A Problem with the Industry

Implantable medical devices are, first and foremost, designed to provide enormous health benefits to patients. These devices, such as insulin pumps and cardiac defibrillators, all feature wireless communication to monitor and treat patients through personalized care and send reports to their physicians. They also are updated remotely with the latest firmware, all for the benefit of the patient. As manufacturers keep improving quality of care and technology by making the devices lighter, smaller, and faster, they tend to ignore cybersecurity for the devices.

Implantable medical devices do not have cybersecurity built into them when they are made. This is due to a myriad of reasons: The “limitations in computing power or memory space” from having such a small device that is “[un]able to run traditional [anti-virus] software without impacting [the device’s] performance;” fear of creating “a critical, life-threatening situation if the system responds to a false positive if there is anti-virus software in the medical device;” standard security software is difficult to use with the limited memory in a customized/scaled back version of the operating system in the device; authentication security measures on the devices risk patient safety in cases of an emergency when a medical professional may need to disable or alter the device to treat a patient; and

---

20. See infra Section II.C.
23. Id.
25. Finkle, supra note 24.
27. Id.
28. Id. at 28.

http://nsuworks.nova.edu/nlr/vol41/iss3/1
heavy encryption for security of the device may drain enough energy that it 
would require frequent device replacement, which would require surgery, 
resulting in burdening both the patient and the medical profession.30 The 
FDA has echoed these fears of “medical device security measures doing 
more harm than good in emergency situations.”31 Implantable medical 
devices are meant to improve patients’ lives, and thus, manufacturers and 
designers have apportioned this above all else to cybersecurity.32 
The healthcare industry is estimated to be “‘five to seven years 
behind’ other industries in . . . cybersecurity.”33 This is because the 
healthcare industry is very diverse and fragmented compared to other 
industries, such as the energy industry.34 Traditionally, “[t]he medical device 
industry has . . . ignored warnings that its products [are not] protected against 
[a] cyberattack.”35 If there is any type of security protection put into devices 
by manufacturers, it tends to focus on data theft, not device manipulation by 
malicious actors.36 Also, compared to other industries that spend 12% of 
their information technology (“IT”) security budget on data protection alone, 
a majority of healthcare organizations spend less than 3% of their IT security 
budgets on it.37 With the percentage of healthcare organizations that have 
reported being hacked rising from 20% in 2009 to 40% in 2013, the medical 
industry’s dismal security budget focus and funding, compared to industry 
standards of preventative IT security budget, could be considered negligent.38 
 “[Ninety-four percent] of [all] healthcare institutions [have] reported . . . 
be[ing] victims of cyberattacks.”39 

Lastly, there is not an effective national reporting system for 
cybersecurity related failures that play a significant role in patient injuries or

30. See Burleson & Carrara, supra note 21, at 4. 
32. Ransford et al., supra note 2, at 170. 
33. Alex Ruoff, Security Exec: Medical Device Industry at Least Five Years 
Behind on Cybersecurity, 6 BNA HEALTH L. REP. 17, 17 (2014). 
34. Daniel J. Barnett et al., Cyber Security Threats to Public Health, 5 WORLD 
MED. & HEALTH POL’Y 37, 38 (2013). 
35. Ruoff, supra note 33, at 17. 
36. Id. 
37. Alex Ruoff, Hacking Incidents on the Rise, But IT Security Budgets 
38. See Caroline Humer & Jim Finkle, Your Medical Record Is Worth More to 
Hackers Than Your Credit Card, REUTERS (Sept. 24, 2014, 2:24 PM), 
http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21120140924; Ruoff, 
supra note 37, at 20. 
deaths. “Approximately 1.2 million adverse events of medical devices were reported to the FDA’s Manufacturer and User Facility Device Experience . . . database” between 2006 and 2011, but there is no information on those cybersecurity related failures, as cybersecurity problems are not included in the reporting system. Out of the 1.2 million, 23% were listed only as computer-related failures, 94% of which "presented medium to high risk” of harm to the patient.

Similarly, the FDA’s Manufacturer and User Facility Device Experience “database is qualitative rather than quantitative,” and it does not concern itself with security events. For example, if a clinician is using a device that is slower because of a malware infection, it would most likely not be reported. This is because admitting a role in infecting a medical device or a network, such as inserting an infected flash drive in a computer or connecting an infected phone to the network, would lead to disciplinary action. Therefore, the actual number of what is reported is most likely low because of employees not realizing an issue or fearing retribution.

B. The Digital Vulnerabilities of Implantable Medical Devices

Current implantable medical devices can be hacked into and taken over, overloaded with malware to slow them down, turned off completely, and overloaded to kill the host at the behest of a malicious actor or actors, and all harming the host of the device. For instance, a Medtronic pacemaker does not need a password to access the device and the wireless communication is not encrypted, which makes it easy for a hacker to collect data from the device, reverse engineer the protocol, and take over the device. Public information, such as any implantable medical device user’s manual and the specifications for the device’s radio chip, make the reverse engineering and finding of the remote control personal identification number

41. Id. at 35.
42. Id. at 35–36.
43. Id. at 35.
44. Id. at 36.
45. Fu & Blum, supra note 40, at 36.
46. Id.
47. See id.
49. Id.
to control the device relatively simple.\textsuperscript{50} Once this is done with readily available information, the hacker can generate misleading information, such as false readings on an insulin pump or just cause it to inject “insulin into the patient’s body.”\textsuperscript{51} Implantable medical devices are exposed to common cyber threats that normal computers experience because the operating system, central processing unit, and other software components are generally \textit{off-the-shelf} components.\textsuperscript{52} Medical devices still tend to rely on the original versions of their operating system—such as Windows XP—even long after support for the operating system has ended.\textsuperscript{53} Hackers can also take control of the device as long as it is around any sort of wireless Internet, and the strength of the transmission and radio frequency of the implantable medical device does not matter.\textsuperscript{54} This is possible because Federal Communications Commission regulations make it so that implanted medical devices have a certain radio frequency range, as implantable medical devices “[d]o not normally initiate communication [and only] transmit [as a] response to a transmission from [another party] or if [they] detect[] a life-threatening condition.”\textsuperscript{55} No matter what the implantable medical device is, once it is connected to a network, it is essentially a node on the network that can be seen, interacted with, and controlled.\textsuperscript{56} As these devices are increasingly using wireless communications among components to improve health and reporting, hackers have a larger avenue for control of a system.\textsuperscript{57}

Unfortunately, the implanted medical devices already in patients cannot just have cybersecurity protocols and software patched into them to resolve this gaping security hole.\textsuperscript{58} The medical device industry in the United States is tightly regulated by the FDA, which requires that the

\begin{footnotesize}
\begin{itemize}
\item[50.] Ransford et al., \textit{supra} note 2, at 176.
\item[51.] Id.
\item[52.] Wirth, \textit{supra} note 26, at 27.
\item[53.] Fu & Blum, \textit{supra} note 40, at 36. In 2012, it was reported to the National Institute of Standards and Technology ("NIST") Information Security and Privacy Advisory Board that the Beth Israel Deaconess Medical Center in Boston was still using medical devices that were using the original versions of Windows 95 and Windows XP, despite the support for these ending in 2006 and 2010 respectively. \textit{Id.} These devices were not even the final patch of these versions, and were never upgraded to include any of the patches that came out to these operating systems over the years. \textit{Id.} This shows that, even if patching does occur to devices, hospitals and medical professionals need to apply them in order to be effective. \textit{See id.}
\item[54.] \textit{See} Gollakota et al., \textit{supra} note 5, at 3–4.
\item[55.] Id.
\item[57.] Ransford et al., \textit{supra} note 2, at 176.
\end{itemize}
\end{footnotesize}
cybersecurity for any medical device and its upgrades be applied by the manufacturer and not any person in the stream of commerce for the device.\textsuperscript{59} Therefore, a hospital cannot upgrade or add any type of cybersecurity to any medical device without the manufacturer approving the upgrade.\textsuperscript{60} In compliance with the FDA review process, a manufacturer needs to test the proposed patch on the device, making sure the changes to the operating system do not impact the behavior and functionality of the device.\textsuperscript{61} That means that medical devices from a patch level are often “months, if not years, behind where the operating system manufacturer is,” leading to a security gap that cannot be remedied swiftly.\textsuperscript{62} When patches are approved and finally applied, “they may require complex installation procedures and acceptance testing” which may result in the patch not actually being applied.\textsuperscript{63} Unlike in computers and other software, full automatic distribution and application of upgrades are difficult to implement in implantable medical devices because of the associated upgrade timing and the system reboot endangering the patient; if there were an issue, the patient would be vulnerable.\textsuperscript{64} Implantable medical devices can last up to ten years, leaving the patients vulnerable to attack for a long time.\textsuperscript{65}

The issue of patching and updating medical devices is not new, as it has been widely recognized by the FDA as being an issue.\textsuperscript{66} The Department of Homeland Security has also recognized this issue; for example, it reported that the Conficker virus has not only been known to have infected pacemakers through wireless and other connections but, also, cannot be removed because removal of the virus would be considered a “modification to the certified software” under governmental regulations.\textsuperscript{67}

Implantable medical devices can also be infected with viruses or targeted malware from networked devices.\textsuperscript{68} Any type of medical equipment that is infected with a virus or malware and is connected to a network will spread it to the implanted medical device.\textsuperscript{69} This can either give a hacker control—if that is the target—or the ability to disable or slow down the device.\textsuperscript{70} Many hospitals tend to get medical technology—devices and

\begin{itemize}
  \item 59. Wirth, \textit{supra} note 26, at 27.
  \item 60. \textit{Id}.
  \item 61. Vockley, \textit{supra} note 58, at 167.
  \item 62. \textit{Id}.
  \item 63. Wirth, \textit{supra} note 26, at 28.
  \item 64. \textit{See id.} at 32.
  \item 65. Gollakota et al., \textit{supra} note 5, at 2.
  \item 66. Wirth, \textit{supra} note 26, at 28.
  \item 67. Templeton, \textit{supra} note 48, at § 2.2.
  \item 68. Vockley, \textit{supra} note 58, at 167.
  \item 69. \textit{Id}.
  \item 70. \textit{See} Ransford et al., \textit{supra} note 2, at 161; Vockley, \textit{supra} note 58, at 167.
\end{itemize}
equipment—from a single vendor, and vendors tend to keep all of their “equipment on the same patch or configuration level,” which makes the spread of the virus or malware very easy.\textsuperscript{71} Even if a hospital purchased medical technology and devices from multiple vendors, having different devices from different manufacturers, each with its own structure and potential levels of security, would create an insecure tangled digital web of cybersecurity.\textsuperscript{72} Targeted malware can move between different devices and systems passively until it reaches the implantable medical device where it is designed to activate.\textsuperscript{73} Due to the fact that implantable “medical devices such as pacemakers [each] have [a] unique identifier[,]” it is possible to target a specific individual or class of people.\textsuperscript{74} This \textit{Internet of things} that connects physical equipment all together on a network via computers has created many different avenues for cyberattacks.\textsuperscript{75}

C. \textit{National Security Risk}

Concerns about the varying lapses in cybersecurity in implantable medical devices and medical devices on the same network have merit.\textsuperscript{76} “Between . . . 2009 and . . . 2011, the [Department of Veterans’ Affairs] detected 142 . . . instances of malware infections affecting 207 medical devices found in [fourteen different parts of hospitals].”\textsuperscript{77} In one instance, in the catheterization lab, the malware infection of equipment was so severe that it “required transport of [the] patients to a different hospital.”\textsuperscript{78} In 2010, a Veterans’ Affairs catheterization laboratory in New Jersey was closed due to malware that infected hundreds of medical devices and computers on that network.\textsuperscript{79} “[T]he Conficker worm [caused] . . . approximately 10[\%] of the [healthcare] IT infrastructure in Sweden” to go dark in 2010.\textsuperscript{80} That same year, the same worm took “15[\%] of New Zealand’s [total healthcare] system . . . offline.”\textsuperscript{81} These kinds of viruses that can take over computers

\begin{singlespace}
\begin{footnotes}
\item[71.] Vockley, supra note 58, at 167.
\item[72.] \textit{Id}.
\item[73.] Templeton, supra note 48, at § 2.2.
\item[74.] \textit{Id}.
\item[75.] Perakslis, supra note 39, at 396.
\item[76.] See Mankovich, supra note 7, at 174; Fu & Blum, supra note 40, at 36; Daniel B. Kramer et al., \textit{Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance}, PLOS ONE, July 19, 2012, at 1, 4.
\item[77.] Kramer et al., supra note 76, at 4.
\item[78.] \textit{Id}.
\item[79.] See Fu & Blum, supra note 40, at 36.
\item[80.] Mankovich, supra note 7, at 174.
\item[81.] \textit{Id}.
\end{footnotes}
\end{singlespace}
and devices are not bound by country borders and infect anything that links into the network.\textsuperscript{82}  

In addition, there is a real danger of implementing already existing safety measures, such as anti-virus software, in implantable medical devices.\textsuperscript{83}  “On April 21, 2010, one-third of the hospitals in Rhode Island were forced to” stop elective surgeries and treatment of non-trauma patients in the emergency room because the “anti-virus software update had . . . misclassified a critical Windows [dynamic link library] as malicious.”\textsuperscript{84}  Another example occurred when a “tornado hit St. John’s hospital in Kansas City in May 2011.”\textsuperscript{85}  The tornado “caus[ed] the electricity to go out, [and as a result] doctors and nurses lost access to . . . vital medicine[] in the [emergency room] and in [almost] every other department,” because the drugs were in a powered metal cabinet which had an automatic lock controlled by software.\textsuperscript{86}  

“Researchers at [the] Massachusetts Institute of Technology and the University of Massachusetts, Amherst, . . . have demonstrated [in a laboratory] that it is possible to hack into wireless implantable medical devices,” including pacemakers, heart defibrillators, insulin pumps, and even cochlear implants and neurostimulators, and take control of them to the detriment of patients.\textsuperscript{87}  Even a programmable radio could control an implantable defibrillator or an insulin pump by replaying messages, allowing the operator of the radio to stop the device or to cause it to kill the host.\textsuperscript{88}  Researcher Jerome Radcliffe inspected the Java-based configuration program in his own insulin pump and was able to “reverse-engineer[] the pump’s packet structure, revealing that [it did not] encrypt the medical data . . . or . . . authenticate [when] the components [of the insulin pump communicated] to one another.”\textsuperscript{89}  A researcher with Radcliffe also demonstrated his ability to take over and shut down a volunteer’s insulin pump, showing how easy and swiftly it could be done.\textsuperscript{90}  To further the point, a group of researchers demonstrated how “analog signal injection of low-frequency waveforms . . . on the sensing leads of” an implantable defibrillator could be tricked by crafting electromagnetic interference waveforms to deliver a defibrillation shock.\textsuperscript{91}  This means that even an attacker who cannot perfectly match an

\begin{itemize}
  \item \textsuperscript{82} See id. at 174–75.
  \item \textsuperscript{83} See Fu & Blum, supra note 40, at 36.
  \item \textsuperscript{84} Id.
  \item \textsuperscript{85} Klein & Kagan, supra note 29, at 2.
  \item \textsuperscript{86} Id.
  \item \textsuperscript{87} Vockley, supra note 58, at 170.
  \item \textsuperscript{88} Ransford et al., supra note 2, at 161.
  \item \textsuperscript{89} Id.
  \item \textsuperscript{90} Id. at 164.
  \item \textsuperscript{91} Id. at 166.
\end{itemize}
electromagnetic interference signal’s wavelength to the length of the sensing leads could just increase the power to override and trigger the implantable medical device.92 Researchers have not only been able to do something once thought of as science fiction in a laboratory, but they have also been able to do it in the course of a live demonstration.93

III. CURRENT STATE OF GOVERNMENTAL AFFAIRS

The FDA’s mission is to protect “the public health by assuring the safety, efficacy, and security of medical devices.”94 The FDA regulates medical devices and approves them, but its authority is in flux regarding regulation of cybersecurity.95 Part A of this Section delves into the FDA and its numerous attempts to tackle cybersecurity of implantable medical devices through voluntary guidance, regulations, and proposed regulations.96 Part B examines various congressional attempts to tackle cybersecurity of implantable medical devices, along with other governmental bodies such as the Federal Trade Commission (“FTC”), the Department of Homeland Security, the Department of Defense, and the White House.97 This Section highlights the contradictory nature of all of the various governmental bodies’ solutions to the important issue of cybersecurity in implantable medical devices.98

A. The Power of the FDA

The FDA classifies a device as an “instrument, . . . machine, . . . implant, . . . or other similar . . . article, including any component, part, or accessory, which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals.”99 The FDA subjects all of these to the same laws and standards, with a definition that is vague enough that even a smartphone becomes a medical device when employing a cell phone camera to determine urine analytes.100 “The FDA considers [most] [h]ealth IT products to be ‘similar or related to’ other medical device products,” which results in the

92. See id.
93. Ransford et al., supra note 2, at 164.
94. Fu & Blum, supra note 40, at 36.
95. See Vockley, supra note 58, at 166–67.
96. See infra Section III.A.
97. See infra Section III.B.
98. See infra Section III.B.
100. See U.S. FOOD & DRUG ADMIN., LETTER TO BIOSENSE TECHNOLOGIES PRIVATE LIMITED CONCERNING THE uCHECK URINE ANALYZER (2013).
FDA classifications referring back to themselves in defining medical devices and standards.  

The FDA has released numerous guidance documents on cybersecurity throughout the years, all echoing each other with no actual effect on implantable medical devices.  

“In 2005, the [FDA] issued [a] ‘Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software,’” which stated that it was “the responsibility of medical device manufacturers to maintain cybersecurity” and to keep them safe and effective through maintenance plans for its cybersecurity.  

“On September 25, 2013, the FDA [released the] Mobile Medical Applications Guidance . . . (“MMA Guidance”),” which declared that it “intend[ed] to regulate software that poses significant risks to patients . . .”. The MMA Guidance also explained that devices classified as “[mobile medical applications] must have premarket approval or clearance [from the FDA] before commercialization may begin.” The MMA Guidance also defined “[a] manufacturer as [being] anyone who ‘creates, designs, develops, labels, re-labels, . . . modifies, or creates a software system or application for a regulated medical device in whole or from multiple software components,’” This software classification sweeps in all types of medical devices, including smartphones, although Congress has stated that the FDA does not have authority to do so.  

To further complicate things, in February 2011, the FDA reclassified its Medical Device Data Systems (“MDDS”) rule from a Class III, highest risk, to a Class I, lowest risk classification. This MDDS rule defines MDDS as devices intended to transfer, store, and convert from one format to another or display medical device data. Implantable medical devices fall

102. See Mankovich, supra note 7, at 175; Kupchyk, supra note 101, at 2–3.
103. Mankovich, supra note 7, at 175; see also U.S. FOOD & DRUG ADMIN., CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE: GUIDANCE FOR INDUSTRY (2005).
105. Kupchyk, supra note 101, at 2; see also U.S. FOOD & DRUG ADMIN., supra note 104.
106. Kupchyk, supra note 101, at 3; see also U.S. FOOD & DRUG ADMIN., supra note 104.
107. See Kupchyk, supra note 101, at 5.
108. See 21 C.F.R. § 880.6310(b) (2016); U.S. FOOD & DRUG ADMIN., supra note 104.
109. 21 C.F.R. § 880.6310(a)(1)(i)–(iv).
within this classification. Under the new MDDS rule classification, the FDA does not consider “software that is critical to keeping a patient alive, such as blood pressure cuffs and glucose monitors, to be [a] MDDS product.” The FDA determined that the new classification to lowest risk is because these products pose the lowest risk to the patient, and the controls of the devices “would provide . . . reasonable assurance of safety and effectiveness.” Under this new classification, which incorporates implantable medical devices, “[m]anufacturers are only required to comply with the registration and listing requirements, the Medical Device Reporting regulation . . . and the Quality System Regulation” of the FDA.

The FDA has numerous proposals in the works as well. First, the “FDA has proposed to expand the types of . . . device[s] . . . [under the MDDS Rule] that would be exempt from FDA enforcement.” The FDA also plans “to revise its [MMA Guidance] to conform [to] the MDDS expansion and clarify the types of mobile medical [applications] that would be exempt from FDA enforcement as a medical device.” “The FDA [also] has proposed not to enforce compliance with any regulatory controls that apply to the MDDS;” “medical image storage device[s], [which provide] electronic storage and retrieval functions for medical images;” and “medical image communication device[s], [which are] device[s] that provide electronic transfer of medical image data between medical devices,” “based on a determination that these devices pose low risk to patient safety.” The language of the proposal, however, is vague enough to incorporate implantable medical devices such as insulin pumps. Lastly, the FDA published the Health Information Technology ("HIT") Report at the request of Congress in April 2014, in accordance with the Food and Drug Administration Safety and Innovation Act ("FDASIA"), which proposed another strategy based on classifying healthcare intellectual technology products. The recommended categories were administrative products, health management products, and medical devices. This report led to

110. See id.; Gupta, supra note 22.
111. Kupchyk, supra note 101, at 3.
112. Id.
113. Id.
114. See id.
115. Id.
116. Kupchyk, supra note 101, at 3; see also U.S. FOOD & DRUG ADMIN., supra note 104.
117. Kupchyk, supra note 101, at 4; see also U.S. FOOD & DRUG ADMIN., supra note 104.
118. See U.S. FOOD & DRUG ADMIN., supra note 104.
120. Id. at 4.
proposed legislation based on a function-based framework when evaluating applications and products, and it does not address medical software or have any binding authority.121

The FDA came out with a new series of nonbinding recommendations in October 2014, after an investigation by the Department of Homeland Security into the cybersecurity of implantable medical devices was made public.122 This new guidance began by recognizing “[t]he need for effective cybersecurity to assure medical device functionality and safety [in light of] increasing use of wireless, Internet, and network connect[ive] devices.”123 The FDA recognized the threat stemming from failure to maintain cybersecurity in these devices, including the possibility that compromising medical devices could cause harm and death to patients.124 The FDA’s nonbinding recommendations [were] modeled on the [National Institute of Standards and Technology (“NIST”)] Cybersecurity Framework,” recommended by the White House, and it “encourages manufacturers to develop controls to ensure the security of medical devices” in the Internet of things.125 It also “encourages manufacturers to treat [cybersecurity] as a fundamental part of the development[] process” and “acknowledge[s] that device makers face [the] challenge[] [of] striking the balance between . . . cybersecurity” and making sure the device itself would remain usable.126 “The FDA also recommends that manufacturers includ[e] certain documentation as part of the premarket submission process to ensure implementation of appropriate cybersecurity controls,”127 That “documentation includes a hazard analysis, a summary of [the] controls, and a traceability matrix that ‘links actual cybersecurity . . . to the . . . risks that were considered.”128 The FDA guidance documents for software, however,

121. Id. at 2, 4.
123. U.S. FOOD & DRUG ADMIN., supra note 122.
124. Id.
125. Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices, supra note 122, at 2; U.S. FOOD & DRUG ADMIN., supra note 122. The Internet of things is a term that describes all devices with the capability of connecting to the Internet, other devices, or other networks. See Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices, supra note 122, at 2; Perakslis, supra note 39, at 396.
126. Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices, supra note 122, at 2; see also U.S. FOOD & DRUG ADMIN., supra note 122.
128. Id.
generally always focus on “large-scale computer-based equipment [and] not computerized devices,” with focus on data security and not safety. All of these are purely recommendations with no binding authority.

On December 28, 2016, the FDA published its final guidance for the Postmarket Management of Cybersecurity in Medical Devices. The guidance states repeatedly that it in no way “establishes any rights . . . and it is not binding on [the] FDA or the public.” The FDA emphasizes “that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of [the] medical devices.” In an effort to streamline this process, the FDA states that it does not intend to enforce its own reporting requirements for device patches. The FDA’s rationale is that “cybersecurity . . . updates and patches are generally considered to be a type of device enhancement for which the FDA does not require advance notification or reporting.”

However, should a cybersecurity vulnerability or exploit “pose a risk to health,” the medical device manufacturer would be required to report this to the FDA. Beyond finding a risk to health, the FDA also recommends that manufacturers use a cybersecurity vulnerability assessment tool in determining the probability of the occurrence of harm for a device, as well as for assessing the severity of harm to the patient. The rest of the December 2016 guidance echoes the other FDA rules and regulations, particularly the October guidance in terms of cybersecurity practice.

The changes to the patching of medical devices in this guidance are non-binding and unclear as

129. Templeton, supra note 48, at § 1; see also U.S. FOOD & DRUG ADMIN., supra note 122.
130. Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices, supra note 122, at 2; see also U.S. FOOD & DRUG ADMIN., supra note 122.
132. Id.
133. Id.
134. Id.
135. Id. (quoting U.S. FOOD & DRUG ADMIN., supra note 122).
136. U.S. FOOD & DRUG ADMIN., supra note 131. While a medical device manufacturer would be required to report a cybersecurity vulnerability or exploit that “pose[s] a risk to health,” it is unknown under the Guidance when the notification would occur, or if the device manufacturer would be punished for patching the exploit before notification and approval by the FDA. Id.
137. Id.
138. See id.; U.S. FOOD & DRUG ADMIN., supra note 122.
to when reporting to the FDA would be necessary for health risk cybersecurity vulnerabilities in medical devices.\(^{139}\)

The recent FDA regulations do not put forth any new ideas.\(^{140}\) The FDA created “a cross-agency working group [as long ago as 2013] involving . . . the Office of the National Coordinator for Health Information Technology and the Federal Communications Commission,” which called for recommendations and a risk-based regulatory framework but did not define what that meant.\(^{141}\) In addition, the FDA also has recommended in the past that manufacturers provide “[a] specific list of all cybersecurity risks that were considered in the design of [the] device,” controls for the device, and a plan for providing updates along the device lifecycle.\(^{142}\) The working group also recommended that manufacturers send “[a]ppropriate documentation to demonstrate that the device will . . . [arrive] free of malware,” include in the device instructions what kind of anti-virus software or firewall is on the device, if any, and that the manufacturers anticipate and include in the instructions whether a particular type of user will put their own anti-virus software on the device.\(^{143}\) This is contrary to the FDA 510(k) certification process, which requires manufacturers to be the sole party to upgrade the device and to send the patch to the FDA for approval before it goes into effect.\(^{144}\) There are so many FDA regulations and recommendations that are vague and contradictory to one another that something must be done to clarify this bureaucratic mess and establish a standard for cybersecurity of implantable medical devices.\(^{145}\)

B. Governmental Reclassifications, Power Shifts, and Executive Orders

The Health Insurance Portability and Accountability Act (“HIPAA”) pervasively regulates electronic health information through its privacy and security rules, but HIPAA focuses on data security rather than device

\(^{139}\) See U.S. FOOD & DRUG ADMIN., supra note 131; U.S. FOOD & DRUG ADMIN., supra note 122.

\(^{140}\) See U.S. FOOD & DRUG ADMIN., supra note 131; Fu & Blum, supra note 40, at 36; Perakslis, supra note 39, at 396.

\(^{141}\) Perakslis, supra note 39, at 396.

\(^{142}\) Fu & Blum, supra note 40, at 37.

\(^{143}\) Id.

\(^{144}\) See Ransford et al., supra note 2, at 162.

\(^{145}\) See U.S. FOOD & DRUG ADMIN., supra note 131; Wirth, supra note 26, at 27–28. While the agency itself has a process of reviewing and approving upgrades, the FDA itself recommends that manufacturers anticipate users putting on cybersecurity, which is contradictory to establishing any sort of standard for the device and help against the FDA’s own regulations. See U.S. FOOD & DRUG ADMIN., supra note 131; Wirth, supra note 26, at 27–28. The agency has been so malleable on this issue that it contradicts itself. See U.S. FOOD & DRUG ADMIN., supra note 131; Wirth, supra note 26, at 27–28.
security.\textsuperscript{146} Congress defined security under HIPAA as “physically protecting health information stored or transmitted electronically,” thus, failing to include cybersecurity of medical devices against hackers who want to control the device.\textsuperscript{147} Congress passed the FDASIA, which delves into levels of medical device classification for federal protection and addresses which type of FDA scrutiny they each undergo.\textsuperscript{148} The FDASIA requires the FDA to propose a strategy and recommends it on “an appropriate risk based regulatory framework focused on functionality for Health IT.”\textsuperscript{149} In April 2014, the FDA published the HIT Report, which suggested a function-based framework companies could refer to, but it did not address the “multifunctional nature of medical software.”\textsuperscript{150} Overall, the FDASIA and the HIT Report attempted to reclassify certain aspects of medical technology and devices, but that was not a strong attempt at a solution, at least in part because Congress designated the HIT Report, which it petitioned the FDA to issue as having no authority.\textsuperscript{151}

“As the FDA was completing the HIT Report [at the request of Congress], a bipartisan congressional coalition introduced the Sensible Oversight for Technology, which Advances Regulatory Efficiency Act of 2013 (“SOFTWARE Act”) . . ..”\textsuperscript{152} Just like the FDASIA, the SOFTWARE Act is another reclassification of medical device products under three different categories at the FDA.\textsuperscript{153} However, the FDA would only have jurisdiction to regulate under one of the categories.\textsuperscript{154} Clinical and health software, including software that analyzes and changes patient data, would be exempt from regulation.\textsuperscript{155}

The United States Consumer Product Safety Administration has oversight of software vulnerabilities where the FDA does not, despite the FDA having the oversight of the medical devices that host the software.\textsuperscript{156} However, the United States Consumer Product Safety Administration does not cover computer security on vulnerability assessments of software.\textsuperscript{157}

\textsuperscript{146} R.L. Garrie & P.E. Paustian, mHealth Regulation, Legislation, and Cybersecurity, in mHEALTH: TRANSFORMING HEALTHCARE 45, 46 (2014).
\textsuperscript{147} Id.
\textsuperscript{148} Kupchyk, supra note 101, at 2.
\textsuperscript{149} Id.
\textsuperscript{150} Id.
\textsuperscript{151} See id. at 2, 4.
\textsuperscript{152} Id. at 2.
\textsuperscript{153} Kupchyk, supra note 101, at 2, 4.
\textsuperscript{154} Id.
\textsuperscript{155} Id.
\textsuperscript{156} Templeton, supra note 48, at § 3.3.
\textsuperscript{157} Id.
This is just proposed legislation and another contradictory attempt at reclassification from Congress.\textsuperscript{158}

The Preventing Regulatory Overreach to Enhance Care Technology Act of 2014 ("PROTECT Act") is another proposed law, again attempting to reclassify medical devices within the FDA.\textsuperscript{159} The PROTECT Act was a congressional response to the FDA’s failure to respond to questions from the Health IT industry.\textsuperscript{160} The congressional purpose of the PROTECT Act is to prevent FDA overregulation while protecting innovation and exempting low-risk health software from a new tax under the Affordable Care Act.\textsuperscript{161} This is another attempt by Congress to reclassify medical devices, further muddying efforts to identify medical devices and implement protection at a federally consistent level.\textsuperscript{162}

The FTC is also influencing the medical device field, as the devices use wireless frequencies available in the open air.\textsuperscript{163} The data transmitted from these devices could be used and stolen as a result from cyberattacks, and this crosses over into the FTC’s administrative realm.\textsuperscript{164} The FTC issued an order in \textit{GMR Transcription Services, Inc.}, stating that the cybersecurity issue of medical records on devices that they have are poorly defined.\textsuperscript{165} The FTC then ordered GMR Transcription Services to have its security looked at and inspected for a set number of years, in order to make sure they were doing something with cybersecurity.\textsuperscript{166} This demonstrates another agency recognizing the issue of poor cybersecurity and issuing compliance check-ins to make sure that some level of cybersecurity is achieved.\textsuperscript{167}

In an executive order, President Obama issued the NIST Framework in 2013, which was designed to improve cybersecurity practices across all critical United States sectors vulnerable to cyberattack.\textsuperscript{168} The executive order required the “NIST, a division of the Department of Commerce, to develop a [set] . . . of voluntary cybersecurity best practices for [United States] critical infrastructure sectors.”\textsuperscript{169} That framework would provide an entity with an understanding of where each critical United States sector is in

\textsuperscript{158} See id.; Kupchyk, supra note 101, at 2, 4.
\textsuperscript{159} See Kupchyk, supra note 101, at 2.
\textsuperscript{160} Id. at 5.
\textsuperscript{161} Id.
\textsuperscript{162} See id.
\textsuperscript{163} See Alex Ruoff, supra note 37, at 20.
\textsuperscript{164} See id.
\textsuperscript{165} See id.
\textsuperscript{166} Id. at 3–5.
\textsuperscript{167} See id. at 4.
\textsuperscript{169} Id.
terms of vulnerability and attempt to analyze each level of security.\textsuperscript{170} The NIST Framework analyzes the usefulness of controls to a particular device in three separate areas of cybersecurity—confidentiality, integrity, and availability—and sets control levels per device for risk assessment.\textsuperscript{171} If an area is classified as high risk, the framework determines what controls need to be implemented to try to mitigate that risk.\textsuperscript{172} This is another voluntary measure that brings in another agency, along with another reclassification, separated from the many that Congress and the FDA have, which makes having any cohesive protection of implantable medical devices’ cybersecurity that much more complicated.\textsuperscript{173}

Adding another layer of complexity, during the George W. Bush administration, the Department of Homeland Security was involved in trying to tackle the issue of cybersecurity of implantable medical devices.\textsuperscript{174} The Bush Administration formed a private-sector group in partnership with the Department of Homeland Security and the Department of Health and Human Services, to convince the healthcare industry to conform to the Bush Administration’s “National Strategy to Secure Cyberspace.”\textsuperscript{175} This group ended up finding that nobody knows the condition of the healthcare sector’s collective security infrastructure, since the industry is fragmented, and each institution gauges its cybersecurity and its vulnerabilities differently.\textsuperscript{176} The group recommended raising the bar for manufacturers, “possibly by establishing [a] minimum-security standard[] for certain products and . . . [even] creating a certification process for [cybersecurity].”\textsuperscript{177} Finally, the group recommended devising a standardizing tool to help assess vulnerabilities for manufacturers, something that is still repeatedly mentioned over a decade later.\textsuperscript{178}

In October 2014, the Department of Homeland Security revealed an investigation of cybersecurity vulnerabilities in medical devices and hospital equipment that may be exploitable by cyber criminals and are susceptible to malicious hacking.\textsuperscript{179} The vulnerabilities investigated could cause severe injury and death; they were found in implantable medical devices including

\begin{footnotesize}
170. See id.  
171. Caruso & Masters, supra note 56, at 32.  
172. See id.  
173. See id.; Ruoff, supra note 168, at 1282.  
174. See Colias, supra note 4, at 62.  
175. Id.  
176. Id.  
177. Id. at 64.  
178. See id.  
179. Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices, supra note 122, at 1.
\end{footnotesize}
infusion pumps and implantable heart devices.\textsuperscript{180} The Department, however, stated that the probe started when a deceased cybersecurity expert, Barnaby Jack, demonstrated in 2012 that he could hack wireless communications and remotely cause an implanted pacemaker to deliver a lethal shock to the host.\textsuperscript{181} In response, the Department of Homeland Security said it had been “working with . . . manufacturers to identify and repair” the issues in the software of the implantable medical devices “that would allow . . . [hackers] to take control of them.”\textsuperscript{182}

In contrast to all these ambiguous regulations, proposals, executive orders, legislation, and proposed legislation, the Department of Defense has a very strict policy for all devices that the military uses.\textsuperscript{183} The “Department of Defense Information Assurance Certification and Accreditation Process program mandates strict certification requirements for [all] . . . computer systems” provided for the military, including hospital equipment and medical devices of all kinds.\textsuperscript{184} In order for these devices to be sold to the Department of Defense, they must meet a strict security certification.\textsuperscript{185} This has caused problems, as most manufacturers are not willing or even capable of bearing the financial cost necessary of meeting the standards due to the size of the market.\textsuperscript{186}

IV. PROPOSED SOLUTIONS

In all, at least five agencies have indicated intent to regulate cybersecurity in medical devices, but nothing is clear and concrete, and what exists is overlapping, confusing, and contradictory.\textsuperscript{187} The private sector recognizes the need for an enforceable system pursuant to which medical devices can be tested on a baseline of cybersecurity standards through the FDA.\textsuperscript{188} The nature of the medical industry, comprised of both private and public entities, requires a willingness to unify to address cybersecurity at a

\begin{itemize}
  \item \textsuperscript{180} Id.
  \item \textsuperscript{181} Id. at 1–2.
  \item \textsuperscript{183} Templeton, \textit{supra} note 48, at § 4.3.
  \item \textsuperscript{184} Id.
  \item \textsuperscript{185} Id.
  \item \textsuperscript{186} Id.
  \item \textsuperscript{187} See Mathias Klümper & Erik Vollebregt, \textit{Navigating the New EU Rules for Medical Device Software}, 2009 REG. AFF. J. DEVICES, 83, 83; Ruoff, \textit{supra} note 168; Ruoff, \textit{supra} note 37.
  \item \textsuperscript{188} \textit{Homeland Security Investigating Medical Device Cybersecurity}, \textit{supra} note 1; Ruoff, \textit{supra} note 33.
\end{itemize}
consistent level nationwide.\textsuperscript{189} This can be achieved by combining the strengths of the federal government—homeland security and public safety—with the innovative ability of the private sector to tackle cybersecurity for implantable medical devices.\textsuperscript{190} This is important, for knowledge of the technological domain specific to implantable medical devices needs to be coupled with the regulation if it is to be strong and not a hindrance to the medical devices’ purpose.\textsuperscript{191} Just as the federal government and its agencies have developed ways to detect, track, identify risks, and prevent and combat epidemics with the help of the private sector, so too can the government, to an extent, do the same thing to mitigate the harm that can result from the vulnerabilities in implantable medical devices.\textsuperscript{192} Standards are useful in creating secure products, as they can help a manufacturer ensure that all known issues have been considered, and this is especially important in very complex devices such as implantable medical devices.\textsuperscript{193} Part A discusses possible federal solutions to clearing up the bureaucratic confusion among all of the various governmental bodies.\textsuperscript{194} Part B explores various private sector solutions, including traditional and nontraditional solutions to tackling cybersecurity in implantable medical devices.\textsuperscript{195} This also includes some potential private regulation.\textsuperscript{196} Some persuasive examples emanate from the European Union (“EU”) and an international standards body, both of which have attempted to secure implantable medical devices.\textsuperscript{197} Lastly, Part C warns of the dangers of poorly drafted regulations in this area, highlighting how bad regulation can both compromise the user of an implantable medical device and harm the medical device industry.\textsuperscript{198}

A. \textit{Governmental Solutions}

Governmental solutions in the United States could vary greatly. One absolutely necessary step is for the agencies to collaborate on a set of universal definitions.\textsuperscript{199} There are classifications that Congress, the FDA,
the White House, and the other agencies must clarify, with the first step being the use of universal definitions.200 “[M]edical applications can be of two types: [W]earable and implanted. Wearable devices are those that can be used on [the] body surface of a human or [in] close proximity [to] the user,” such as, a heart rate monitor, blood pressure monitor, and glucose sensor.201 Implantable medical devices, on the other hand, “are those [devices] that are inserted inside [the] human body,” such as, an implantable defibrillator and insulin pump.202 Having clear, non-ambiguous definitions used by all agencies, whether the list appears in legislation or regulations, would help alleviate some of the confusion.

Another solution would be to expand HIPAA to give the Department of Health and Human Services power over cybersecurity issues in this realm and teeth to enforce the new regulations.203 The Department of Health and Human Services Office for Civil Rights estimates that 66% of providers have not complied with the HIPAA-mandated audit of security controls for their electronic health records.204 Organizations generally “wait until an attack or breach has occurred to perform an audit,” and apparently are willing to take the risk of incurring civil monetary penalties imposed for noncompliance with HIPAA.205 Even if organizations complied with HIPAA, most of the HIPAA protection relies on standard methods of isolating critical data, which is bypassed by attackers when taking over or overloading an implantable medical device.206 A possible solution would be to give HIPAA coverage of cybersecurity of devices and put power into the enforcement of its provisions for cybersecurity.

The FDA has already recommended a set of regulatory improvements.207 The October FDA Guidance included recommendations that would help to address the cybersecurity issues if they were implemented as requirements in a regulation on implantable medical devices.208 Starting with the premarket submission process to the FDA, demonstrating the existence of a hazard analysis, a summary of controls, and a traceability matrix that links actual controls to the cybersecurity risks foreseen by the manufacturer would ensure that devices incorporate some sort of

200. See id.
202. Id.
203. See Ruoff, supra note 37, at 20.
204. Ruoff, supra note 168, at 1282.
205. Id.
207. U.S. FOOD & DRUG ADMIN., supra note 122.
208. Id.; see also Medical Devices and Cybersecurity Risks: DHS Investigates At-Risk Devices, supra note 122, at 2.
cybersecurity precautions.209 “Manufacturers should address cybersecurity during the design and development of the medical device,” with a vulnerability and management approach for the life of the device.210 Due to the longevity of implantable medical devices, it is important that a cybersecurity plan—from the beginning—is in place, instead of being reactionary and doing ad hoc fixes once problems occur.211 This can be coupled with the “software validation and risk analysis” that is already required for certification of an implantable medical device by the FDA.212

The cybersecurity and vulnerability approach should assess threats and vulnerabilities, mitigation strategies, risk, and accepted risk.213 It should also balance the safeguards that the manufacturer decides to put in place, to make them appropriate to the user and location of use, so that security controls will not hinder access in an emergency situation.214 There should also be features in implantable medical devices that recognize and detect breaches, log them, and act on them during normal use, as well as have a failsafe mode for when the device is compromised, so that the critical functionality is still protected.215 The current language is only persuasive and suggestively vague to consider all devices; yet, having it as a pre-market approval requirement would force manufacturers and the FDA to take cybersecurity into account as part of the FDA approval process.216

B. Other Solutions

The private sector also has recommendations on ways to implement a national cybersecurity standard.217 One is to certify third-party testers to test security vulnerabilities in devices.218 Another is a national information sharing system for medical device cybersecurity to detect the latest security vulnerabilities and tackle them.219 This, coupled with a federal safe harbor provision for reporting cybersecurity breaches of medical devices, would allow a clearer picture of the state of cybersecurity of the devices and allow

---

209. U.S. FOOD & DRUG ADMIN., supra note 122.
210. Id.
211. Caruso & Masters, supra note 56, at 33.
212. U.S. FOOD & DRUG ADMIN., supra note 122.
213. Id.
214. Id.
215. Templeton, supra note 48, at § 2.1.6; U.S. FOOD & DRUG ADMIN., supra note 122.
216. See U.S. FOOD & DRUG ADMIN., supra note 122.
217. See Vijayan, supra note 182.
218. Id.
219. See Kramer et al., supra note 76, at 7.
new cybersecurity issues to be addressed.220 “[A]ctive and real-time surveillance and communication of emerging cyberthreats” can only help in securing all implantable medical devices.221 While there is an inherent perceived danger to knowing and reporting cybersecurity of devices, security experts have long stated that secret cybersecurity protocols are commonly reversed engineered and easily defeated.222 A better method of security is to have a system that is completely open to critique, thus making it more secure across the board.223 This follows “[a] fundamental tenant of cryptography . . . known as Kerckhoffs’ principle,” which states that a system “should be secure even if the adversary knows everything about the system except its key.”224 By choosing a system that is in the public, the community as a whole only strengthens the end product’s security by working on it together.225

A Host Intrusion Detection and Prevention System (“HIDS/HIPS”) is another means of protecting implantable medical devices.226 HIDS/HIPS, “technologies are based on managing a known behavior of a system,” and preventing any unknown behavior from happening or taking over.227 This kind of system would work well in implantable medical devices because it provides strong protection against attacks that have never occurred before.228 However, there is always the possibility of a HIDS/HIPS preventing critical support from the device, and it can be tricked by a hacker.229 Despite this, a HIDS/HIPS addresses some concerns for cybersecurity of implantable medical devices and warrants further exploration of implementation in implantable medical devices.230

There are other means to address cybersecurity concerns of implantable medical devices outside of conventional cybersecurity methods.231 One involves “tattooing the encryption key” to an encrypted implantable medical device on the patient in an “invisible, UV-light-readable ink” for emergency situations.232 Along the same vein of modifying the user for added cybersecurity protection is one type of cybersecurity control, tested

220. See id. at 2–3.
221. Perakslis, supra note 39, at 397.
222. Templeton, supra note 48, at § 2.1.8.
223. See id.
224. Ransford et al., supra note 2, at 160.
225. Id.
226. Wirth, supra note 26, at 31.
227. Id.
228. Id.
229. See id.
230. See id. at 31–32.
231. See Templeton, supra note 48, at § 3.1.
232. Id.
in a pacemaker, that allows access in emergency situations to medical personnel by connecting to a computer and using the patient’s heartbeat as authorization for commands by an external system. This, however, defeats the purpose of a wireless implantable medical device, and it would require surgery to access the internal medical device, putting the patient at risk. Another option is a subcutaneous push switch that would be implanted under the skin of the patient for the purpose of reprogramming the device and allowing access, thus, allowing emergency personnel to be able to be reset in a failsafe mode. Additionally, RF-shielding wearable pouches can accompany the patient, which would restrict the wireless communication of the implantable medical device to millimeters and require a security token to access. Lastly, a standardizing score that applies to a device that answers in a satisfies/does not satisfy evaluation for each aspect of the device can be used to evaluate whether or not a device meets a certain score, which would determine whether it should be marketed. While a high score in this area could be used by medical device manufacturers to promote their products as a new type of marketing edge over competitors, it trivializes cybersecurity and is not focused enough towards tackling specific issues. If this system was coupled with suggestive FDA regulations, however, it could prove to be a general solution.

Lastly, the United States can look towards the EU as a guidepost for how to approach cybersecurity in medical device software. In Directive 2007/47/EC, the EU imposed stricter rules on software used with medical devices, although it only applies to software that directly controls the device. The directive makes it so that all software is updated, validated, and approved from an authoritative agency, and does not change the risk classification of the device. While this echoes what the FDA already does to an extent, the fact that it specifically covers and classifies the software of the medical device should be taken into consideration. Additionally, the EU conducted a cybersecurity “exercise involving 29 countries and 200

---

233. Caruso & Masters, supra note 56, at 35.
234. See Ransford et al., supra note 2, at 162.
235. Templeton, supra note 48, at § 3.1.
236. Id.
237. Caruso & Masters, supra note 56, at 35.
238. See id.
239. See U.S. FOOD & DRUG ADMIN., supra note 122; Caruso & Masters, supra note 56, at 32, 35.
240. See Klümper & Vollebregt, supra note 187, at 83.
241. Id. at 83.
242. Id. at 85–86.
agencies deal[ing] with attack scenarios against critical infrastructure[s],” which included hospitals and hacking into medical devices.\(^{244}\) As the EU Commission Vice President stated, “[t]he sophistication and volume of cyberattacks are increasing every day. . . . They cannot be countered if individual states work alone or just a handful of them act together.”\(^{245}\) Outside of the EU, international standards bodies, such as the Association for the Advancement of Medical Instrumentation, have formed working groups and issued standards on medical device security that include manufacturers and regulators.\(^{246}\) Regardless of whether the United States follows the EU or an international standardizing body, international harmonization of cybersecurity is almost inevitable due to the nature of the Internet.\(^{247}\)

C. Dangers with Governmental Regulation

There are dangers with increased regulations that must be considered.\(^{248}\) Regulations can become burdensome to technological advancement, with Congress—or any executive administrative body—failing to take into account the concerns of the healthcare industry and the knowledge of how to make a device that would not harm a patient by running slowly when implementing the regulations.\(^{249}\) The industry itself must understand the capital and operating costs of implementing a cybersecurity system and factor that in, or else face potential inept and burdensome regulations.\(^{250}\)

The FDA Guidance also recommends that manufacturers consider implementing things like authentication protocols, automatic timers to terminate connections with a device after a period of time, placing physical locks on the devices, and making stronger passwords to the devices.\(^{251}\) It also recommends a layered user authentication procedure and restriction of updates, allowing users to download and update their own software and

---


\(^{245}\) Id.

\(^{246}\) Fu & Blum, supra note 40, at 37.

\(^{247}\) See id.


\(^{249}\) See id. at 55.

\(^{250}\) Id. at 55.

\(^{251}\) U.S. FOOD & DRUG ADMIN., supra note 122, at 5.
firmware from the manufacturer. These recommendations, however, have already been considered to be dangerous by medical device manufacturers and have been proven to be harmful in locking out medical personnel in an emergency to a patient. Many good cybersecurity requirements, in fact, conflict with the need for emergency access to a device. Additionally, requiring implantable medical devices to incorporate certain software can have a major impact on the battery life of the device, reducing the longevity of the device and causing other potential issues. This carries over into the plain fact that there are different levels of severity of vulnerabilities in implantable medical devices. For example, a cardiac defibrillator can kill its user, while a non-actuating glucose sensor cannot do lethal damage on its own. This danger must be taken into consideration when making any sort of regulations for implantable medical devices.

Another regulatory concern is that there are usually compromises that specifically exclude certain areas from needing to be secured in making any regulation. One example is “the NERC-CIP cybersecurity standard for the North American bulk power system,” which specifically excludes non-routable protocols and narrowly defines devices considered critical assets bound by the regulatory standards. Organizations typically do the minimum to meet regulatory compliance, which means excluding some areas, which would highlight weak areas for attackers to gain access. Due to this practice, numerous people in the medical industry and the government are concerned that if standards are written and enforced, they may actually undermine the purpose of trying to protect the user of the implantable medical device.

Finally, of course, increased regulation of certain medical devices can lead to an increase in the cost of certification and testing of the devices themselves. An example is in the aviation industry, “where over 50% of the resources required to develop new, safety critical systems” are used in

252. Id.
253. See Gupta, supra note 22.
254. See id.
255. Ransford et al., supra note 2, at 159.
256. Id. at 161.
257. Id.
258. See Gupta, supra note 22.
259. Templeton, supra note 48, at § 4.2.
260. Id.
261. Id.
262. Id.
just certifying the system.\textsuperscript{264} For medical devices and cybersecurity, much of the hardware and software are still incapable of being reliant due to the need for more advanced and integrated technology, as current widely used techniques and protocols are inappropriate for the confined space of an implantable medical device.\textsuperscript{265} The right balance needs to be found in regulation to establish security without creating expensive and complicated standards that are contradictory in nature.\textsuperscript{266} Legislation and regulation can facilitate increasing cybersecurity through base guidelines for implantable medical devices, but they can also harm patients if they fail to take into account industry knowledge and dangers.\textsuperscript{267}

V. CONCLUSION

Hackers have turned from hacking businesses and governments for fame and fortune to covert organized cybercrime, which is estimated to be exceeding the illegal drug trafficking trade.\textsuperscript{268} It is dangerously naïve for the federal government and medical device manufacturers to fail to understand that “many individuals . . . are highly intelligent, skilled, and motivated” to find and exploit weaknesses in medical devices.\textsuperscript{269} These devices were “not designed to withstand terrorist attacks. . . . ‘Permitting control of a component in a human body without authentication seems grossly negligent, and should raise the ire of the FDA.’”\textsuperscript{270} Former Secretary of Defense, Leon Panetta, was correct in stating that an organized attack focused on vulnerabilities of implantable medical devices “could be a cyber Pearl Harbor, an attack that would cause physical destruction and the loss of life.”\textsuperscript{271}

The problem facing implantable medical device manufacturers is complex, requiring a balance of usability, performance, and safety, while taking into consideration the cybersecurity threats of a growing digitally connected world.\textsuperscript{272} Without a standardized baseline for specifications, the interconnectivity of every medical device will negate some security features of others and create opportunities for attacks.\textsuperscript{273} The “healthcare industry needs to . . . [become] involved in [the current] legislative process [on

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{264} Id. at 163.
\item \textsuperscript{265} Gupta, \textit{supra} note 22.
\item \textsuperscript{266} Perakslis, \textit{supra} note 39, at 397.
\item \textsuperscript{267} See Garrie & Paustian, \textit{supra} note 146, at 45.
\item \textsuperscript{268} Wirth, \textit{supra} note 26, at 26, 29.
\item \textsuperscript{269} Templeton, \textit{supra} note 48, at \S\ 2.1.7.
\item \textsuperscript{270} Id. at \S\ 3.1.
\item \textsuperscript{271} Barnett et al., \textit{supra} note 34, at 44.
\item \textsuperscript{272} Caruso & Masters, \textit{supra} note 56, at 32.
\item \textsuperscript{273} See Templeton, \textit{supra} note 48, at \S\S\ 2.1, 4, 4.2.
\end{enumerate}
\end{footnotesize}
implantable medical devices] or risk the imposition of . . . regulations” that can harm the product through unintended consequences and hinder the technological growth of implantable medical devices.274

The threat of cyberattacks is a clear and present danger, and it is time to focus on ways to protect the user from a technology that can be altered remotely to be a weapon instead of a significant life-changing tool.275 It is up to key players—the “[p]roviders, manufacturers, security experts, industry organiz[ers], [and the government] . . . to work together to . . . protect [the] integrated healthcare” industry that is becoming more connected with the Internet every day.276

274. Mittman & Cain, supra note 248, at 55.
275. Perakslis, supra note 39, at 397.
276. Wirth, supra note 26, at 33.
ARTICLES AND SPEECHES

INTRODUCTION TO REGULATING INNOVATION IN HEALTHCARE: PROTECTING THE PUBLIC OR STIFLING PROGRESS?  
KATHY L. CERMINARA  
MARILYN UZDAVINES

THE PERSISTENCE OF OPPORTUNISTIC BUSINESS MODELS IN HEALTHCARE AND A STRONGER ROLE FOR INSURANCE REGULATORS IN CONTAINING HEALTH CARE COSTS  
JACKSON WILLIAMS

STATE LAW GOVERNANCE OF HEALTH INFORMATION TECHNOLOGY  
CASON SCHMIT

KEEPING INTERNET PIRATES AT BAY: RANSOMWARE NEGOTIATION IN THE HEALTHCARE INDUSTRY  
PAUL R. DEMURO

PATIENT SAFETY SHOULD INCLUDE PATIENT PRIVACY: THE SHORTCOMINGS OF THE FDA’S RECENT DRAFT GUIDANCE REGARDING CYBERSECURITY OF MEDICAL DEVICES  
CHRISTOPHER KERSBERGEN

CARDIAC DEFIBRILLATORS NEED TO HAVE A BULLETPROOF VEST: THE NATIONAL SECURITY RISK POSED BY THE LACK OF CYBERSECURITY IN IMPLANTABLE MEDICAL DEVICES  
MICHAEL WOODS
ARTICLES AND SPEECHES

INTRODUCTION TO REGULATING INNOVATION IN HEALTHCARE: PROTECTING THE PUBLIC OR STIFLING PROGRESS? 
KATHY L. CERMINARA MARILYN UZDAVINES

THE PERSISTENCE OF OPPORTUNISTIC BUSINESS MODELS IN HEALTHCARE AND A STRONGER ROLE FOR INSURANCE REGULATORS IN-containing health care costs
JACKSON WILLIAMS

STATE LAW GOVERNANCE OF HEALTH INFORMATION TECHNOLOGY
CASON SCHMIT

KEEPING INTERNET PIRATES AT BAY: RANSOMWARE NEGOTIATION IN THE HEALTHCARE INDUSTRY
PAUL R. DEMURO

PATIENT SAFETY SHOULD INCLUDE PATIENT PRIVACY: THE SHORTCOMINGS OF THE FDA’S RECENT DRAFT GUIDANCE REGARDING CYBERSECURITY OF MEDICAL DEVICES
CHRISTOPHER KERSBERGEN

CARDIAC DEFIBRILLATORS NEED TO HAVE A BULLETPROOF VEST: THE NATIONAL SECURITY RISKPOSED BY THE LACK OF CYBERSECURITY IN IMPLANTABLE MEDICAL DEVICES
MICHAEL WOODS