U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

Frequently Asked Questions About the Disposal of Protected Health Information

1. 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).

2. May a covered entity dispose of protected health information in dumpsters accessible by the public?

No, unless the protected health information (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 identification 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. The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, in any form, including in connection with the disposal of such information. See 45 CFR 164.530(c). 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. See 45 CFR 164.310(d)(2)(i). Depositing PHI in a trash receptacle generally accessible by the public or other unauthorized persons is not an appropriate privacy or security safeguard. Instead, covered entities 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):

- 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.

- 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.

- 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.

- 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.

3. May a covered entity hire a business associate to dispose of protected health information?

Yes, a covered entity may, but is not required to, hire a business associate to appropriately dispose of protected health information (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.

4. May a covered entity reuse or dispose of computers or other electronic media that store electronic protected health information?

Yes, 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. 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 sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization.

5. How should home health workers or other workforce members of a covered entity dispose of protected health information that they use off of the covered entity's premises?

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 protected health information (PHI), including through final disposition. See 45 CFR 164.530(c). 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. See 45 CFR 164.310(d)(2)(i). 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. See 45 CFR 164.530(c)(2) and 164.306(a). Whatever the disposal method, a covered entity must ensure that appropriate workforce members, either working on the premises or off-site, receive training on and follow the disposal policies and procedures of the covered entity. 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. These policies and procedures could require, for example, that employees or other workforce members who use PHI off-site, 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. See 45 CFR 164.530(e).

6. Does the HIPAA Privacy Rule require covered entities to keep patients' medical records for any period of time?

No, the HIPAA Privacy Rule does not include medical record retention requirements. Rather, State laws generally govern how long medical records are to be retained. However, the HIPAA Privacy Rule does require that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other protected health information (PHI) for whatever period such information is maintained by a covered entity, including through disposal. See 45 CFR 164.530(c).