

HIPAA's Privacy Rule: Are Hospitals Falling Down on the Job?

When we talk about HIPAA (the Health Insurance Portability and Accountability Act), we usually talk about the importance of keeping sensitive patient health data away from people not authorized to access it. But what about the patients themselves?

HIPAA affords patients the right to receive copies of their own health records. However, a new study by the Yale University School of Medicine reveals that many hospitals are failing to comply with HIPAA's Privacy Rule when patients request copies of their records.

Many hospitals didn't fare well in the study

Yale University researchers assessed medical record release protocol at 83 major hospitals across the country and discovered high numbers of Privacy Rule breaches, including the failure to give patients their full medical records when requested, and charging patients fees higher than recommended by the Department of Health and Human Services' Office of Civil Rights (OCR).

The study found that only 53% of the hospitals evaluated clearly and directly offered patients the opportunity to receive their full health record. And when it came to the pragmatics of delivering records to patients, more than half of the hospitals charge patients more than the \$6.50 flat fee recommended by the OCR for releasing "electronically maintained" health records. In a jaw-droppingly extreme example, one facility charged a patient more than \$500 for the release of a 200-page medical file.

Records request forms themselves were often found to be beset with errors or issues of incompleteness. For instance: nearly half of the hospitals failed to include what patients would be charged for a records delivery on the request form itself, and only around a third of facilities stated that amount on the form or the web page from which the form could be downloaded.

"The lack of a uniform procedure for requesting medical records across US hospitals highlights a systemic problem in complying with the right of access under HIPAA," wrote the researchers. "Because every institution creates its own process and implements its own regulations, variability in what and how records can be received occurs."

Privacy Rule is 15 years old, but some hospitals are still lax about following it to the letter

HIPAA's Privacy Rule has been required protocol since 2003, but that doesn't mean hospitals consistently comply. For example, in 2011 the OCR slapped a \$4,300,000 penalty on Cignet Health of Prince George's County for failing to provide copies of medical records to patients who requested them. It's not hard to see that monetary figure as a message sent to other healthcare providers who might get sloppy with the Privacy Rule.

Around 8% of the hospitals assessed in the study failed to turn around the records request within the 30 days mandated by the Privacy Rule. Furthermore, HIPAA requires that patients receive a copy of their requested records in the format they prefer, but hospital providers were often inconsistent when it came to communicating those options. And of course, that can lead to patients becoming needlessly confused.

For instance, one option is medical records on CD; while over 60% of hospitals shared this choice with patients over the phone, only a quarter of providers listed that format possibility on records request forms. Similarly, more than 80% of facilities told patients over the phone that they could retrieve the file in person, while under half of them noted that on the forms.

Co-author of the report, Harlan Krumholz, MD, had this to say to HIPAA Journal: "If we really want to move to a healthcare



system where patients are at the center, then we need to find ways to ensure that they have agency over their own data. We're far from that right now."

The study recently appeared in JAMA Network Open.

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.