AN A.S. PRATT PUBLICATION
OCTOBER 2017
VOL. 3 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 8 OCTOBER 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:

Deneil C. Targowski at	908-673-3380
Email:	Deneil.C.Targowski@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at	(800) 833-9844
Outside the United States and Canada, please call	(518) 487-3385
Fax Number	(800) 828-8341
Customer Service Web site	http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or	(800) 223-1940
Outside the United States and Canada, please call	(937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [272] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2017 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Filling in the Gaps on Medical Device Cybersecurity

By Yarmela Pavlovic and Shilpa Prem [*]

The authors of this article discuss a recent multi-agency public workshop on the cybersecurity of medical devices.

The Food and Drug Administration ("FDA"), in collaboration with the National Science Foundation ("NSF") and the Department of Homeland Security ("DHS") Science and Technology Directorate ("S&T") recently convened a public workshop on cybersecurity of medical devices. Cybersecurity has become a hot button topic for many in the medical device industry following the announcement of several high-profile medical device vulnerabilities and ransomware attacks. A number of the world's largest healthcare tech companies have released warnings about WannaCry and the possible impact the virus may have on their products. Many device companies have recently and reactively generated and released patches to protect systems from possible future attacks. FDA's workshop, held amid these events, sought to gather further feedback regarding the steps FDA should be taking to characterize and address medical device cybersecurity.

THE WORKSHOP

The workshop was organized by the Regulatory Science Subcommittee of the CDRH Center Science Council, which assesses and prioritizes gaps in regulatory issues for medical devices based on input from CDRH Offices. Although FDA has now released two guidance documents addressing premarket and postmarket regulatory issues, cybersecurity of medical devices continues to be identified as one of the top ten gaps where new regulatory tools, technologies, and approaches are needed to address potential threats. Through the workshop, FDA, NSF, and DHS S&T gathered input from major stakeholders in the industry on how to address these gaps. Speakers at the workshop came from various backgrounds, including government, medical device companies, healthcare institutions, research management companies, and consulting firms.

Common Themes

The top common themes amongst the presenters on the first day of the workshop included:

[*] Yarmela Pavlovic is a partner at Hogan Lovells helping medical device manufacturers get FDA marketing approval for their devices. Shilpa Prem is an associate at the firm representing clients in FDA medical device approval and clearance associated matters. The authors may be reached at yarmela.pavlovic@hoganlovells.com and shilpa.prem@hoganlovells.com, respectively.

- *Collaborative risk management*. The process of risk mitigation must involve a collective effort between medical device manufacturers, hospitals, and patients to trace and address cybersecurity vulnerabilities.
- *Medical devices do not stand alone*. Cybersecurity mitigation tools must address more than stand-alone medical devices, but should also include the network of technologies the medical device may be connected to.
- *Scalability of protections*. Medical device manufactures must ensure that their cybersecurity protection mechanisms are scalable.
- *Involvement by all stakeholders*. Involvement of all major stakeholders, including medical device manufacturers, hospitals, and patients, is critical to the risk mitigation process.

The workshop highlighted that each stakeholder group brings different perspectives about the approach to cybersecurity. Throughout the first day, speakers representing medical device manufacturers commented on their own best practices. One medical device manufacturer indicated that they offer customers security white papers and include a security privacy website that customers can review. Another medical device manufacturer commented on the creation of a formal mechanism to report possible security vulnerabilities so that risks can be addressed as soon as they are known. Speakers commented that such action creates a culture of transparency so that a manufacturer's security program can be continuously built and improved. Speakers from medical device companies suggested that safety and security are two legs of the stool and that actual usability is the third leg (i.e. how the patient will interact with the device and any unique healthcare institutional factors that may need to be considered during the use of the device). Medical device manufactures also emphasized that tailoring security protections to the expected real-world use of the device is important.

Key Observation

Key among the observations during the workshop was the theme that cybersecurity mitigation tools should contemplate the entire network of technologies into which the medical device connects, rather than each device in standalone fashion. Individual medical devices are typically developed in silos and are cleared/approved independently by the FDA. However, interoperability is also key and at some point in the process an analysis should be conducted evaluating how a device would be used in the real-world and the extent to which connections to other devices and systems may introduce vulnerability. One speaker from a large healthcare institution commented that their facility had implemented an initiation process where new devices that are added to the network undergo a rigorous process to address cybersecurity risks from the start. The speaker emphasized that this method assists in continuously addressing vulnerabilities as they come up. However, the same speaker caveated this process, indicating that larger health networks that have a number of resources have the ability to conduct such analysis, whereas smaller healthcare entities may find this more challenging. The speaker suggested that for smaller entities, it is important for medical device manufacturers to partner with hospital administration to ensure the security risk mitigation tools are tailored appropriately for the institution. A medical device manufacturer further emphasized that manufacturers should not be afraid of having open dialogs with their customers regarding these very real risks.

Cybersecurity Protection Mechanisms

Medical device manufactures highlighted the fact that cybersecurity protection mechanisms should be scalable. They emphasized that depending on the size of the organization, each healthcare facility's network of interconnected devices presents unique challenges that may not be the same for other hospital systems. A speaker from a healthcare institution indicated that "medical devices [present] the weakest link" and that at one hospital, for an example, there are 25,000 network connected devices that consist of greater than 6,000 unique make, model, versions, each having their own security challenges. Medical device manufacturers stressed that cybersecurity protections that may be effective for smaller hospital systems that may not have as many interconnected devices should be scalable to cater to larger entities as well. Medical device manufacturers recommended that manufacturers use already established mechanisms in combating cybersecurity risks that would work in larger and small healthcare entities including the adoption of using secure coding standards, performing static code analysis, adopting hardening standards, performing vulnerability scanning, performing product security requirements risk assessment, performing robustness and penetration testing, developing vulnerability monitoring, and a patch management plan.

Working Group Questions

A significant portion of the workshop was dedicated to smaller breakout groups where representatives from the government, medical device companies, healthcare institutions, research management companies, and consulting firms contributed to opportunities for FDA engagement and discussed innovative strategies to address these challenges moving forward. In large part, the focus of the groups was to identify areas for further research and work by FDA. One working group proposed the following questions to be researched by the agency in order to better understand the gaps that may need to be addressed to tackle cybersecurity:

- When is the proposed cybersecurity protection enough? Should FDA develop a "building code" for cybersecurity, indicating at a minimum the factors manufacturers should consider when developing cybersecurity risk mitigation tools?
- Who is ultimately responsible in ensuring that the medical device has adequate protections against cyber-attacks (i.e. should it be the medical device manufacturer or the healthcare facility)?

- How should the industry handle aging products? Does the responsibility shift at a certain point in the lifecycle of the device? (Perhaps a possible analysis of other critical infrastructure industries could provide some guidance).
- Given increasing dependence on clinical decision support, what requirements should be in place to ensure that it is trustworthy given possible cybersecurity risks?

CONCLUSION

With these questions to be answered, FDA continues to dig into the complicated and ever-changing world of cybersecurity. FDA is expected to issue a report arising from the workshop discussions.