PUBLICATION

State Enforcement Action for HIPAA Violations Set to Increase [Ober|Kaler]

2012: Issue 10 - Focus on White Collar

Massachusetts Hospital Settles Improper Record Disposal Accusations as OCR Makes Public Its State AG Training Materials

After two boxes of un-encrypted backup tapes were lost in shipment (and following a two-year investigation by the Attorney General of Massachusetts) South Shore Hospital (SSH) in Massachusetts has agreed to a settlement of $750,000 for failure to adequately safeguard patient health information under the Health Information Portability and Accountability Act (HIPAA) and state consumer protection laws. SSH's settlement, much like the federal Office of Civil Rights' (OCR's) “Resolution Agreements” also requires broad and ongoing compliance and third-party auditing activities likely to result in substantial additional costs. The state's action could be seen as emblematic of a new rise of state, rather than federal, enforcement action against both providers and their business associates. State attorneys general, thanks to changes made by the Health Information Technology for Economic and Clinical Health (HITECH) Act, are learning to wield newfound authority to bring lucrative civil actions based on violations of federal HIPAA requirements and state consumer protection and privacy laws.

SSH became the subject of the state's investigation after losing two boxes of un-encrypted backup tapes containing patient names, social security numbers, financial account numbers, and the medical diagnoses of over 800,000 individuals. SSH had retained a third-party contractor, Archive Data, to erase the backup tapes and resell them. Three boxes containing 473 tapes were shipped to Archive Data. SSH later learned that only one of the three boxes containing records had reached its intended destination. The other two boxes were simply lost along the way. In addition, the Attorney General of Massachusetts alleged SSH lacked a business associate agreement with Archive Data, had failed to inform Archive Data that the tapes contained protected health information (PHI), and had not properly trained its staff with respect to appropriate health data privacy protocol.

Under the consent judgment, SSH agreed to pay a total of $750,000. $250,000 of the judgment was dedicated to the payment of a civil penalty; $225,000 was dedicated to a state fund to be used at the discretion of the Attorney General in support of the creation of educational programs for the protection of PHI. SSH was “credited” the final $275,000 in return for the extensive security measures already implemented and agreed to in the settlement. Under the consent judgment, SSH is obligated to take a variety of measures to ensure compliance with state and federal security laws and regulations, including the creation of standardized and approved business associate agreements, extensive yearly work force training, and the engagement of an independent third-party auditor with the results reported to the Massachusetts Attorneys General.

Providers should not mistake the SSH settlement as an anomaly or the result of a particularly egregious violation. The HITECH Act has allowed state attorneys general to pursue parallel state and federal actions related to privacy laws, and in turn, to increase potential settlement amounts with providers. And, increasingly, state enforcement authorities are becoming comfortable bringing enforcement actions for what providers might consider “minor” breaches, or simple mistakes. In 2010, attorneys general in Connecticut and Vermont brought suit against insurer Health Net as a result of security breaches of patients' PHI. Health Net later settled for approximately $300,000. Likewise, in January 2012, the Minnesota Attorney General brought an enforcement action against a business associate, Accretive Health, for HIPAA violations following reports of the theft of an

unencrypted laptop computer containing PHI. And, OCR has continued to encourage state-level enforcement actions. It recently made available to the public, for instance, the materials used during the June 2011 Safeguarding Health Information Building Assurance through HIPAA Security Conference.

The now public training materials are indicative of the increased focus placed on state-level enforcement activity. The materials include both video and computer training modules on how to both identify and investigate potential HIPAA violations, among other topics including:

- General introductory materials to the HIPAA Privacy and Security Rules;
- Discussion of the HITECH Act;
- OCR's role in enforcing the HIPAA Privacy and Security Rules;
- Resources for state attorneys general in pursuing potential HIPAA violations, including OCR guidance documents and case studies;
- Relationship between security violations and privacy violations under HIPAA; and
- The interaction between HIPAA and state law.

The materials make clear that OCR expects that state authorities will take a more active role enforcing both state and federal privacy laws in the coming years.

Ober|Kaler's Comments

The SSH settlement is instructive in several respects. First, covered entities must ensure that their compliance programs cover both federal and state laws, and are regularly reviewed and updated as required by changes to either. Second, providers should keep in mind that state law may require additional compliance steps (SSH's settlement, for instance, references several Massachusetts-specific requirements). Finally, providers should note that settlements can be negotiated. While SSH's settlement itself totaled over $700,000, over a third was credited back to SSH in response to the security and privacy measures taken following the 2010 data breach, and reflecting the added costs of the measures mandated by the settlement itself.

Finally, providers should note the increased enforcement efforts to promote state-level enforcement. State attorneys general may choose to bring actions under HIPAA, but they may also choose more expansive or vague state consumer protection laws. Increasingly, a well-prepared provider will need to be fluent in both.