Codify
BY AAPC

Health Information Compliance Alert

HIPAA Compliance: Add This Expert Advice to Your PHI Disposal Wheelhouse

Tip: Train staff accordingly.

You can cut down on protected health information (PHI) disposal faux pas with a solid HIPAA compliance plan that guides staff on how to get rid of patient data correctly.

Human error factors heavily in many HIPAA violations, including cases related to PHI disposal. These breaches are often the result of unimplemented policies and procedures and inadequate training as evidenced by the recent New England Dermatology P.C., d/b/a New England Dermatology and Laser Center (NDELC) case (see story, p. 1). Read on for advice on disposing of PHI.

Consider These Factors As You Arrange Your PHI Disposal Policies

It's essential that your staff know the basics on what exactly PHI is and how to effectively dispose of it.

"I think a lot of the disposal problems are just plain old organizational-procedural inertia - staff are doing things the way they've always been done and nobody has checked to see if it's the proper, secure way," explains **Jim Sheldon-Dean**, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte,Vermont.

First: PHI is best defined as "all 'individually identifiable health information' held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral," according to the HHS Office for Civil Rights (OCR) guidance on the HIPAA Privacy Rule. Furthermore, any personal information that can identify the patient and is

associated with the medical record is also protected data. In fact, federal guidance lists 18 categories of "personal identifiers" that must be secured by covered entities (CEs) and business associates (BAs) (see Health Information Compliance Alert, Vol. 22, No. 2).

Next: Your staff must understand that if they are throwing out PHI with the trash, it must be "rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster," OCR notes in a Frequently Asked Questions (FAQs) on PHI disposal.

"Staff may assume what they throw away is destroyed when it may not be," Sheldon-Dean says. "They need to look at their non-electronic information and make sure it is handled with the same care that electronic information is these days. Paper, pill bottles, or data, it all needs to be subject to information flow analysis to ensure all information is secure until destroyed," he advises.

Reminder: Though the HIPAA Privacy and Security Rules don't offer specifics on the best way to dispose of PHI, OCR does provide helpful examples on how to safeguard used patient data and how to safely discard it (see Health Information Compliance Alert, Vol. 22, No. 7).

OCR also offers guidance on the intersection of the rules and PHI disposal in its FAQs on the subject. Topics covered include:

- Acceptable methods for getting rid of PHI, ePHI, and other associated items
- Business associates' roles in disposal
- Reusing hardware that may contain old ePHI
- Off-site disposal of PHI/ePHI by home health and hospice workers
- Medical records retention and disposal

Pocket These Training Tips

Staff education should always be an integral part of your HIPAA compliance plan - and your policies must include PHI disposal training, Sheldon-Dean maintains. "Do a training session with managers on the topic of handling all kinds of data securely, and then be sure each department talks through how they use and protect any PHI in any form. Then adopt

and train all the staff in appropriate procedures.”

He cautions, "Finally, do an audit (look in the trash) to make sure the message got through, and follow up as necessary until it does get through. The important thing is to do your own auditing, and don't leave it to the local TV news team to do your auditing for you.”

Resource: Find the FAQs on PHI disposal at www.hhs.gov/sites/default/files/disposalfaqs.pdf.