EDITOR’S NOTE: HEALTHY DATA
Victoria Prussen Spears

HEALTHIER DATA, HEALTHIER PATIENTS: CYBERSECURITY AND BETTER HEALTH OUTCOMES
Kimberly C. Metzger

NINTH CIRCUIT HOLDS NO PRIVATE RIGHT OF ACTION FOR DATA RETENTION VIOLATION UNDER THE VIDEO PRIVACY PROTECTION ACT
Sharon R. Klein and Alex C. Nisenbaum

HACKERS CONTINUE TO PERPETRATE WIRE TRANSFER FRAUD SCAMS ON A GLOBAL SCALE
Greg Burch, David Harrell, and Adrian Taylor

SEC SETTLES CHARGES AGAINST INVESTMENT FIRM THAT FAILED TO ADOPT CYBERSECURITY POLICIES BEFORE DATA BREACH
Richard H. Martin

IN THE COURTS
Steven A. Meyerowitz

LEGISLATIVE AND REGULATORY DEVELOPMENTS
Victoria Prussen Spears

INDUSTRY NEWS
Victoria Prussen Spears
Editor’s Note: Healthy Data
Victoria Prussen Spears

Healthier Data, Healthier Patients: Cybersecurity and Better Health Outcomes
Kimberly C. Metzger

Ninth Circuit Holds No Private Right of Action for Data Retention Violation under the Video Privacy Protection Act
Sharon R. Klein and Alex C. Nisenbaum

Hackers Continue to Perpetrate Wire Transfer Fraud Scams on a Global Scale
Greg Burch, David Harrell, and Adrian Taylor

SEC Settles Charges Against Investment Firm that Failed to Adopt Cybersecurity Policies Before Data Breach
Richard H. Martin

In the Courts
Steven A. Meyerowitz

Legislative and Regulatory Developments
Victoria Prussen Spears

Industry News
Victoria Prussen Spears
Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
STEVEN A. MEYEROWITZ
President, Meyerowitz Communications Inc.

EDITOR
VICTORIA PRUSSEN SPEARS
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES
Partner, Venable LLP

RICHARD COHEN
Special Counsel, Kelley Drye & Warren LLP

CHRISTOPHER G. CWALINA
Partner, Holland & Knight LLP

RICHARD D. HARRIS
Partner, Day Pitney LLP

DAVID C. LASHWAY
Partner, Baker & McKenzie LLP

CRAIG A. NEWMAN
Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL
Partner, Sidley Austin LLP

AARON P. SIMPSON
Partner, Hunton & Williams LLP

RANDI SINGER
Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI
Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE
Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH
Partner, Thompson Hine
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 2016 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 inquiries 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.
Healthier Data, Healthier Patients: Cybersecurity and Better Health Outcomes

By Kimberly C. Metzger*

Medical identity theft, and incomplete patient disclosure due to cybersecurity concerns, can be dangerous – even deadly – to individuals, and can compromise community wellness. Breaches of health information can have serious economic and other consequences for providers as well. The author of this article discusses the cybersecurity landscape in healthcare, medical identity theft, patient disclosures, and implementing a security management program for health information.

Breaches of health information can have serious consequences for both providers and patients. It is easy to imagine the financial implications of cybersecurity incidents and data breaches.¹ The effort and expense associated with investigation, forensics, mitigation of damages, lost good will and reputation, billing problems, and monitoring and unraveling consumer credit are significant and can have far reaching effects for all parties.

While monetary losses are a large and well-known part of an incident or breach, compromised data security at health organizations can also contribute to a less-recognized, but perhaps more insidious, problem: poorer health outcomes. Medical identity theft, and incomplete patient disclosure due to cybersecurity concerns, can be dangerous – even deadly – to individuals, and can compromise community wellness.

Health organizations hold a wide variety of highly confidential personally identifying information ("PII") that can wreak havoc in the wrong hands. Names, addresses, dates of birth, Social Security and driver’s license numbers, and financial account information are data points wrongdoers traditionally seek to commit financial identity theft. Records from health organizations contain this information and more. By their very nature, health records include data of an extremely private and personal nature related to patients’ overall physical condition, disease states, medical ailments, disabilities, and insurance, including Medicare, Medicaid, and Social Security ("medical PII"). Breach and misuse of medical PII, or even the perceived risk of breach or misuse, can cause physical as well as financial harm. As Federal Trade Commission ("FTC") Commissioner Terrell McSweeney remarked in March 2015:

* Kimberly C. Metzger is a partner in Ice Miller LLP’s litigation group, concentrating her practice in drug and device litigation and data privacy and security, particularly HIPAA privacy compliance. She may be reached at kimberly.metzger@icemiller.com.

¹ A useful definition of "security incident" can be found in the HIPAA Security Rule: "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." (45 CFR 164.304.) A "breach" typically refers to an actual unauthorized acquisition, access, use, or disclosure that compromises the security or privacy of unsecured data.
One of the most lucrative avenues for identity thieves has become the stealing and exploitation of medical records. Unlike other forms of identification, our medical records offer nearly complete portraits of our lives and data. These factors have made medical records, and more specifically children’s medical records, the most valuable consumer information in the black market. Scammers can use the medical records of children to steal identities and commit frauds that have a good chance of remaining undetected until a child turns 18.2

Because health records contain information that could be particularly embarrassing if disclosed, a patient who is insecure about a provider’s data practices might fear revealing sensitive, but highly relevant, medical information such as smoking status, risky sexual behavior, drug or alcohol use, and mental health concerns. If an incident or breach actually occurs, a patient’s medical PII could be used to commit medical identity theft (the fraudulent use of medical credentials to receive or bill for healthcare), resulting in a “mixed medical record” and serious physical harm to the patient.

THE CYBERSECURITY LANDSCAPE IN HEALTHCARE

Security incidents and data breaches are prevalent in health organizations. From cyberattacks and systems failures to employee negligence and malicious insiders, the question is really no longer if, but when and how, an incident or breach will occur. Small health care providers, who believe their size and low profile immunize them from attack, may actually be at higher risk because they are less likely to take protective action (and criminals know this).

The Ponemon Institute’s recently-published Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data paints an unsettling picture: during the last two years, 65 percent of represented health care organizations experienced electronic-based security incidents, and 54 percent experienced paper-based security incidents. More than 90 percent had a data breach, and 40 percent had more than five breaches. The study estimates that the health care industry accounted for 44 percent of all 2013 data breaches – more than any other economic sector.

Several factors have converged to create a perfect storm on the healthcare landscape. First, electronic medical PII is more available than ever before. Both the American Recovery and Reinvestment Act and the Affordable Care Act incentivize – and sometimes require – healthcare providers to digitize patient data. Second, medical PII has high black market value. While estimates vary, one cybersecurity expert who monitored underground transactions posits that stolen health credentials can command

---

10-20 times the price of a U.S. credit card number. Third, health organizations have lagged behind the more traditional targets (financial services and retail) in cybersecurity savvy. Because the transition to digitized health data is relatively recent, the healthcare sector has simply not been pushed earlier to prepare. In April 2014, the Federal Bureau of Investigation (“FBI”) issued a private industry notification to healthcare providers warning “[t]he healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely. . . .”

Cybercriminals recognize that medical PII is a lucrative asset in a less-secure environment.

Despite the “universal risk for data breach,” the Ponemon study found that health organizations are not, overall, particularly confident of their ability to detect and respond to incidents and breaches:

- 58 percent report having policies and procedures in place to effectively prevent or quickly detect unauthorized access, loss, or theft of patient data.
- 53 percent report that personnel have the technical expertise to identify and resolve data breaches.
- Only 49 percent agree they have sufficient technologies to effectively prevent or quickly detect breaches.
- Only 33 percent report having sufficient resources to effectively prevent or quickly detect breaches.

The study concludes:

Healthcare organizations . . . face a rapidly changing threat landscape. Cybercriminals recognize two critical facts of the healthcare industry: 1) healthcare organizations manage a treasure trove of financially lucrative personal information and 2) healthcare organizations do not have the resources, processes, and technologies to prevent and detect attacks and adequately protect patient data. While the findings reveal a slow but steady increase in technologies, the pace of investments is not fast enough to keep up with the threats to achieve a stronger security posture.

---

3 Caroline Humer and Jim Finkle, Your medical record is worth more to hackers than your credit card number. Reuters (September 24, 2014), accessed June 30, 2015 at http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.
5 Ponemon Institute, Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data (the “Study”), p. 3.
6 Id. at 26.
MEDICAL IDENTITY THEFT

Medical identity theft occurs when a wrongdoer uses health credentials to fraudulently bill for goods or services, or to obtain healthcare in someone else’s name. The wrongdoer may accomplish this with the true patient’s consent – for example, when the true patient shares health credentials with an uninsured family member or friend – or by stealing the true patient’s medical PII. Medical identity theft is underappreciated, but on the rise. The Ponemon Institute estimates the number of victims increased from more than 1.5 million in 2012, to more than 1.8 million in 2013.7

Like its financial counterpart, medical identity theft can cause monetary loss, damaged credit, and reputational harm. Medical identity theft is unique, however, in its ability to cause physical injury via a “mixed medical record.” When a person obtains medical care in another’s name, the fraudulent user’s medical information is integrated with the true patient’s information in a single, corrupted medical record that does not accurately reflect the true patient’s health condition. It is easy to imagine the potential for harm: The fraudulent user’s blood type is given to the true patient, who has a different blood type. The fraudulent user’s medication allergies are attributed to the true patient, who either receives a medicine to which she is allergic, or is denied a medicine to which she is not allergic. The fraudulent user’s “no medications” history is attributed to the true patient, who is given a medicine that interacts with another that he is, in fact, taking.

These potential harms are more than theoretical. The 2013 Ponemon survey queried 788 adults who reported they, or a close family member, were the victim of medical identity theft. Of those surveyed:

- 56 percent lost trust and confidence in their health care provider.
- 15 percent reported misdiagnosis because of inaccuracies in the health record.
- 14 percent experienced a delay in receiving medical treatment because of inaccuracies in the health record.
- 13 percent experienced mistreatment of illness because of inaccuracies in the health record.
- 11 percent were prescribed the wrong pharmaceutical.

Medical identity theft is clearly a quality of care issue.

PATIENT DISCLOSURES

Healthcare providers’ cybersecurity practices, and patients’ perceptions of those practices, may have profound effects on both patients and public health. A 2014 study by researchers at the Harvard School of Public Health showed that patients who are concerned about their healthcare provider’s cybersecurity practices are more

---

7 Ponemon Institute, 2013 Survey on Medical Identity Theft, p. 5.
likely to withhold medical information. According to this study, more than 12 percent of respondents had withheld information from their provider because of security concerns. Federal government statistics indicate an even higher rate of withholding: compared to the overall population, individuals who strongly disagree that healthcare providers have reasonable protections in place for electronic health records are almost five times more likely to have withheld information from their provider (33 percent vs. seven percent).

This withholding impacts both patient care and public health:

Patients’ withholding medical information from healthcare professionals may not only impact negatively on the patient directly, but could also potentially compromise the health of others and the quality of healthcare surveillance systems. The consequences to the individual may range from relatively minor ones (such as missed opportunities for tobacco cessation counseling or treatment because of non-disclosure of smoking status) to more serious medical consequences (such as potential compromise in the timeliness, quality, and appropriateness of medical care). Patients with infectious, notifiable conditions who withhold all or part of necessary medical information . . . may inadvertently put the lives of others at increased risk. Furthermore, non-disclosure, underinformation or misinformation may jeopardize the data quality of healthcare surveillance systems. This is of significant public health concern, since such surveillance systems depend on accurate data to monitor existing and emerging trends in health outcomes and provide the basis for policy and population-based interventions.

Most adults are, naturally, interested in their providers’ health information practices. While the 2014 study has limitations, it indicates – and common sense dictates – that if a patient is concerned about the privacy and security of health records, he or she will be less likely to disclose sensitive health information. This, too, is a quality of care issue as well as a public health concern.

HEALTHIER DATA: IMPLEMENTING A SECURITY MANAGEMENT PROGRAM

Risk management is essential to every organization. While it is impossible to prevent every security incident and data breach, a security management program helps an
organization build a culture of concern, determine potential exposure, and appropriately manage risk to an acceptable level. This, in turn, contributes to better individual and community health outcomes by building patient trust and maintaining the integrity health records. A robust program also helps health organizations meet applicable state and federal standards, including those found in the HIPAA Privacy and Security Rules, and the Medicare and Medicaid EHR Incentive (“Meaningful Use”) Programs. Finally, a strong data management program can help businesses successfully resolve consumer complaints, limit audits, enforcement actions, and penalties by the Department of Health and Human Services Office for Civil Rights (“OCR”) (which enforces HIPAA) or the Federal Trade Commission (which enforces the prohibition against unfair and deceptive trade practices), and reduce liability under other applicable state and federal law.

*Reasonableness* is the cornerstone of both OCR’s and FTC's approach to data security. For example, FTC states that a business’s data security measures must be “reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.” Many aspects of a program are therefore flexible, and scalable to the specific needs of an individual organization. However, successful security management programs share key components.

In its 2015 *Guide to Privacy and Security of Electronic Health Information*, the Office of the National Coordinator for Health Information Technology (“ONC”) provides a sample approach for implementing a security management process in healthcare. While this approach does not address all the requirements of Meaningful Use or the HIPAA Security Rule, it provides a basic framework for compliance:

**STEP 1:** Establish a culture of compliance, select a team, and build a knowledge base.
This will include designating a security officer, using qualified professionals to assist with a risk analysis, and promoting an organization-wide culture of protecting privacy and securing PII.

**STEP 2:** Document the organization’s process, findings, and actions. These records will serve as an accurate record for the workforce, and will prove essential if the organization is subject to a compliance audit.

---

11 Health organizations may also have to comply with other privacy and security laws and requirements, including those in or promulgated by 42 CFR Part 2 (confidentiality of alcohol and drug abuse records), the Family Educational Rights and Privacy Act (FERPA), Title X of the Public Health Service Act, the Genetic Information Nondiscrimination Act (GINA), private-sector contracts, state law, state boards of medicine, state associations, etc.


STEP 3: Perform a Security Risk Analysis. The risk analysis assesses potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic PII. In general, the risk analysis will involve determining where electronic PII exists and how it is created, received, maintained, and transmitted (creation of a “data map”); identifying potential threats and vulnerabilities to the data; and evaluating risks and their associated levels – how likely it is that threats will exploit existing vulnerabilities, and how this will impact the confidentiality, integrity, and availability of data. The results will inform the organization’s risk management strategy.

STEP 4: Develop an action plan. This involves mitigating the potential risks identified by the Security Risk Analysis, focusing on high priority threats and vulnerabilities. The action plan should account for the organization’s characteristics and environment – and be feasible and affordable. The action plan should include administrative, physical, and technical safeguards, organizational standards, and policies and procedures.

STEP 5: Manage and mitigate risk. This involves implementing the action plan, educating and training the workforce, communicating with patients, and updating vendor contracts.

STEP 6: Monitor, audit, and update security on an ongoing basis. This involves both monitoring the adequacy and effectiveness of the security infrastructure and making needed changes, and maintaining retrospective documentation – such as an “audit log” – of who, what, when, where, and how PII has been accessed.

ONC also offers its “Top 10 Tips for Cybersecurity in Health Care,”14 generally applicable to organizations of all sizes:

1. Establish a security culture.
   • Build a security-minded educational culture so good habits and practices become automatic.
   • Conduct information security education frequently, on an ongoing basis.
   • Ensure managers and other leaders set a good example in attitude and action.
   • Make taking responsibility for information security a core organizational value.

2. Protect mobile devices.
   • Ensure mobile devices are equipped with strong authentication and access controls (ensure laptops have password protection, and enable password protection on mobile devices; take extra physical control precautions if password protection is not provided).
   • Protect wireless transmissions from intrusion.

• Do not transmit unencrypted protected health information across public networks.
• Encrypt data when it is necessary to commit health information to a mobile device, or remove a device from a secure area.
• Do not use mobile devices that cannot support encryption.
• Install and activate remote wiping and/or remote disabling.
• Disable and do not install or use file sharing applications.
• Install and enable security software, and keep it up-to-date.
• Research mobile applications before downloading.
• Maintain physical control: keep it with you or lock it in a secure location; lock the screen when not in use; do not let others use it.

3. Maintain good computer habits.

• Configuration management
  o Uninstall unessential software applications.
  o Use caution when accepting default or standard configurations when installing software.
  o Ask whether your electronic health record (“EHR”) developer maintains an open connection to installed software to provide updates and support – if so, ensure a secure connection at the firewall and request that this access be disabled when not in use.
  o Disable remote file sharing and remote printing within the operating system.

• Software maintenance
  o Automate software updates to occur regularly.
  o Monitor for critical and urgent patches and updates that require immediate attention, and act upon them as soon as possible.

• Operating system maintenance
  o Disable user accounts for former employees quickly and appropriately. Close access to the accounts of involuntarily terminated employees before serving notice of termination.
  o Before disposal, sanitize computers and other devices that have had data stored on them. The National Institute of Standards and Technology (“NIST”) publishes guidelines for disposal.
  o Archive old data files for storage if needed, or clean them off the system if not needed, subject to applicable data retention requirements.
  o Fully uninstall software that is no longer needed, including trial software and old versions of current software.
  o Work with your IT team or other resources to perform malware, vulnerability, configuration, and other security audits on a regular basis.
4. **Use a firewall.**
   - Unless the EHR is completely disconnected from the Internet, install a firewall to protect against outside intrusions and threats.
   - Large practices that use a Local Area Network (“LAN”) should consider a hardware firewall.

5. **Install and maintain anti-virus software.**
   - Use an anti-virus product that provides continuously updated protection against malware, viruses, and other code that attacks computers through web downloads, CDs, email, and flash drives.
   - Keep anti-virus software up-to-date.

6. **Plan for the unexpected.**
   - Create regular and reliable data backups.
   - Consider storing backup far from the main system.
   - Protect backup media with access controls.
   - Test backup media regularly for ability to properly restore data.
   - Have a sound recovery plan. Know what data was backed up, when backups were done, where backups are stored, and what equipment is needed to restore backups.
   - Keep the recovery plan securely and remotely, where an identified person has responsibility to produce it in an emergency.

7. **Control access to health information.**
   - Configure electronic records to grant access only to people with a need to know.
   - Set access permissions using an access control list. Before setting permissions, identify which files should be accessible to which staff members.
   - Configure role-based access as needed. In role-based access, a staff member’s role within the organization (for example: physician, nurse, billing specialist) determines what information he or she may access. Assign staff to the correct roles, and set access permissions for each role correctly, on a need-to-know basis.

8. **Use strong passwords and change them regularly.**
   - Choose passwords that wrongdoers cannot easily guess. For example, a strong password may be of a certain length (the longer the better), combining upper- and lower-case letters, and special characters such as punctuation marks.
   - Do not include personal information in passwords, such as birthdates, one’s own name or the names of family members or pets, Social Security numbers, or information on social networking sites or other locations that others could easily discover.
• Require multi-factor authentication, such as passwords plus fingerprint scans or randomly-generated PINs.
• Configure systems so that passwords must be regularly changed.
• Develop a password reset process to provide quick and easy assistance for forgotten passwords. This will discourage staff from writing down passwords.

9. **Limit network access.**

• Prohibit installation of software without prior approval.
• Set any wireless router to operate only in encrypted mode.
• Prohibit casual network access by visitors.
• Ensure that file sharing, instant messaging, and other peer-to-peer applications have not been installed without explicit review and approval.

10. **Control physical access.**

• Limit the opportunity for devices to be tampered with, lost, or stolen.
• Document and enforce policies limiting physical access to devices and information.

**CONCLUSION**

The security of PII is a quality of care issue. Patient concerns can impact disclosure of important health information, and breach of medical PII can lead – among other things – to medical identity theft, a mixed medical record, and physical harm to the patient. While electronic health records offer many benefits to patient care, they also offer new and complex avenues for breach. Wrongdoers recognize both the value of health data, and its ever-increasing availability. They will exploit vulnerabilities to obtain this data, regardless of the organization’s size or profile.

A robust security management program will guide organizations in identifying their own security holes and threat environment, and implementing a mitigation strategy to reduce potential harm to both the entity and its patients. Successful programs share key components, which may be mandated by applicable state or federal law, such as the HIPAA Security Rule. However, programs are also flexible, and scalable to the organization’s size and complexity, the amount of PII it holds, and available resources.

Because patient perception may impact disclosure and, thereby, quality of care, organizations should proactively communicate with patients about cybersecurity. Communications should emphasize that the organization places a priority on the security and confidentiality of PII, including health information. These communications should be culturally appropriate, and take into account any particular needs of the patient population.
Most importantly, the organization should back these communications with documented, ongoing efforts to achieve and maintain a culture of commitment to the privacy and security of patient data. By achieving compliance, health organizations can protect both themselves and their patients, and improve the quality of individual care and community health.