Codify
BY AAPC

Health Information Compliance Alert

Case Study: Know the Rules on the Secure Disposal of PHI

Hint: Ignoring the HIPAA requirements can land you in hot water.

Protecting your patients' personal information and health data is the central point of HIPAA. But, what you may not realize is that how you dispose of PHI is another critical piece of the Privacy Rule puzzle. And, merely throwing it away without securing the data may have dire consequences for your organization.

Background: On Aug. 23, the New England Dermatology P.C., d/b/a New England Dermatology and Laser Center (NDELC) settled charges of potential HIPAA violations with the HHS Office for Civil Rights (OCR), an agency release indicates. The Springfield, Massachusetts-based NDELC agreed to pay the feds $300,640 for improperly disposing of patients' protected health information (PHI) that resulted in a HIPAA breach. Additionally, the dermatology services provider will enter into a two-year corrective action plan (CAP) that OCR labels "robust."

Over the last few years, COVID has dominated the healthcare realm and Right of Access violations have been a primary target for OCR; however, this case should be a reminder that the feds are still on top of small infractions and a variety of breach types.

"The settlement reinforces that HIPAA compliance includes not only protection of electronic patient records, but proper handling of physical items as well," explains attorney **Mary Connolly** with Rivkin Radler LLP in the law firm's Rivkin Rounds blog.

Check Out the Case Details

"On May 11, 2021, NEDLC filed a breach report with OCR stating that empty specimen containers with protected health information on the labels were placed in a garbage bin in their parking lot," according to the OCR release. "The containers' labels included patient names and dates of birth, dates of sample collection, and name of the provider who took the specimen."

After receiving the breach report, OCR began an investigation and discovered the potential violations. The agency revealed that NEDLC failed to implement proper compliance to better protect PHI, the release suggests.

"Improper disposal of protected health information creates an unnecessary risk to patient privacy," cautions Acting OCR Director **Melanie Fontes Rainer** in the release. "HIPAA regulated entities should take every step to ensure that safeguards are in place when disposing of patient information to keep it from being accessible by the public," Fontes Rainer adds.

Under the CAP, NEDLC is required to institute a variety of HIPAA Privacy Rule requirements including:

- Designate a privacy officer to develop and implement a HIPAA compliance plan.
- Create, update, and modify policies and procedures that protect PHI.
- Distribute HIPAA materials to staff.
- Educate employees on the HIPAA-related policies/ procedures, including the risks involved and penalties for non-compliance.
- Get OCR approval of the plan and submit annual reports during the two years of monitoring.

Resource: Review the resolution specifics at www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/nedlc-ra-cap/index.html.