Shumaker

APRIL 15, 2026 | PUBLICATION

Client Alert: The Government May Actually Be Here to Help - Health Insurance Portability and Accountability Act of 1996 (HIPAA) Part III

INDUSTRY SECTOR

Health Care

SERVICE LINE

Health Law

RELATED PROFESSIONALS

Grant P. Dearborn
Katherine H. Crawford

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The United States Department of Health and Human Services (HHS) provides a helpful set of questions and answers on its website regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Health care professionals should note that this guidance is informal and may be updated or withdrawn. In addition, state laws may differ on these issues. Below, we highlight three questions and answers from the HHS website.

What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. See 45 CFR 164.530(c). This means that 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. See 45 CFR 164.310(d)(2)(i) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

Further, 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. See 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i). Therefore, any workforce member

involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers. See 45 CFR 160.103 (definition of "workforce").

Thus, 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:

- 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.
- 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.
- 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).

For more information on proper disposal of electronic PHI, see the HHS HIPAA Security Series 3: Security Standards – Physical Safeguards. In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization.

Other methods of disposal also may be appropriate, depending on the circumstances. Covered entities are encouraged to consider the steps that other prudent health care and health information professionals are taking to protect patient privacy in connection with record disposal. In addition, if a covered entity is winding up a business, the covered entity may wish to consider giving patients the opportunity to pick up their records prior to any disposition by the covered entity (and note that many states may impose requirements on covered entities to retain and make available for a limited time, as appropriate, medical records after dissolution of a business).

Created 02.18.09

Content last reviewed November 6, 2015

May a covered entity hire a business associate to dispose of PHI?

Yes, 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. See 45 CFR 164.308(b), 164.314(a), 164.502(e), and 164.504(e). Thus, for example, 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.

Created 02.18.09

Content last reviewed July 26, 2013

May a covered entity reuse or dispose of computers or other electronic media that store electronic PHI?

Yes, but only if certain steps are 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. See 45 CFR 164.310(d)(2)(i) and (ii). 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. Covered entities may contract with business associates to perform these services for them.

For more information on proper disposal of ePHI and reuse of electronic media, see the HHS HIPAA Security Series 3: Security Standards – Physical Safeguards. In addition, for practical information on how to handle the sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization.

Created 02.18.09

Content last reviewed November 6, 2015

For health care providers, there is risk that billing records, appointment logs, medical records, and other documents contain PHI. It is essential that relevant staff are trained on the risks and proper procedures for managing PHI. These risks make it imperative that health care entities have policies on destruction of PHI and that the relevant staff are appropriately trained on such policies. Moreover, this training should be documented on an annual basis. The policies should also require that the who, what, when, where, and how of the destruction aredocumented. Any third party implementing the destruction should have a Business Associate Agreement with the health care provider. Failure to take reasonable care and comply with destruction requirements may lead to fines and a poor public image for the business. Likewise, it is invaluable to regularly review, update, and refine policies and training. Being proactive can in this case prevent a call from local media asking about a box of records found in a trash receptacle.

For more information, please contact Grant Dearborn, Kate Crawford, or another member of Shumaker's Health Law Service Line.

Shumaker