Bloomberg BNA

BNA's
Health Law Reporter™

HIPAA Settlement With Community Pharmacy Highlights Best Practices For the Handling and Disposal of Paper PHI

BY MICHAEL A. DOWELL

On April 27, 2015, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) announced a resolution agreement and settlement with a small, single-location pharmacy arising from alleged violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. In the resolution agreement, the pharmacy agreed to pay a $125,000 settlement and to enter into a two-year corrective action plan to correct deficiencies in its HIPAA compliance program.[1]

HIPAA applies to organizations and individuals who submit health care reimbursement claims electronically. Since the majority of pharmacies and pharmacists submit claims electronically, they are covered entities under the HIPAA Privacy and Security Rules (the rules) and are required to protect the confidentiality of protected health information (PHI)[2] and have a number of legal obligations under the rules. Many pharmacy records meet the definition of PHI, including prescription records, prescription labels, billing records, patient profiles, and counseling records. Thus, pharmacies must protect such records as required by the rules.

Cornell Prescription Pharmacy provides in-store and prescription services to patients in the Denver, Colo., metropolitan area, and specializes in compounded medications and services for hospice care agencies in the area. In January 2012, the HHS Office for Civil Rights (OCR) initiated a compliance review and investigation of the pharmacy following receipt of a television news report that the pharmacy had disposed of unsecured hard copy protected health information (PHI) of 1,610 patients in an unlocked open dumpster. The documents were not shredded and contained identifiable information regarding specific patients. As a result of the investigation, OCR concluded that the pharmacy failed to reasonably safeguard PHI; failed to implement written HIPAA Privacy policies and procedures; and failed to provide training on HIPAA Privacy Rule policies and procedures for the members of its workforce.[3]

In the OCR press release announcing the resolution agreement and settlement, OCR Director Jocelyn Samuels stated that, ''Regardless of size, organizations cannot abandon protected health information or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons. Even in our increasingly electronic world, it is critical that policies and procedures be in place for secure dis-

[1] ''HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records,'' HHS Press Release, April 27, 2015, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cornell/cornell-press-release.html.

Michael A. Dowell is a partner and member of the Health Care Law Group in the Los Angeles office of Hinshaw & Culbertson LLP. He counsels pharmacies, pharmaceutical manufacturers, wholesalers, pharmacy benefit management companies, Medicare Part D plans, drug wholesalers, drug and dietary supplement manufacturers, and retail medical oxygen dealers on licensure, pharmacy regulation, contracts, acquisitions and sales, and HIPAA privacy and security compliance, among other matters. He can be reached at mdowell@hinshawlaw.com.

[2] HIPAA refers to the Administrative Simplification subtitle, Title II Subtitle F of the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) (Aug. 21, 1996), and the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), and Title XIII Division A and Title IV Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111–5) (Feb. 17, 2009). The regulations published under these laws include: the Privacy Rule, 45 C.F.R. Parts 160 Subpart A and 164 Subpart C, originally published in 2000; the Security Rule, 45 C.F.R. Parts 160 Subpart A and 164 Subpart A, originally published in 2003; and the ''Breach Notification Rule,'' Parts 160 Subpart A and 164 Subpart D, originally published in 2009.

[3] Id.

 ISSN 1064-2137

posal of patient information, whether that information is in electronic form or on paper.''[4]

Although the HIPAA Privacy Rule has been in place for more than 12 years, the pharmacy settlement demonstrates that there are covered entities and business associates that are not fully compliant with applicable provisions of the rules, and have not provided HIPAA Privacy Rule training to their workforce members. The pharmacy settlement follows a recent Safeway $9.9 million settlement with California district attorneys for unlawful disposal of pharmacy customer confidential medical information and hazardous waste[5], and similar OCR settlements with CVS Pharmacy for $2.25 million in 2009 for failure to properly dispose of labels from prescription bottles and old prescriptions, and Rite Aid for $1 million in 2010 for the pharmacy's failure to safeguard the privacy of its customers when disposing of identifying information on pill bottle labels and other health information.[6]

Pharmacy Corrective Action Plan Obligations

The corrective action plan (CAP) requires the pharmacy to develop and implement a comprehensive set of policies and procedures to comply with the HIPAA Privacy Rule; to train its workforce in those policies and procedures; and to appropriately document such training. The CAP also sets minimum standards for the content of the policies and workforce training. The pharmacy is required to file a copy of its CAP implementation plan with OCR within 60 days, and to submit annual reports that include workforce member certifications and officer attestations.[7] The CAP obligations are further described below.

Policies and Procedures. The pharmacy must develop, maintain, and revise, as necessary, written policies and procedures to comply with the federal standards that govern the privacy of individually identifiable health information[8]. The pharmacy policies and procedures must include, but not be limited to, the minimum content set forth below. The pharmacy must provide the policies and procedures to HHS within 30 days of the settlement date for review and approval. The pharmacy must adopt and begin implementation of such policies and procedures within 30 days of receipt of HHS's approval.[9]

Distribution and Updating of Policies and Procedures. The pharmacy must distribute the policies and procedures to all members of its workforce within 30 days of HHS approval of such policies and procedures and to new members of the workforce within 30 days of their beginning of service. In addition, the pharmacy must require, at the time of distribution of such policies and procedures, a signed written or electronic initial compliance certification from each member of the workforce, stating that the workforce member has read, understands, and shall abide by such policies and procedures. The pharmacy must assess and update and revise, as necessary, the policies and procedures at least annually, and provide such revised policies and procedures to HHS for review and approval. Within 30 days of the effective date of any approved, substantive revisions, the pharmacy must distribute such revised policies and procedures to all members of its workforce, and to new members as required above, and must obtain new compliance certifications. The pharmacy is prohibited from involving any member of its workforce in the use or disclosure, including disposal, of PHI if that workforce member has not signed or provided the required written or electronic certification.[10]

Minimum Content of the Policies and Procedures. The pharmacy policies and procedures must include, but not be limited to:

1. Administrative and physical safeguards for the disposal of all non-electronic PHI that appropriately and reasonably safeguard such PHI from any use or disclosure in violation of the Privacy Rule and that limit incidental uses and disclosures, including, but not limited to, providing that paper PHI intended for disposal shall be shredded, burned, pulped, or pulverized so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

2. Measures that address the following Privacy Rule provisions: a. Uses and disclosures of PHI;[11] b. Safeguards;[12] c. Training;[13] and d. Internal Reporting Procedures–The pharmacy must require all members of its workforce to report to the designated privacy officer at the earliest possible time, any violation of the policies and procedures of which she or he is aware.

3. Measures providing that upon receiving information that a member of its workforce may have violated these policies and procedures, the pharmacy must promptly investigate and address the violation in an appropriate and timely manner.

4. Application of appropriate sanctions (which may include re-training or other instructive corrective action, depending on the circumstances) against members of the pharmacy's workforce, including supervisors and managers, who fail to comply with the pharmacy policies and procedures.[14]

---

[4] Id.

[5] Safeway to pay nearly $10 million in hazardous waste settlement, Los Angeles Times, Jan. 5, 2015, http://touch.latimes.com/#section/-1/article/p2p-82458386/

[6] Annual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance for Calendar Years 2009 and 2010 as Required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 111-5, Section 13424, submitted to the Senate Committee on Health, Education, Labor, and Pensions, House Committee on Ways and Means, and House Committee on Energy and Commerce, U.S. Department of Health and Human Services Office for Civil Rights; http://www.hhs.gov/ocr/privacy/hipaa/enforcement/complianceрept.pdf.

[7] Cornell Prescription Pharmacy Resolution Agreement with the U.S. Department of Health and Human Services Office for Civil Rights, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cornell/cornell-cap.pdf

[8] 45 C.F.R. Part 160 and Subparts A and E of Part 164, the Privacy Rule.

[9] Note 6, supra.

[10] Id.

[11] 45 C.F.R. § 164.502(a).

[12] 45 C.F.R. § 164.530(c)(1).

[13] 45 C.F.R. § 164.530(b)(1).

[14] Id.

  HLR ISSN 1064-2137

Training. All members of the pharmacy's workforce must receive training on the pharmacy's policies and procedures to comply with the Privacy Rule within 30 days of the implementation of the policies and procedures, or within 30 days of when they become a member of the workforce of the pharmacy. At a minimum, training must cover all of the topics that are necessary and appropriate for each member of the workforce to carry out that workforce member's function within the pharmacy. Each pharmacy workforce member must certify, in writing or in electronic form, that she or he has received and understands the required training. The training certification must specify the date on which training was received. The pharmacy must review the training annually, and, where appropriate, update the training to reflect changes in federal law or HHS guidance, any issues discovered during internal or external audits or reviews, and any other relevant developments the pharmacy is prohibited from involving any member of its workforce in the use or disclosure, including disposal, of PHI if that workforce member has not provided the required written or electronic training certification.[15]

Reportable Events. In the event that a workforce member may have failed to comply with the pharmacy's policies and procedures or otherwise there may have been a violation of the HIPAA Privacy Rules, the pharmacy is required to promptly investigate the matter. If the pharmacy determines, after review and investigation, that a member of its workforce has failed to comply with its policies and procedures or that there has otherwise been a violation of the HIPAA Rules, the pharmacy must notify HHS in writing within 30 days. The report to HHS must include a complete description of the event, including the relevant facts, the persons involved, and the provision(s) of the pharmacy's policies and procedures or HIPAA Rules implicated; and description of the actions taken and any further steps the pharmacy plans to take to address the matter, to mitigate any harm, and to prevent it from recurring, including the application of appropriate sanctions against workforce members who failed to comply with its policies and procedures or otherwise violated the HIPAA Rules. [16]

Unique Aspects of Paper PHI Handling, Storage and Disposal for Pharmacies and Other Health Care Organizations

Health care organizations have always grappled with the development of effective strategies for secure handling, storage, and disposal of PHI. The biggest problem is the volume of paper PHI in most health care organizations. Another issue is the fact that the size and nature of many health care organizations require a large number of employees with significant employee turnover. There is plenty of room for human error in dealing with the volume of paper PHI and the large number of employees. Ninety-nine percent daily compliance at many health care organizations could still result in 10 or more daily data breaches. What level of compliance is enough?

Why Data Disposal is Important for Health Care Organizations. Reports have shown that medical identity theft is on the rise. Identity thieves and cybercriminals have made health care PHI the most common data breach as they view medical records as particularly valuable because they include names, addresses, dates of birth, telephone numbers, employer, Social Security numbers, and bank account/credit card information. The disclosure of PHI may cause reputational harm and result in stigma, embarrassment, and discrimination because that private information is known by others. PHI disclosure may also result in economic harm as individuals could lose their job, health insurance, or housing if the wrong type of information becomes public knowledge. Individuals could also experience economic harm as the victims of medical or financial identity theft.[17]

Without some assurance of privacy, patients may be reluctant to provide candid and complete disclosures of sensitive information even to their physicians. Ensuring privacy will promote more effective communication between physician and patient, which is essential for quality of care, enhanced autonomy, and preventing economic harm, reputational harm, and discrimination.[18]

Handling Paper PHI in the Work Area. When using paper PHI, health care organization workforce members should avoid unnecessarily exposing documents containing PHI. To the extent feasible PHI should be removed from high visibility areas, even if those areas are not open to the public, and should be maintained in a confidential manner in order to prevent workforce members and others that do not have a need to know from accessing such PHI. Documents must not be left unattended in areas accessible to the public (*e.g.*, charts may not be left unattended on a counter that is open to the public). Paper PHI should be placed face down or facing away from the view of others when the workforce member is not working with the document(s). Blank cover sheets should be placed over the front of paper charts and medical records that are located in semi-public areas (*e.g.*, outside of patients' doors). Similarly, any binders used to house patient records should be closed and PHI should not be readily visible by others. Paper PHI should not be left unattended on photocopiers, printers, fax machines, or in other common areas (such as conference rooms). Access to areas containing PHI must be limited to authorized personnel.[19]

Transporting Paper PHI. When transporting paper PHI within the health care organization, an envelope, folder, file, cart, or box should be used to house paper PHI documents in transit. In addition, no patient identifier should be visible. Documents containing paper PHI should not be removed from the health care organization unless the workforce member has a legitimate business need and supervisor approval to do so and another copy of the PHI removed remains at the office or facility. Paper PHI should never be left unattended in a

[15] Id.
[16] Id.
[17] Saver R. Medical research and intangible harm. University of Cincinnati Law Review. 2006; 74:941–1012.
[18] Gostin L. Health information: Reconciling personal privacy with the public good of human health. Health Care Analysis. 2001; 9:321.
[19] Safeguarding Protected Health Information, HCA Ethics Policy IP.PRI.012 (Sept. 23, 2013), www.hcaethics.com/policies/IPPRI012.doc.

vehicle or other unsecure location. If documents are transported by vehicle, the documents should always be in the trunk of a locked vehicle during transport to ensure the security of the documents. Workforce members should also take steps to safeguard paper PHI in their homes and prevent others from viewing the documents.[20]

Storage of Paper PHI. Paper PHI should be stored in secure locations (*e.g.*, locked file cabinets or access-controlled rooms or areas). The design and location of PHI storage areas and fixtures, including the use of security measures such as key cards, keys, or security cameras, should take into account both the physical protection of the PHI and the protection of its confidentiality. If PHI is to be stored at a site away from the covered entity or business associate (e.g., records storage facility), an employee should review the facility to confirm that the facility has adequate measures in place to protect the physical integrity and the confidentiality of the PHI. The covered entity or business associate should have a business associate agreement in place with the storage facility prior to sending any PHI there for storage.[21]

Disposal of Paper PHI. HIPAA does not require any particular method for disposing of paper PHI; however, the selected method must be reasonably designed to keep PHI away from the public and unauthorized persons. Paper PHI should never be thrown in the trash or recycling bin. If accessible to the public, shred bins must be locked and secured to prevent access. Before PHI is disposed of it must be made indecipherable by shredding, burning, pulping or pulverizing. Some health care organizations have all paper trash burned or shredded to avoid any confusion as to whether or not the papers contain PHI. Pharmacies should maintain labeled prescription bottles and similar forms of PHI in a secure area in opaque bags, and using a business associate disposal vendor to remove and shred or otherwise destroy the PHI.[22]

OCR Guidance on the Proper Disposal of PHI

HHS has previously released guidance on the proper disposal of paper and electronic PHI,[23] which is further described below.

General Requirements for the Disposal of PHI. The HIPAA Privacy Rule requires covered entities to apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI in any form.[24] Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.[25] Failing to implement reasonable safeguards to protect PHI in connection with disposal may result in impermissible disclosures of PHI.

Covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member.[26] Any workforce member (including volunteers) involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal.[27] Covered entities are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons. However, the Privacy and Security Rules do not require a particular disposal method. Covered entities must review their own circumstances to determine what steps are reasonable to safeguard PHI through disposal, and develop and implement policies and procedures to carry out those steps. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the form, type, and amount of PHI to be disposed. For instance, the disposal of certain types of PHI such as name, Social Security number, driver's license number, debit or credit card number, diagnosis, treatment information, or other sensitive information may warrant more care due to the risk that inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual's reputation. In general, examples of proper disposal methods may include, but are not limited to:

- *Paper Records.* For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- *Prescription Bottles and Labels.* Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- *Electronic Media.* For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).[28]

Disposal of PHI in Dumpsters. A pharmacy may not dispose of PHI information in dumpsters accessible by the public unless the PHI has been rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster. In general, a covered entity may not dispose of PHI in paper records, labeled prescription bottles, hospital iden-

[20] Id.
[21] Id.
[22] Id.
[23] HIPAA Privacy and Security Rules, ''Frequently Asked Questions About the Disposal of Protected Health Information,'' U.S. Department of Health and Human Services, Office for Civil Rights, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf.
[24] 45 CFR 164.530(c).
[25] 45 CFR 164.310(d)(2)(i) and (ii).
[26] 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i).
[27] See 45 CFR 160.103 (definition of ''workforce'').
[28] Note 13, supra.

  HLR ISSN 1064-2137

tification bracelets, PHI on electronic media, or other forms of PHI in dumpsters, recycling bins, garbage cans, or other trash receptacles generally accessible by the public or other unauthorized persons. PHI in a trash receptacle generally accessible by the public or other unauthorized persons is not an appropriate privacy or security safeguard. Pharmacies must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI. Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI. For example, depending on the circumstances, proper disposal methods may include (but are not limited to:

- *Destruction.* Shredding, or otherwise destroying PHI in paper records so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster or other trash receptacle.
- *Disposal Vendors.* Maintaining PHI for disposal in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- *Locked Dumpsters.* In justifiable cases, based on the size and the type of the covered entity, and the nature of the PHI, depositing PHI in locked dumpsters that are accessible only by authorized persons, such as appropriate refuse workers.
- *Electronic Media.* For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).[29]

Hiring a Business Associate to Dispose of PHI. A covered entity may, but is not required to, hire a business associate to appropriately dispose of PHI on its behalf. In doing so, the covered entity must enter into a contract or other agreement with the business associate that requires the business associate, among other things, to appropriately safeguard the PHI through disposal.[30] Thus, a covered entity may hire an outside vendor to pick up PHI in paper records or on electronic media from its premises, shred, burn, pulp, or pulverize the PHI, or purge or destroy the electronic media, and deposit the deconstructed material in a landfill or other appropriate area.

Reuse or Disposal of Computers or Electronic Media That Store PHI. A pharmacy may reuse or dispose of computers or other electronic media that store electronic protected health information, but only if certain steps have been taken to remove the electronic protected health information (ePHI) stored on the computers or other media before its disposal or reuse, or if the media itself is destroyed before its disposal. The HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of ePHI from electronic media before the media are made available for reuse. Depending on the circumstances, appropriate methods for removing ePHI from electronic media prior to reuse or disposal may be by clearing (using software or hardware products to overwrite media with non-sensitive data) or purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) the information from the electronic media. If circumstances warrant the destruction of the electronic media prior to disposal, destruction methods may include disintegrating, pulverizing, melting, incinerating, or shredding the media. If desired, covered entities may contract with business associates to perform these services for them.[31]

Disposal of PHI by Home Health Workers or Workforce Members Who Use PHI Away From the Covered Entity. The HIPAA Privacy Rule requires that covered entities develop and apply policies and procedures for appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, including through final disposition.[32] In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored.[33] The rules are flexible and thus, do not specify particular types of disposal methods; however, covered entities must ensure that the disposal method reasonably protects against impermissible uses and disclosures of PHI and protects against reasonably anticipated threats or hazards to the security of electronic PHI.[34] Whatever the disposal method, a covered entity must ensure that appropriate workforce members, either working on the premises or offsite, receive training on and follow the disposal policies and procedures of the covered entity.[35] These policies and procedures could require, for example, that employees or other workforce members who use PHI offsite, including electronic PHI, return all PHI to the covered entity for appropriate disposal. Or, for example, if appropriate under the circumstances, a covered entity could give off-site workforce members the option of either properly shredding PHI in paper records themselves or returning the PHI to the covered entity for disposal. In cases where workforce members fail to comply with the covered entity's disposal policies and procedures, the covered entity must apply appropriate sanctions.[36]

Conclusion

The large volume of paper PHI makes health care organizations particularly vulnerable to data breaches, as the encryption data breach safe harbor is not available for paper PHI since aper PHI cannot be encrypted. Thus, health care organization PHI data disposal policies and procedures, and workforce member training related thereto, play an important role in PHI privacy

[29] Id.

[30] 45 CFR 164.308(b), 164.314(a), 164.502(e), and 164.504(e).

[31] Note 13, supra.

[32] 45 CFR 164.530(c).

[33] 45 CFR 164.310(d)(2)(i).

[34] 45 CFR 164.530(c)(2) and 164.306(a).

[35] See 45 CFR 164.530(b) and (i), as well as 164.306(a)(4) and 164.308(a)(5) with regard to electronic PHI.

[36] 45 CFR 164.530(e).

and the prevention of data breaches. Proactively implementing the HIPAA Privacy Rule with written policies and procedures, and documentation of workforce training are essential to reduce the risk of noncompliance for covered entities.

The pharmacy settlement emphasizes OCR's expectations that covered entities, regardless of size, develop appropriate policies and procedures and training programs that address requirements of the HIPAA Privacy and Security Rules. The settlement further emphasizes OCR's expectation that organizations adopt and follow policies and procedures for secure disposal of PHI. In light of the pharmacy enforcement action, all covered entities, regardless of their size, should take appropriate steps to minimize the chances of impermissible disclosures of PHI (in any format) and any resulting enforcement action by HHS. At minimum, covered entities and business associates should:

- Annually conduct a comprehensive risk analysis to identify and mitigate security risks and vulnerabilities associated with PHI
- Adopt or revise policies and procedures to address risks and vulnerabilities identified in the risk analysis;
- Implement general policies and procedures to meet the requirements of the HIPAA Privacy and Security Rules;
- Review and revise policies and procedures frequently based on the results of compliance program audits and monitoring to ensure that PHI is safeguarded;
- Provide and update privacy and security training for workforce members annually;
- Ensure that paper PHI is shredded, burned, pulverized, pulped or otherwise rendered secured prior to disposal;
- Investigate and sanction workforce members promptly for violations of HIPAA policies and procedures;
- In the event of a suspected privacy breach, comply with data breach investigation and notification requirements; and
- Ensure that the health care organization has adequate cybersecurity insurance coverage.

Health care organizations and providers should always request advice from experienced health care legal counsel to determine the appropriate methods for handling, storage, and disposal of PHI, and to ensure compliance with federal and state privacy and security laws.

  HLR ISSN 1064-2137