

## Health Information Compliance Alert

### Reader Questions: Don't Forget About These HIPAA Rules on PHI Disposal

**Question:** We have some student helpers working at our practice this summer. We were going to have them dispose of records for patients that are no longer at our practice. Is there a specific way to go about this kind of records' purge? Do they need to be trained?

Ohio Subscriber

**Answer:** Actually, there are specific examples outlined by the HHS Office for Civil Rights (OCR) on the proper way to dispose of patients' protected health information (PHI). In addition, your summertime staff should be thoroughly trained on these disposal protocols, too.

Since the HIPAA Privacy and Security Rules do not specify a particular disposal method, it's a good idea to review the various suggestions that OCR gives to cover all your bases. However, know that covered entities cannot dispose of PHI in dumpsters or other places where the public or other unauthorized persons could get to it.

"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," OCR cautions. "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 of."



"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 inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual's reputation," the agency explains.

Check out these examples on the proper way to dispose of PHI, according to OCR guidance:

- **Paper records:** For PHI in paper records, shredding, burning, pulping, or pulverizing the records so PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed. The best practice is on-site destruction to reduce the chance of accidental disclosure during transport.
- **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).
- **Prescription bottles:** For PHI on labeled prescription bottles, maintaining bottles 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.

**Consider this:** If you think that improperly disposing of patients' PHI isn't breachworthy, think again. OCR is currently investigating three separate cases of healthcare providers who improperly disposed of their patients' data, according to the OCR breach portal.