HIPAA Enforcement Against UCLA and New Rule Proposal Bring Scrutiny to Workforce Access to Health Information

07.29.2011

Elizabeth H. Johnson

Kimberly A. Licata

On May 31, 2011, the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) issued a notice of proposed rulemaking (NPRM) that would provide individuals with a new right under HIPAA. The NPRM would allow individuals to request an "access report" from HIPAA covered entities that must reflect virtually every instance of access to their electronic protected health information (ePHI), including all access by individual employees. Weeks later, OCR followed the NPRM's release with an announcement on July 7, 2011 that it had entered into an $865,000 settlement with the University of California at Los Angeles Health Systems (UCLAHS) to resolve potential HIPAA violations raised by celebrity complainants who claimed that employees of UCLAHS repeatedly looked at their ePHI without a permissible purpose. Employee "snooping" of this nature is precisely the type of behavior that the new "access report" described in the NPRM would capture. Individuals' ability to request such reports from covered entities (and OCR's ability to do the same) not only creates a new and burdensome obligation for covered entities, but also creates new enforcement risks in the process.

UCLAHS's Settlement of Privacy and Security Rule Violations

OCR's enforcement action against UCLAHS followed an extended period in which employees allegedly repeatedly accessed ePHI of many patients, including several celebrity patients, when they did not have any job-related need to access the data. OCR's investigation of this potential HIPAA violation led to the identification of multiple alleged deficiencies by UCLAHS under the

Privacy and Security Rules. These included failing to implement security controls to reduce the risk of impermissible access, failing to provide Security Rule training, and failing to apply appropriate sanctions against workforce members who violated UCLAHS policies and procedures. The end result for UCLAHS was imposition of an $865,500 resolution amount and a Corrective Action Plan (CAP). The CAP has a three-year duration that begins once OCR approves the "Monitor Plan" established by UCLAHS, which includes, among other items:

- A comprehensive revamping of all UCLAHS's policies and procedures related to the Privacy and Security Rules, with all policies and procedures subject to OCR's approval;
- Implementation of the OCR-approved policies and procedures;
- Identification of minimum content of the policies and procedures and "reportable events" that consist of specific events or violations UCLAHS must proactively report to OCR;
- Regular and robust training of the workforce; and
- Monitoring by an "independent monitor," that will develop the "Monitor Plan," to include semi-annual monitor review reports to be submitted to OCR, among other required activities.

The New Proposed Right to an Access Report

This enforcement action raises the stakes on the NPRM which, if finalized as written, would provide individuals with the right to request an access report reflecting virtually all instances of electronic access to ePHI by covered entity employees, third parties, and information systems. Inherent in this requirement is an underlying obligation to implement system logging capabilities that would not only track all access (including view-only access) to ePHI but store those logs for three years. An express purpose of this proposal is to allow individuals to identify situations in which a member of a covered entity's workforce inappropriately accessed their records. In other

words, patients and customers requesting these access reports will be able to detect employee snooping. The UCLAHS action provides an example of the potential result for the covered entity.

The access report, as proposed by OCR, must reflect the full name of every person or entity that accessed an individual's ePHI (if maintained in a designated record set) in the prior three years. In the NPRM, OCR stated that it believes this degree of access logging is currently captured and stored by covered entities' electronic information systems used by covered entities because OCR interprets HIPAA's audit controls standard (45 C.F.R. § 164.312(b)) and information system activity review implementation specification (45 C.F.R. § 164.308(a)(1)(ii)(D)) as requiring that all such access be logged, including "view" or "read only" access. This interpretation of the Security Rule is much broader that what many covered entitles and business associates had previously understood, and the NPRM has already fallen under criticism as a result. If implemented by OCR in the form currently proposed, covered entities will incur significant unexpected costs related to systems modifications, data storage (access logs must be retained for three years), training, privacy notice revision and redistribution and response to individual requests.

Presumably, individual privacy complaints filed with covered entities and OCR also will increase, whether because covered entities will fail to completely or timely provide the access report, or because individuals reviewing their access report will find real or (more likely) perceived cases of inappropriate access to their records. Business associates will also have to undertake a similar degree of implementation to provide covered entities with access logs relevant to the access report, as required by the NPRM. Covered entities, in turn, would be well advised to update business associate agreements to reflect this requirement if it becomes a final rule. Comments on this NPRM, including on the general costs and benefits of the proposal are due August 1.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075