Codify
BY AAPC

Health Information Compliance Alert

Case Study: HIPAA Compliance Continues Past Business Closures

State and federal laws often differ on the protection, retention, and disposal of PHI.

Ensuring the safety of your patients' protected health information (PHI) on your computers, networks, and mobile devices is important. However, you're wise to remember that the HIPAA Privacy Rule still mandates the security of the paper records in your office, too. Those protocols must be followed even if your business goes belly up - or it could cost you, a recent breach demonstrates.

Last month, the HHS Office for Civil Rights (OCR) warned providers and their business associates in a release that anyone handling PHI, including physician's offices, storage vendors, and other covered entities (CEs), is subject to the full consequences of a HIPAA violation - up to and beyond your business's viability or lifespan.

Context: After liquidating the assets of Filefax Inc., the appointed receiver agreed to pay $100,000 out of the estate to settle violations of the HIPAA Privacy Rule. Filefax Inc. advertised its provision of storage, maintenance, and delivery of medical records for covered entities, according to the OCR press release.

OCR opened an investigation after an anonymous tipster alleged that someone transported Filefax medical records to a shredding and recycling facility in order to sell them. OCR found evidence of 2,150 patients' medical records - records containing PHI - at the shredding and recycling facility and in an unlocked truck in the Filefax parking lot. OCR's investigation indicated that Filefax had granted permission to an unauthorized person to remove the PHI from Filefax, who left the PHI unsecured outside the Filefax facility, according to the report.

Though Filefax shuttered during the investigation, it was still held to the consequences of violating the HIPAA Privacy Rule. "In 2016, a court in unrelated litigation appointed a receiver to liquidate its assets for distribution to creditors and others," according to the press release. "In addition to a $100,000 monetary settlement, the receiver has agreed, on behalf of Filefax, to properly store and dispose of remaining medical records found at Filefax's facility in compliance with HIPAA."

Consider this: Although there has been intense focus in the healthcare industry on securing ePHI and medical records, paper records are still highly vulnerable as this case illustrates. "While not as easily transferable as its digital counterpart, the information in paper-based medical records remains extremely lucrative in the black market," warned partner attorney **Laurie Cohen** in a blog posting for the law firm Nixon Peabody LLP. Experts estimate that an individual's medical data can fetch as much as 10 times the value of a credit card number.

Make Long-Term Plans for PHI in Your Protocols

Filefax was slapped with a corrective action plan that addressed Privacy and Security Rule issues. The proper disposal of PHI is one of the OCR's top five hot spots, and one the department takes very seriously.

"Organizations should pay careful attention to the transfer and disposal of both electronic and paper patient records," stressed associate attorney **Jefferson Lin** in a blog posting for the Seattle-based law firm Ogden Murphy Wallace Attorneys.

Under the HIPAA Privacy rule, Section 45 CFR 164.530(c), "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," OCR guidance reminds. It's also essential to set up standards after your risk analysis for the disposal of ePHI, ensuring that the electronic devices and tools aren't reused for nefarious purposes after your practice dissolves, the Security Rule says in 45 CFR Part 160 and Subparts A and C of Part 164.

Read a summary of the OCR guidance on disposing PHI at www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html?language=en.

Ask Yourself These 5 Questions

Take care to outline specific guidelines for the retention and disposal of PHI and ePHI, keeping the HIPAA Privacy and Security Rules in mind. Consider these OCR questions for CEs when writing up your HIPAA compliance plans:

1. May a CE dispose of PHI in dumpsters accessible by the public?

2. May a CE hire a business associate (BA) to dispose of PHI?

3. May a CE reuse or dispose of computers or other electronic media that store electronic PHI?

4. How should home health workers or other workforce members of a CE dispose of PHI that they use off the CE's premises?

5. Does the HIPAA Privacy Rule require CEs to keep patients' medical records for any period of time?

Important: Healthcare is a competitive business, and practice closures are an all too common occurrence. Records management must include the proper disposal of records, taking every safeguard into account to secure PHI. The scope of the facility, how a practice dissolves, the number of business partnerships, and the state in which the provider practices, are all things that factor into how long PHI and ePHI are retained, managed, and eventually discarded and/or destroyed, advises the American Health Information Management Association (AHIMA) in its online guidance "Protecting Patient Information After a Facility Closure."

Endnote: "The careless handling of PHI is never acceptable," said **Roger Severino**, OCR director. "Covered entities and business associates need to be aware that OCR is committed to enforcing HIPAA regardless of whether a covered entity is opening its doors or closing them. HIPAA still applies."

Resources: Take a look at the OCR release of the Filefax, Inc. case at www.hhs.gov/about/news/2018/02/13/consequences-hipaa-violations-dont-stop-when-business-closes.html.

To see AHIMA's advice on securing PHI after practice closure, visit http://library.ahima.org/doc?oid=105074#.WqZm8WaZNAY.