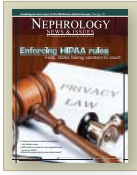
Part 2

HIPAA: Privacy, security and the consequences of a breach for dialysis providers

Tatiana Melnik • Ralph Levy, Jr.



Read Part 1 of this series in the September issue of NN&I at www.nephrologynews.com/magazine/2012

The first article in this two part series, published last month, reviewed the federal privacy and security laws governing patient data and the recent enforcement actions taken at the federal level against health care providers who have experienced data breaches. This article provides dialysis providers and nephrologists with recommendations to minimize their exposure to HIPAA and HITECH violations.

Why should providers be concerned about compliance with HIPAA and HITECH?

With increases in enforcement activity and enhanced scrutiny of compliance to protect patients and their privacy, dialysis providers and nephrologists should be concerned about the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). In addition, if a dialysis provider breaches the Conditions for Participation (CfCs) that apply to all federally compensated providers of dialysis services and that require protection of patient privacy and records, it faces loss of provider status with Medicare.

The authors are with the law firm of Dickinson Wright PLLC (www.dickinsonwright.com), and are based in Ann Arbor, Mich., and Nashville, Tenn., respectively.

Increased enforcement activity

Congress passed HIPAA in 1996. However, compliance with the Privacy Rule[1] for most covered entities was not required until April 14, 2003. Similarly, compliance with the Security Rule[2] was not required until April 20, 2005.[3] Even after the two rules went into effect, however, the privacy and security requirements of HIPAA were rarely enforced by the Department of Health and Human Services. In 2006, for example, The Wall Street Journal reported that while the United States Department of Health and Human Services received 23,896 complaints between April 2003 and November 30, 2006, "it has not yet taken any enforcement actions against hospitals, doctors, insurers, or anyone else for rule violations."[4] Similarly, while HIPAA does include criminal penalties, the first criminal conviction for violating HIPAA did not come until 2004, when a Seattle phlebotomist pleaded guilty to using a cancer patient's information to fraudulently obtain four credit cards.[5]

Since the enactment of HITECH, however, investigations and resulting enforcement activity have been on the rise. As discussed in more detail in part I of this series, the Office of Civil Rights (OCR), the division of HHS that is responsible for enforcing HIPAA and HITECH, has become much more active. To date, OCR has acted against a large insurance company, a clinic provider, a state agency, a large hospital system, and a physician's practice.[6] Similarly, state attorneys' general have also become active in this space, bringing actions against covered entities under both federal and state law. The Attorneys' General from the states of Connecticut, Massachusetts, Indiana, and Vermont have all taken action against covered entities.[7] Most recently,

1. As noted in Part I, "the Privacy Rule sets the standards for, among other things, who may have access to PHI." HHS, HIPAA Security Series: Security 101 for Covered Entities, Vol. 2, Paper 1, 4 (2007), available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf [hereinafter Security Series].
2. As noted in Part I, "the Security Rule sets the standards for ensuring that only those who should have access to [electronic PHI] will actually have access." Security Series at 4.
3. As used in this article, HIPAA refers collectively to the Health Insurance Portability and Accountability Act and the Privacy Rule and the Security Rule promulgated thereunder.
4. Theo Francis. Spread of records stirs fears of privacy erosion, Wall Street Journal, Dec. 28, 2006, available at http://old.post-gazette.com/pg/06362/749444-114.stm#ixzz242HBMpNa.
5. See Ian C. Smith DeWaal, Successfully Prosecuting Health Insurance Portability and Accountability Act Medical Privacy Violations Against Noncovered Entities, The United States Attorneys' Bulletin, vol. 55 no. 4 (July 2007), available at http://www.justice.gov/usao/eousa/foia_reading_room/usab5504.pdf.
6. For further discussion, please see Part I of this Series published in the September issue of Nephrology News & Issues.
7. See press release, Attorney General sues Health Net for massive security breach involving private medical records and financial information on 446,000 enrollees (Jan. 13, 2010), available at http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=453918; press release, South Shore Hospital to pay $750,000 to settle data breach allegations (May 24, 2012), available at http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html; press release, WellPoint's notification delay following data breach brings action by Attorney General's Office (Oct. 29, 2010), available at http://www.in.gov/portal/news_events/58723.htm; press release, Attorney General settles security breach allegations against health insurer (Jan. 18, 2011), available at http://www.atg.state.vt.us/news/attorney-general-settles-security-breach-allegations-against-health-insurer.php.

the Minnesota State Attorney General filed an action against a business associate, Accretive Health Inc., a debt collection company that works with several Minnesota hospitals. The Minnesota case represents the first time an enforcement action was taken against a business associate.[8] As part of the settlement agreement of this action, Accretive agreed to cease all operations in Minnesota by Nov. 1, 2012, is banned from all operations in the state for two years, and then, for the next four years, may re-enter the state only with the prior approval from the Attorney General.[9]

Protection of patients

Providers should also be concerned about compliance because they are privy to their patients' most private details, including their patients' mental health, types of medical procedures they have undergone, the types of illnesses they have, or their prescription history. Patients expect their doctors to protect their medical information because the disclosure of such information can stigmatize them and adversely impact their employment opportunities, availability of insurance, and feelings of self-worth.[10] Further, patient trust is an integral part of the doctor-patient relationship and patient health may be adversely affected if patients do not feel comfortable sharing their health care details. In a 2005 survey, for example, one out of eight respondents "reported that they had engaged in a behavior intended to protect his or her privacy, including taking such actions as avoiding their regular doctor, asking their doctor not to record their health information or to 'fudge' a diagnosis, paying out of pocket so as not to file an insurance claim and even avoiding care altogether."[11] As such, doctors need to take care to ensure that patient data is protected.

What are the costs of dealing with a data breach?

Addressing a data breach is generally quite costly and may threaten the survival of a provider's practice. As more providers transition to storing data electronically, data breach costs will increase because it becomes easier for providers to lose large amounts of data (e.g., losing a laptop or USB drive). Regardless of whether or not a governmental investigation ensues as a result of a data breach, a dialysis provider or nephrologist may incur one or more of the following costs:

- employee overtime and productivity loss
- engaging an outside vendor to investigate the breach
- reviewing affected records
- notifying patients
- credit monitoring services
- reporting the breach to the Office of Civil Rights
- pursuant to the data breach notification laws of several states,[12] reporting the breach to State Attorneys' General
- addressing federal and state inves-

HIPAA violations and penalties

HIPAA violation	Minimum penalty under HITECH	Maximum penalty under HITECH
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but the violation is corrected within 30 days of the date on which the person liable for the violation knew, or by exercising reasonable diligence would have known, that he/she violated HIPAA. **This penalty is mandatory**	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected. **This penalty is mandatory**	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

8. Press release, Attorney General Swanson sues Accretive Health for patient privacy violations (Aug. 19, 2012), available at http://www.ag.state.mn.us/Consumer/PressRelease/120119AccretiveHealth.asp.
9. Press release, Attorney General Swanson says Accretive will cease operations in the state of Minnesota under settlement of federal lawsuit (July 31, 2012), available at http://www.ag.state.mn.us/Consumer/PressRelease/07312012AccretiveCeaseOperations.asp.
10. See generally, Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin, The Value and Importance of Health Information Privacy, in Beyond the HIPAA privacy rule: Enhancing privacy, improving health through research (2009), available at http://www.nap.edu/openbook.php?record_id=12458&page=75.
11. Joy L. Pritts, The importance and value of protecting the privacy of health information: The roles of the HIPAA privacy rule and the common rule in health research, Nat'l Academy Sci. 6 (2008), citing Forrester Research for the California HealthCare Foundation, National Consumer Health Privacy Survey (CHCF 2005 Survey).
12. The breach notification laws of Massachusetts, Louisiana, and Indiana, for example, require that data breaches be reported to the State Attorney General under certain circumstances. See Mass. Gen. Ch. 93H, § 3; La. Rev. Stat. § 51:3071 et seq.; Ind. Code § 4-1-11 et seq.; § 24-4.9-1 et seq.

tigations into a security breach
- paying federal and state fines and investigation settlement costs
- class action lawsuits
- remediation steps (e.g., upgrading security, revising manuals, training, etc.)
- reputation damage and loss of patient trust
- legal cost

It is important that dialysis providers and nephrologists understand that the HITECH Act imposes mandatory data breach penalties that are only avoidable under certain circumstances. For example, the secretary is prohibited from imposing civil monetary penalties if the violation is corrected "during the 30-day period beginning on the first date the person liable for the penalty or damages knew, or by exercising reasonable diligence would have known, that the failure to comply occurred."[13] HIPAA violations that are "due to willful neglect" are subject to a mandatory penalty of at least $10,000 per violation even if they are corrected during the 30-day discovery and cure period described above and at least $50,000 per violation if they are not corrected in a timely manner.

HITECH provides the HHS Secretary with discretion to determine the amount of the penalty based on the "nature and extent of the [HIPAA privacy or security] violation and the nature and extent of the harm resulting from such violation."[14] The penalties are not unlimited—Congress did set a maximum annual penalty of $1.5 million.

With the various costs involved in addressing a data breach, the Ponemon Institute estimated that, during 2011, organizations—both in and outside health care—incurred approximately $194 per compromised record to address a data breach.[15] In a separate 2011 study, the Ponemon Institute estimated that on average the cost to a health care organization to address a data breach was approximately $2,243,700,[16] with an average of $249,290 being spent on legal fees "to resolve data breaches and other privacy violations."[17]

Minimizing your exposure

Although as discussed above, it is generally very expensive to address data breaches, dialysis providers and nephrologists can take several steps to protect against a breach in order to minimize their exposure to data breach-related liabilities. These actions are yet another example that "an ounce of prevention" is far less costly than "a pound of cure."

HIPAA risk analysis

As the first step of any data security management process,[18] each health care provider should conduct a HIPAA risk analysis. As the "foundational element in the process of achieving compliance,"[19] through this risk analysis, providers "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by" such practice.[20]

There is no one right way to conduct a risk analysis and the steps providers take will vary with the size of their practice.[21] Providers may consider an approach set out by the National Institute of Standards, which is summarized below in modified form:[22]

1. **Identify**—The first step in any risk analysis is to identify all instances of electronic protected health information (ePHI) that the provider handles. Specifically, providers should consider where ePHI is created, received, maintained, processed, or transmitted.
2. **Trace**—The second step is to trace how the ePHI moves through the provider's practice, including transfer to mobile devices and remote access availability by employees and vendors. For dialysis providers, this part of the analysis should include the tracing of information flow of machine and patient-related data that is generated by dialysis machines, either for each patient treatment or as part of routine or other required machine maintenance.
3. **Threats and vulnerabilities**—Third, at each step of the trace, the provider should identify all of the threats and vulnerabilities to the ePHI.

13. 42 USC § 1320d–5(b)(2)(A) (emphasis added).
14. 42 USC § 1320d–5(a).
15. See Ponemon Institute LLC, 2011 Cost of data breach study 5 (2012), available at http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf.
16. Ponemon Institute, second annual Benchmark Study on Patient Privacy & Data Security (2011) [hereinafter Ponemon Study].
17. Ponemon Study at 14.
18. 42 C.F.R. § 164.308(a)(1)(i).
19. HHS, OCR, Guidance on risk analysis requirements under the HIPAA Security Rule 2 (July 12, 2010), available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.
20. 42 C.F.R. § 164.308(a)(1)(ii).
21. For guidance, see Dept. of Health & Human Services, Office of the Nat'l Coordinator for Health Information Technology, Guide to Privacy and Security of Health Information, Version 1.1 022312 (2012), available at http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf; U.S. Dept. of Commerce, Nat'l Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (2008), available at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf [hereinafter NIST Report].
22. NIST Report at E-3.

For example, if a particular practice permits employees to access data on mobile devices, then a threat would be that a breach can occur if the mobile device is lost. Dialysis providers should adopt specific policies as to the "wiping" of treatment and other patient-related information contained in dialysis machines that are repaired offsite or that are replaced once they no longer function properly or are disposed of by the provider.

4. Mitigation—Fourth, as each threat is identified, providers need to describe how they currently mitigate the threat and whether the current controls do in fact minimize or eliminate the threat. So, with respect to the mobile device example, an option would be to configure the mobile devices that have access to a practice's network to be remotely wiped if they are lost. For dialysis providers, "data wiping" policies and procedures may need to be adopted and implemented for the repair and replacement of dialysis machines.

5. Likelihood and effect—Fifth, for each threat identified, providers need to determine the likelihood that the contemplated security risk will occur and the effect such a security risk will have on the provider. These risks should be prioritized based on effect.

6. New controls—Sixth, providers should recommend and implement new controls if necessary. New controls should be reasonable and appropriate to the particular provider's practice. In deciding what is reasonable and appropriate, providers can consider i) their size, complexity, and capabilities; ii) their technical infrastructure, hardware, and software security capabilities; iii) the costs of security measures; and iv) the probability and criticality of potential risks to ePHI.[23]

7. Documentation—Seventh, providers must document the results and explain why certain controls were not implemented or why one type of control was selected over another.[24]

This risk analysis is to be performed on an as needed basis.[25] Thus, for example, in a recent action against an insurance company, OCR found it problematic that the insurer did not perform a risk analysis when it relocated its facility.[26] Other circumstances that may indicate that a risk analysis is needed include adding new hardware, upgrading software systems, and hiring a new vendor.

Internal policies and employment training

HIPAA provides regulated entities with broad flexibility in devising the best method(s) that will permit them to comply with the HIPAA requirements. Similarly, while providers must "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations,"[27] HIPAA does not define 'policy' or 'procedure.' As such, HIPAA permits providers to develop policies and procedures to fit their culture. HIPAA does set forth a number of policies that are required including, for example, an employee sanction policy, a security incident response and reporting policy, a data breach notification policy, a data backup plan and a disaster recovery plan.[28]

We noted in the first article in this series that the requirements imposed by the CfCs for patient data are less restrictive than those imposed by HIPAA. Therefore, dialysis providers should make sure that when they adopt, implement, and internally monitor HIPAA policies, compliance efforts should also meet the more stringent requirements of the CfCs.

HIPAA also makes clear that it is the provider's responsibility to ensure that its workforce complies with the security requirements.[29] Workforce is broadly defined to include "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for [an] entity, is under the direct control of such entity, whether or not they are paid by the [...] entity."[30] This means that providers must train their workforce members on the policies and procedures. In a recent action against a provider, for example, OCR discovered that the practice used text messages to transmit ePHI.[31] As part of the remediation, OCR required that the practice develop (i) a risk management plan that implements "security measures sufficient to reduce risks and vulnerabilities to ePHI to a reasonable and appropriate level for ePHI in text messages;" (ii) "[t]echnical security mea-

23. 45 CFR § 164.306(b); Security Series at 7.
24. See 45 CFR § 164.306(d)(3)(ii) ("If implementing the implementation specification is not reasonable and appropriate – 1) Document why it would not be reasonable and appropriate to implement the implementation specification; and 2) Implement an equivalent alternative measure if reasonable and appropriate.")
25. See generally 45 CFR. §§ 164.306(e) and 164.316(b)(2)(iii).
26. See Resolution Agreement, Section I(2)(B) (March 13, 2012), available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution_agreement_and_cap.pdf.
27. 45 CFR § 164.308(a)(1)(i).
28. See generally 45 CFR § 164.308. The data breach notification policy is required under HITECH.
29. See 45 CFR § 164.306(a)(4).
30. 45 CFR § § 160.103.
31. Resolution Agreement, Section I(2)(C) (April 13, 2012), available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf [hereinafter Phoenix Cardiac Surgery].