More Robust HIPAA Compliance Plans Needed to Address Increased Scrutiny

September 25, 2012

The Office of Civil Rights ("OCR"), responsible for enforcement of the Health Insurance Portability and Accountability Act ("HIPAA") announced a $1.5 million settlement on September 17th. The penalties were in response to a breach report filed by the Massachusetts Eye and Ear Infirmary related to the loss of a single laptop. During the investigation of the lost laptop, OCR found that the hospital had insufficient policies, procedures and operations in place to protect information stored on portable devices. In addition to the financial penalties, the facility entered into a corrective action plan with OCR which includes submission of more robust policies and procedures, implementation of more complete security measures, and a more effective incident reporting system.

This settlement is one in a number of recent actions by OCR demonstrating a more aggressive approach to HIPAA enforcement. After years of dormancy, HIPAA once again stepped into the spotlight in 2009 when it was amended under the HITECH Act. Since that time, providers have seen increased scrutiny, more frequent penalties, and expanded applicability of the law. Other enforcement activities announced in 2012 include:

Blue Cross Blue Shield of Tennessee Settlement. In March 2012, OCR settled its case with Blue Cross Blue Shield of Tennessee for $1.5 million and implementation of a corrective action plan. The penalty was associated with the theft of unencrypted hard drives containing over 1 million individuals' protected health information. This settlement was the first penalty leveled by OCR as a result of a breach notification report by a covered entity.

Phoenix Cardiac Surgery Settlement. In April 2012, OCR settled its case against Phoenix Cardiac Surgery for $100,000 and implementation of a corrective action plan. The penalty was in response to a complaint OCR received related to a publicly available internet-based calendar utilized by the practice. This settlement is the first against a small organization for its failure to adequately comply with the requirements of HIPAA Privacy and Security.

Alaska Department of Health and Human Services. In June 2012, OCR settled its case against the Alaska Department of Health and Human Services for $1.7 million and implementation of a corrective action plan. The penalty was associated with the theft of a USB hard drive that may have contained protected

health information. This settlement is the first levied against an organization where the involvement of protected health information was only possible, not confirmed.

Audit Protocol. In June 2012, OCR published its HIPAA Audit Protocol, originally comprised of 77 criteria related to HIPAA security and 88 related to HIPAA privacy and breach. The protocol has already been updated to now include 78 HIPAA security criteria, 81 HIPAA privacy criteria, and ten breach criteria. The audit procedure associated with each criterion includes both the review of policies and procedures for adequacy, the gathering of documentation demonstrating compliance with policies, and assessment of the sufficiency of review and revision of policies and procedures.

Meaningful Use. In addition to the activity by OCR, the sufficiency of HIPAA security policies and procedures may also be assessed by the Centers for Medicare and Medicaid Services ("CMS"). CMS is responsible for auditing providers who receive funds under the meaningful use incentive program. The Office of the Inspector General of the Department of Health and Human Services ("OIG") also listed audits of these payments in its 2012 workplan. In addition to the requirements related to use of a certified electronic health record, receipt of meaningful use incentives requires providers to attest to the performance of a HIPAA security risk assessment and implementation of security measures to address identified risks.

Prudent health care providers will review and revise existing HIPAA compliance plans to ensure policies and procedures are in place to survive this increased scrutiny. Policies considered acceptable by OCR in previous years are now being scrutinized with providers receiving recommendations for increased security. In addition to the policies and procedures, it is necessary for health care providers to ensure staff are trained, business associates are supervised, and documentation is maintained to comply with the law.

The healthcare team at Lathrop Gage LLP is equipped to guide providers through these changes and implement HIPAA compliance programs that demonstrate the organization's commitment to the privacy and security of its patients' information as well as providing rapid response to a data security breach, should one occur. Our services include:

- Performance of a HIPAA risk assessment or HIPAA audit to assess current practices and identify any compliance vulnerabilities;
- Development and implementation of policies and procedures to address HIPAA and state law requirements related to the privacy and security of patient information;
- Education and training for Board Members, Compliance Officers, Managers, and Staff related to HIPAA Compliance;
- Education and guidance related to meaningful use incentive programs and attestation; and
- Management of interactions with OCR, CMS, and other regulatory agencies related to HIPAA breach notification or complaint investigation.

Please contact your Lathrop Gage attorney or a member of our health care department with questions regarding HIPAA compliance.