OBER | KALER
Attorneys at Law

September 19, 2011

Ober|Kaler Healthcare Information Privacy, Security and Technology Bulletin

James B. Wieland | jbwieland@ober.com

Joshua J. Freemire | jjfreemire@ober.com

Changes to HIPAA Privacy Rule and CLIA Regs Will Require Laboratories to Release Test Results to Patients

If the most recent proposed changes to the HIPAA Privacy Rule and CLIA regulations are finalized as proposed, laboratories across America will be obligated to provide test results to individual patients upon request. The changes to CLIA and the HIPAA Privacy Rule are coordinated and, taken together, would result in a marked change from the current web of state-specific laboratory laws (which often prohibits providing patients their own test results) and will require many laboratories to develop HIPAA compliant policies and procedures for accepting, processing, and responding to patient requests for protected health information. For laboratories, a patient request for health information maintained by the laboratory would include a copy of the requesting patient's laboratory reports.

The proposed rule ("NPRM") [PDF] was published on September 14, 2011 in the Federal Register. Comments may be filed in the typical fashion, and, to be considered, must be filed by 5 p.m. on November 14, 2011. The NPRM specifically requests comments on several areas, including, especially, the burdens created by this new requirement for laboratories.

The Privacy Rule's Right-of-Access Provisions

HIPAA has, since its inception, given patients a right to request a copy of their protected health information, if contained in a "designated record set", subject to certain exceptions. These exceptions included one that exempted covered entities subject to CLIA. Laboratories, in other words, were not required to comply with the Privacy Rule's right-of-access provisions, which also include a deadline for the covered entity's response and patient appeal rights where a request for access is denied. The HITECH Act added statutory provisions extending this right of access to records maintained in electronic form and providing patients a right to request that the covered entity transmit a copy of the requested record(s) to an entity or person designated by the individual (such as, for example, the individual's personal health records provider). Unfortunately, the regulations implementing the HITECH Act's changes have not yet been finalized, leaving the Privacy Rule's right-of-access provisions uncertain.

The NPRM proposes changes that will eliminate the Privacy Rule's exception for CLIA-covered or exempt entities. Laboratories, in terms of the Privacy Rule's right-of-access, will now need to comply with patient requests for information in the same manner as other covered entities. Because of the timing of the NPRM relative to the regulatory revisions required by the HITECH Act, however, laboratories may face challenges drafting policies and crafting procedures to comply with the full extent of the Privacy Rule.

The NPRM's Changes to HIPAA and CLIA

The NPRM proposes changes to both the Privacy Rule and the CLIA regulations. As the NPRM explains, the proposed changes will provide "…individuals the right to receive their test reports directly from laboratories by removing the exceptions for CLIA-certified laboratories and CLIA-exempt laboratories from the [Privacy Rule] provision that provides individuals with the right of access to their protected health information." Under the changes to CLIA, laboratories will be permitted to provide patient test results and under the changes to the Privacy Rule, they will no longer be exempted from the Privacy Rule's requirement that they do so.

The relevant CLIA regulations are found at 42 C.F.R. §493.1291. Under the existing rule, laboratories may only release test results to an "authorized person" and, if applicable, the individuals responsible for using the test results (including their representatives, or the laboratory that originally requested the test). Into that section, the NPRM proposes adding an additional group who may receive test results:

> Upon a patient's request, the laboratory may provide access to completed test reports that, using the laboratory's authentication process, can be identified as belonging to that patient.

Notably, laboratories may release test results to patients, and then only when they may be authenticated. The NPRM explains that the may is somewhat illusory – as laboratories are usually "covered entities[1]" under the Privacy Rule, they would be *required* to comply with the Privacy Rule provisions granting patients a right of access. These rules, however, only apply where the covered entity can be certain that the person requesting access is indeed the patient whose records are sought (or someone similarly authorized, such as a personal representative). As the NPRM notes, this authentication is especially important in a laboratory context where anonymous testing is not unusual. If the laboratory cannot be certain, for instance, that the patient requesting the results of accession #123456, is in fact "Anonymous – ID #67890" who was the subject of that accession, they are not obligated to release the results.

The affected Privacy Rule provision is found at 42 C.F.R § 164.524. As that regulation currently reads, covered entities that are "Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a" and CLIA-exempt entities are exempted from the right-of-access requirement. Under the NPRM, these sections would simply be deleted from the regulation. As a result, the NPRM explains:

> HIPAA covered entities that are subject to CLIA would have the same obligations as other types of covered health care providers with respect to providing individuals with access to their protected health information in accordance with §164.524. Similarly, HIPAA covered entities that are CLIA-exempt laboratories (as the term is defined at 42 CFR 493.2) would no longer be excepted from HIPAA's right of access under §164.524(a)(1(iii)(B). As with other covered entities, HIPAA covered laboratories would be required to provide access to the individual or the individual's personal representative.

Covered entity laboratories would also be required to have in place compliant policies and procedures, including policies and procedures governing the receipt, processing, and response to requests within HIPAA compliant time limits.

---

1 Relevant to laboratories, HIPAA and its implementing regulations define a "covered entity" to include a health care provider that conducts (or has conducted at least one) electronic transactions, including, among others, submitting health care claims or similar encounter information (for payment purposes), coordination of benefits activities, checking health care claim status, and certifying referrals or authorizations. Most laboratories perform all or at least some of these activities electronically, but smaller laboratories that do not should investigate whether they are, in fact, "covered entities."

Changes to State Laws

Importantly, the NPRM acknowledges that state law frequently prohibits laboratories from providing test results directly to patients[2]. Other states permit disclosure only with the permission of the ordering physician[3]. In these states, the NPRM will effectuate a direct change in the law. HIPAA's preemption provisions require the application of the Privacy Rule where complying with both the HIPAA Privacy Rule state laws is impossible. In the case of state laws restricting or prohibiting patients' access to their own test results, compliance with both provisions is certainly impossible, and, further, the state laws at issue stand as an obstacle to accomplishing the purposes of HIPAA. Thus, in states that prohibit patient access, state laws would be preempted by the revised Privacy Rule provisions. In states where, heretofore, no patient access law had existed, the proposed rule, if final, would become the applicable legal standard. In terms of patient access, the NPRM makes clear that all relevant state laws will be preempted unless they provide individuals a "more expansive" right of access.

Reasoning, Burden Calculations, and Effective Dates

The NPRM provides a somewhat detailed rational for the proposed regulatory changes. Specifically, it notes that the Health Information Technology Policy Committee ("HITPC")[4] had recommended the removal of the provisions that exempted laboratories from the HIPAA. HITPC stakeholders "perceived" the regulations as "imposing barriers to the exchange of health information. These stakeholders, according to the NPRM included laboratories large and small, EHR vendors, system policy experts, and health information exchanges ("HIEs").

The resulting NPRM was crafted through a partnership between the staff responsible for CLIA, the ONC, and CMS Office of E-Health Standards and Services ("OESS"). While the NPRM is intended to improve patient's access to their own health information (and, one imagines, simplify programming and communication requirements for EHR vendors and HIE operators) the NPRM includes a specific solicitation for comments "regarding the potential impact of this change on improving patients' access to their laboratory results."

The NPRM also specifically solicits comments regarding the effect complying with the new access requirements could have on laboratories. Included in the NPRM are detailed calculations of the potential costs

---

2 The NPRM provides a chart identifying Arkansas, Georgia, Hawaii, Illinois, Kansas, Maine, Missouri, Pennsylvania, Rhode Island, Tennessee, Washington, Wisconsin and Wyoming as states where such laws are in effect.

3 The NPRM provides a chart identifying California, Connecticut, Florida, Massachusetts, Michigan, New York and Virginia as states where such laws are in effect.

4 The HITPC was created by the HITECH Act as part of the health reform legislation. The HITPC, among other responsibilities, provides recommendations and guidance to the Office of the National Coordinator for Health Care Technology, more commonly know as the "National Coordinator" or the "ONC." The ONC, in turn, issues regulations governing, among other things, the technology requirements for various federal incentive programs related to the use of health information technology, including the very well known Electronic Health Record Incentive Program (also known as the "Meaningful Use" program).

imposed (including employee time to create and implement compliant policies and procedures and to receive, record, and respond to patient requests) but uncertainty in the assumptions underlying the calculations resulted in a wide range of potential financial impacts: estimated costs through 2011 range from $3 million to $26 million for all impacted laboratories. Obviously, laboratories in states where providing test results to patients is currently illegal will bear the disproportionate portion of this burden as each must create a compliant response program "from scratch."

The NPRM is a proposed rule – the publication of a final rule, addressing and responding to comments where appropriate, is necessary before any of the proposed changes take effect. A final rule, when published, would take effect 60 days from the date of publication. In accordance with the proposed changes to 45 CFR §160.105[5], (which themselves have not been finalized) laboratories would be required to comply with the provisions of the final rule within 180 days of the rule's effective date. This 180 day period is the minimum permitted by section 1175(b)(2) of the Social Security Act. Clinical laboratories would therefore have a total of 240 days from publication of the final rule to comply.

Current Unsettled State of the Relevant Privacy Rule Provisions

The NPRM's proposed changes to the Privacy Rule and CLIA regulations obligate laboratories to comply with the Privacy Rule. Fair enough. The Privacy Rule itself, however, is itself in flux. The NPRM, in other words, proposes obligating laboratories to craft policies and procedures to comply with the currently existing Privacy Rule now, and then modify them soon thereafter when the changes mandated by the HITECH Act are finalized.

Responding to requirements and changes in the HITECH Act, passed as part of 2009's American Recovery and Reinvestment Act, CMS issued a proposed rule substantially altering the Privacy Rule in July of 2010 [PDF]. Among the changes made, provisions of the proposed rule required that covered entities provide individuals with access to their health information in electronic form in a machine readable format of the individual's choosing (where it is readily producible in such a format). Changes were also proposed to the way that covered entities are permitted to charge individuals for producing such material, including permitting charges for the time spent formatting or creating the information and cost based fees for portable media (where, for example, an individual requests the information be provided on a DVD).

5 The changes provide that changes to the Privacy and Security Rules (or any other regulatory changes affecting HIPAA requirements) must be made effective at least 180 days from the effective date of the final rule making the changes. This change itself was proposed as part of the regulations issued to implement much of the HITECH Act's requirements. The complete proposed rule can be viewed here or by following the link in the text above.

Currently, the Privacy Rule provides for neither of these requirements. Covered entities are required to produce health information in a form or format requested by the individual, but it is not clear that they are required to provide information in an electronic format. Similarly, entities are specifically prohibited from charging patients for time spent "searching for or retrieving" information, and may charge requesting patients only a "reasonable, cost-based" fee based on the cost of copying the (presumably paper) information and postage fees (where applicable).

Assuming for the moment, as the NPRM itself does, that the NPRM will be finalized and made effective before the proposed changes to the Privacy Rule are made effective, laboratories will be asked to craft two sets of policies, not one. Initially, and within the 240 day compliance period, they will be required to create, train staff, and implement policies and procedures which comply with the currently effective provisions of the Privacy Rule. Shortly thereafter, they will be required to revise those policies (and presumably retrain responsible staff members) and implement new policies conforming with the provisions of the final rule implementing the changes required by the HITECH Act.

Ober|Kaler's Comments

The proposed changes to CLIA and the Privacy Rule seem minor, but will require substantial work on the part of many laboratories, especially those in states where the provision of test results to patients was previously not permitted. For laboratories in these states, the work to prepare effective policies and procedures, train staff, and implement processes to receive and compliantly respond to patient communications will likely take time – perhaps more than the 240 days promised by the NPRM. Similarly, the burdens of compliance will fall disproportionately on laboratories in these states. To the extent that laboratories or other interested parties believe that the compliance period provided by CMS is insufficient, or that the burden calculations in the NPRM understate the work required, commenting on the NPRM offers an opportunity to positively impact the final rule's contents.

Similarly, laboratories and other affected entities everywhere should be concerned that the NPRM proposes to obligate them to comply with a standard that itself is not finalized. It is not clear from the NPRM why the proposed changes to CLIA and the Privacy Rule are of such a time sensitive nature that they will require finalization before the HITECH mandated adjustments to the Privacy Rule are finalized. While progression towards universality in EHR and HIE communications promises substantial financial and patient care benefits, its also essential that such progress be made in an orderly fashion that does not unnecessarily place the cost of compliance (or double compliance!) on providers.

About Ober|Kaler

Ober|Kaler is a national law firm that provides integrated regulatory, transaction and litigation services to financial, health care, construction and other business organizations. The firm has more than 130 attorneys in offices in Baltimore, MD, Washington, DC and Falls Church, VA. For more information, visit www.ober.com.