

NEPHROLOGY

NEWS & ISSUES

Balancing Economics & Quality in Renal Care

Enforcing HIPAA rules

Feds, states taking violators to court



PRIVACY
LAW

- Fresenius launches internal investigation into bribery cases
- CMS listens to ideas for new integrated care model for ESRD
- Should the renal diet be more plant-based?

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

Tatiana Melnik • Ralph Levy, Jr.

Recently, enhanced enforcement actions and privately filed class actions have occurred based on alleged violations of state and federal laws and regulations that impose security and confidentiality requirements for patient medical records and other confidential data. These actions should be of interest to providers of dialysis services, businesses that provide administrative, billing, and other support services to these providers, and nephrologists and other members of the renal care team. Such violations can jeopardize Medicare eligibility for dialysis providers, and disallow them from billing Medicare for services provided. This article is the first of a two-part series that provides those affected by data security and patient privacy laws with additional information about these laws and recently stepped up enforcement efforts. We will address several issues:

What is the purpose of the law, what legal requirements are imposed, and what actions are prevented?

What are some examples of how nephrologists and dialysis providers are affected by the law, and what are the consequences of violating the law?

How can providers and other health care professionals make sure they comply with the laws?

The second article in this series will address how dialysis providers and nephrologists can minimize exposure to violations of these laws.



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.

Understanding privacy and security laws governing patient health

What is the purpose of the law? What legal requirements are imposed; what actions are prevented?

One of the first privacy laws impacting health care was the Health Insurance Portability and Accountability Act of 1996 (HIPAA),¹ a primary goal of which was to improve the efficiency and effectiveness of the health care system by, for example, standardizing the electronic exchange of administrative and financial data.² In enacting HIPAA, Congress recognized that, “[h]ealth information is considered relatively ‘safe’ today, not because it is secure, but because it is difficult to access,”³ and the transition to electronic exchange would make health information easier to access. As such, Congress directed the Secretary of Health and Human Services to adopt privacy and security standards aimed at protecting health information. As adopted by the secretary, these rules are called the Privacy Rule and the Security Rule and are both administered and enforced by the Office of Civil Rights (OCR).⁴

Sixteen years after its enactment of HIPAA, Congress further strengthened the privacy and security requirements when it passed the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act of 2009.⁵ In acting to impose stronger privacy and security protections in health care in this manner, Congress responded to concerns over lack of enforcement of HIPAA and continued ongoing concerns based on the growth of electronic health records.⁶ To encourage increased HIPAA compliance and enforcement, the HITECH Act provides for mandatory

breach notification, a tiered civil penalty structure, and grants state Attorneys General the right to enforce HIPAA on behalf of their state citizens. As required by the HITECH Act, the Secretary issued a Breach Notification Rule, which became effective on Sept. 23, 2009,⁷ and it is also enforced by OCR. As such, the HITECH Act increases the financial risks for organizations handling protected health information, or PHI, who are not in compliance with HIPAA.

The Centers for Medicare & Medicaid Services confirmed the applicability of HIPAA to dialysis facilities in its April 15, 2008 release of the final Conditions for Coverage for End-Stage Renal Disease Facilities.⁸ As a result, dialysis providers should be concerned that if they violate HIPAA (and presumably the HITECH Act as well⁹), their ability to bill Medicare for dialysis services provided could also be jeopardized.

What are some examples of how nephrologists and dialysis providers are affected by the law, and what are the consequences of violating the law?

Since the enactment of HITECH and, importantly, its requirement for public disclosure of breaches that affect 500 or more individuals, enforcement activity has increased on several fronts, including actions by OCR, State Attorneys General,²⁷ and class action lawsuits.²⁸ To date, OCR has taken six actions, none of which involved violations by dialysis providers or nephrologists.

Case 1

On Feb. 4, 2011, OCR imposed a \$4,351,600 civil money penalty against Cignet Health of Prince George’s County,

[HIPAA, continued on page 28]

1. Pub. L. 104-191, 110 Stat. 1936 [hereinafter HIPAA Law], available at <http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html>, which was signed into law on August 21, 1996.
2. See id. at § 261, which indicates that the purpose of Title II of HIPAA is ‘Administrative Simplification.’
3. H.R. Rep. No. 104-496 Part 1, at 99 (1996), available at <http://www.gpo.gov/fdsys/pkg/CRPT-104hrpt496/pdf/CRPT-104hrpt496-pt1.pdf>.
4. See generally Dep’t of Health and Human Services (“HHS”), Health Information Privacy, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html> (last visited June 25, 2012), The Privacy Rule and the Security Rule are found at 45 CFR Part 160 and Part 164, Subparts A, C, and E.
5. Public Law 111-5, 123 Stat. 115 [hereinafter the HITECH Act], available at <http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf>.
6. For example, during the Senate Hearings that preceded the passage of HITECH, the Senate heard testimony noting that, “strong privacy protections must be part of any legislation that moves health IT.” S. Hrg. 111-213, Serial No. J-111-3 (Jan. 27, 2009), Statement of Deven McGraw, Director, Health Privacy Project, Center for Democracy and Technology.
7. The Breach Notification Rule is an Interim Final Rule. The Secretary has clarified that until the final breach notification rule is published, the Interim Final Rule is in effect. See HHS, Breach Notification Final Rule Update, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html> (last visited June 25, 2012).
8. The final Conditions for Coverage as released on April 15, 2008 can be found at 73 Fed. Reg. 20369. In the preamble to the CfCs, CMS indicated that “HIPAA requirements protecting patient privacy apply to dialysis facilities”. Specifically, 42 CFR §494.70(a)(4) provides that the patient has the right to “[p]rivacy and confidentiality in personal medical records”.
9. The CfCs provide that “[t]he facility and its staff must operate and furnish services in compliance with applicable Federal, State, and local laws pertaining to licensure and any other relevant health and safety requirements.” 42 CFR §494.20.
27. For example, the Attorneys General of Connecticut, Indiana, Vermont and Minnesota have undertaken enforcement activities.
28. There are a number of class actions currently in California against, for example, Sutter Health, Sutter Medical Foundation and Sutter Physician Services as well as one in Michigan against the Henry Ford Health System. The lawsuits are based on violations of state law because neither HIPAA nor HITECH provide a private cause of action.

The privacy, security, and breach notification rules

The HIPAA Privacy, Security, and Breach Notification rules deal with protecting individuals' medical records and other personal health information, called protected health information (PHI). "[T]he Privacy Rule sets the standards for, among other things, who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to [electronic PHI] will actually have access."¹⁰

The rules apply to "covered entities" and their business associates.¹¹ Covered entities include health care providers.¹² As such, the rules apply directly to dialysis providers and nephrologists and require, among other things, that they enter into business associate agreements which provide satisfactory assurances that such business associates comply with HIPAA.¹³ The Privacy Rule and Breach Notification Rules apply to PHI in any form or media, whether electronic, paper, or oral.¹⁴ The Security Rule, on the other hand, applies to PHI that is in electronic form.

The definition of PHI is quite broad and includes information that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care

to an individual ... [t]hat identifies the individual" or could be used to identify the individual.¹⁵

The Privacy Rule

The Privacy Rule, among other things, sets limits and conditions on the uses and disclosures that dialysis providers and nephrologists may make of PHI without requesting written patient authorization. It provides patients with rights over their PHI. The Privacy Rule also requires that dialysis providers and nephrologists train their workforce members; implement appropriate administrative, technical, and physical safeguards to protect the PHI and ePHI as set forth in the Security Rule; and apply appropriate sanctions against workforce members who violate the privacy policies and procedures. Between April 2003 and September 2011, HHS received more than 64,000 complaints regarding violations of the Privacy Rule¹⁶ and one of the first actions under HITECH involved an organization that failed to provide patients with copies of their records. Similar but less specific restrictions can be found in the Conditions for Coverage.¹⁷

The Security Rule

As noted above, the Security Rule

applies to PHI that is in electronic form and requires that organizations assess their compliance with the HIPAA administrative safeguards, physical safeguards, and technical safeguards. This assessment is done through a risk analysis, which is the "foundational element in the process of achieving compliance."¹⁸ Thus, dialysis providers and nephrologists do not need to implement all Security Rule requirements. However, HHS made it clear that if they choose not to implement a requirement "based on [their] assessment, [they] must document the reason and, if reasonable and appropriate, implement an equivalent alternative measure."¹⁹ The risk analysis is part of the security management process, which includes establishing policies and procedures to prevent, detect, contain, and correct security violations. In addition to the risk analysis, this process also requires dialysis providers and nephrologists to undertake risk management, a sanction policy, and an information system activity review. The Conditions of Coverage impose similar requirements on dialysis providers in regard to security of patient information.²⁰

[OVERVIEW, continued on page 29]

10. 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>.
11. Business associates are entities that perform certain functions on behalf of covered entities, where such functions involve "the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis" or provided certain services such as "management, administrative, accreditation, or financial services . . . , where the provision of the service involves the disclosure of individually identifiable health information." 45 C.F.R. §160.103.
12. See *id.*
13. See e.g., 45 C.F.R. §§164.314(a) and 164.504(e).
14. See *id.* See also the definition of protected health information, which means individually identifiable health information "that is: (i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium." *Id.*
15. See *id.*
16. Leon Rodriguez, Director Office for Civil Rights, Testimony Before the Committee on the Judiciary Subcommittee on Privacy, Technology and the Law United States Senate (Nov. 9, 2011), available at <http://www.judiciary.senate.gov/pdf/11-11-9RodriguezTestimony.pdf>.
17. The preamble to the CfCs indicate that "[p]atients have the right to look at their own medical record," 73 Fed. Reg. 20431 (2008).
18. 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>.
19. HHS, HIPAA Security Series: Security 101 for Covered Entities, Vol. 2, Paper 1, 5 (2007), available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf>.
20. The CfCs require that dialysis facilities protect the patient's medical record, including a specific requirement to safeguard the record from "loss, destruction, or unauthorized use" and to "[k]eep confidential all information contained in the patient's record", 42 CFR §§494.170(a)(1) and (2).

[OVERVIEW, continued from page 27]

The Breach Notification Rule

Upon notice or discovery of a breach²¹ of unsecured PHI, the HITECH Act requires dialysis providers and nephrologists (or their business associate) to 1) investigate the circumstances of the breach, 2) give notice of the breach to the impacted individuals (or to the covered entity if by business associate), 3) reprimand the individual or organization that committed the breach, and 4) notify the secretary of HHS. If the breach impacts more than 500 individuals, notice must be provided to individuals, media, and the secretary “without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach,”²² and the organization’s name is posted

on an online “wall of shame.”²³ As of this writing, this list included 477 breach reports.

Importantly, HITECH provides that “a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person ... that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.”²⁴ HHS has clarified that knowledge of a breach by a covered entity’s workforce member or an agent, such as a business associate, is imputed to the covered entity for purposes of breach notification requirements.²⁵

Dialysis providers and nephrologists must ensure that they “implement reasonable systems for discovery of breaches” because they are “liable for failing to provide notice of a breach when [they] did not know—but by exercising reasonable diligence would have known—of a breach.”²⁶ Additionally, if dialysis providers and nephrologists are working with business associates, they should update their agreements to reflect the 60-day notice requirement because the 60-day notification clock starts running when the business associate discovers, or should have discovered the breach, and not when the business associate notifies the covered entity.

[HIPAA, continued from page 27]

Md., for HIPAA Privacy Rule violations.²⁹ OCR received complaints from 41 patients alleging that Cignet denied them access to their medical records between September 2008 and October 2009. Cignet never produced records related to the investigation to OCR, forcing OCR to go to the U.S. District Court for relief.³⁰ OCR found that Cignet was willfully negligent for failing to cooperate, and assessed Cignet a \$1.3 million penalty for failing to comply with the Privacy Rule and a \$3 million penalty for failing to cooperate with its investigation.

Case 2

On Feb. 14, 2011, OCR settled potential violations of the HIPAA Privacy Rule for \$1 million with General Hospital Corporation and Massachusetts General Physicians

Organization, Inc. (collectively, “Mass General”).³¹ OCR’s investigation of Mass General began when a patient complained that, on March 9, 2009, the hospital lost the PHI of 192 patients, including patients with HIV/AIDS, when an employee left documents containing PHI on a subway. OCR found that “Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General’s premises” and required the hospital to develop written policies addressing physical removal and transport of PHI as well as laptop and USB drive encryption.³²

Case 3

On July 6, 2011, OCR settled potential violations of the HIPAA Privacy and Security Rules for \$865,500 with the

21. A breach is “the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” HITECH Act, supra note 6, at § 13400.

22. *Id.* at § 13402(d).

23. See HHS, Breaches Affecting 500 or More Individuals, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

24. *Id.* at § 13402(c) (emphasis added).

25. Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 74 Fed. Reg. 42749 (Aug. 24, 2009) (“these provisions attribute knowledge of a breach by a workforce member or other agent (other than the person committing the breach), such as certain business associates, to the covered entity itself. Thus, covered entities should ensure their workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so.”)

26. *Id.*

29. Press Release, HHS, Cignet Health Fined a \$4.3M Civil Money Penalty for HIPAA Privacy Rule Violations (Feb. 22, 2011), available at <http://www.hhs.gov/news/press/2011pres/02/20110222a.html>.

30. See *id.*

31. See Corrective Action Plan, Corrective Action Obligations, 3 (Feb. 14, 2011), available at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralracap.pdf>.

32. See *id.* at 3.

University of California at Los Angeles Health System.³³ OCR's investigation was triggered by two complaints filed by celebrity patients in June 2009, alleging that the hospital's employees repeatedly looked at their information without a permissible reason. OCR found numerous violations between 2005 and 2009, including workforce members who repeatedly and without a permissible reason examined the ePHI of patients; showed a lack of workforce training; and failed to "implement security measures sufficient to reduce the risks of impermissible access to [ePHI] by unauthorized users to a reasonable and appropriate level."³⁴ OCR explained that, "[e]mployees must clearly understand that casual review for personal interest of patients' protected health information is unacceptable and against the law."³⁵

Case 4

The next OCR settlement announcement happened on March 13, 2012, when OCR announced settlement of potential violations of the HIPAA Privacy and Security Rules for \$1.5 million with Blue Cross and Blue Shield of Tennessee ("BCBST").³⁶ OCR's investigation was triggered when BCBST submitted a breach notification report in accordance with HITECH after a BCBST employee discovered that 57 hard-drives were stolen from a data closet in October 2009.³⁷ OCR found that BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. That is, BCBST failed to perform a risk assessment when it moved its facility.

Case 5

OCR has also taken direct action against physicians. On April 13, OCR settled potential violations of the HIPAA Privacy and Security Rules for \$100,000 with Phoenix Cardiac Surgery, P.C., a provider of cardiothoracic surgery physician services.³⁸ OCR began its investigation in February 2009 when it received a complaint alleging that Phoenix impermissibly disclosed ePHI by making it

publicly available on the Internet through an unsecured Internet-based calendar and e-mail. OCR found numerous violations between 2005 and 2009, including, for example, Phoenix failing to identify a security official, failing to conduct a risk analysis, failing to train its workforce, and failing to enter into Business Associate Agreements with the companies providing the Internet-based calendar and e-mail systems. OCR noted that, "[t]his case is significant because it highlights a multi-year, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules."³⁹

“OCR's investigation of Mass General began when a patient complained that, on March 9, 2009, the hospital lost the PHI of 192 patients, including patients with HIV/AIDS, when an employee left documents containing PHI on a subway.”

Case 6

Most recently, OCR took action against a state agency. On June 25, 2012, OCR settled potential violations of the HIPAA Privacy and Security Rules for \$1.7 million with the Alaska Department of Health and Human Services (DHHS).⁴⁰ Similar to the BCBST incident, this investigation was also triggered when DHHS submitted a breach report, as required by HITECH, disclosing that a USB drive was stolen from an employee's car in October 2009. OCR determined that DHHS failed to 1) complete a risk analysis; 2) implement sufficient risk management measures; 3) complete security training for its workforce; 4) implement device and media controls; and 5) address device and media encryption.

NN&I

33. Press Release, HHS, UCLA Health System Settle Potential Violations of the HIPAA Privacy and Security Rules (July 7, 2011), available at <http://www.hhs.gov/news/press/2011pres/07/20110707a.html>.

34. Resolution Agreement Section I(2)(B) (July 6, 2011), available at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/uclahsracap.pdf>.

35. See Press Release, *supra* note 33.

36. Press Release, HHS, HHS settles HIPAA case with BCBST for \$1.5 million (March 13, 2012), available at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/bcbstagrmt.html>.

37. 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.

38. Resolution Agreement, Section I(2)(C) (April 13, 2012), available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf.

39. Press Release, HHS, HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards (April 17, 2012), available at <http://www.hhs.gov/news/press/2012pres/04/20120417a.html>.

40. See Resolution Agreement with DHHS, Section I(3) (June 26, 2012), available at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.pdf>.