

HIPPA Privacy – Improper Disposal of Health Information Can Be Costly

This FYI discusses recent guidance on how to properly dispose of health information under the Health Insurance Portability and Accountability Act ("HIPAA") privacy rules. Employers with group health plans are required to properly safeguard protected health information. As discussed below, improper disposal of protected health information can be costly.

Here are links to two recent developments:

- A multi-million dollar settlement involving improper disposal of health information:

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresagrcap.pdf>.

- New government-issued FAQs that address the HIPAA Privacy Rule requirements for disposal of protected health information:

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaq.pdf>.

The guidance is a good reminder to employers to periodically self-audit compliance with privacy policy and procedures, including re-evaluating how protected health information is disposed. Besides concerns about disposing health information in trash containers that are not secure and could be accessed by the public, other concerns raised by the government involved failure to have proper policies and procedures to safeguard protected health information and failure to adequately train employees.

The guidance notes generally that health plans should review their own circumstances to determine what steps are reasonable to safeguard protected health information 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 the individual's privacy, as well as consider such issues as the form, type, and amount of protected health information to be disposed. For instance, the disposal of certain types of protected health information 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.

What should employers do?

- Review disposal of protected health information as part of a regular HIPAA self-audit process. HIPAA record retention requirements should be part of the review process. Check with counsel regarding any other laws that might affect the method of disposal.

- Check written policies and procedures regarding disposal. Ensure that sanctions for violations of the policies and procedures are in place and enforced.
- Make sure business associate arrangements are in order with respect to disposal issues.

Cynthia A. Van Bogaert

is a partner with Boardman, Suhr, Curry & Field LLP. She is a faculty member for employee benefits courses for ALI-ABA and the Employee Benefits Institute of America, as well as author of the 401(k) column on BenefitsLink, a national employee benefits Web site.

These articles are not legal advice. Individuals should seek advice based on their particular circumstances from their own counsel. Nothing in this article is intended to be used, and no information can be used, for the purpose of avoiding penalties under the Internal Revenue Code, or promoting, marketing, or recommending to another party any transaction or matter addressed in this article. © 2008 Cynthia A. Van Bogaert All rights reserved.