Thomas D. Bixby
Law Office LLC
Legal Advice for Health Plans

PRIVACY LAW ALERT
September 18, 2012

Increased Scrutiny of Privacy, Security Practices

Office for Civil Rights Settles HIPAA Security Rule Case for $1.5 Million
Eleventh Circuit Allows Suit Against Health Plan for Stolen Laptop

Two unrelated actions in the past two weeks provide evidence that privacy and security practices are under greater scrutiny. In a release issued this week, the Department of Health and Human Services (HHS) announced a settlement with a health care provider for the provider's alleged failure to implement reasonable security measures for electronic protected health information. The settlement required the provider to pay HHS $1.5 million and engage in a corrective action plan, lasting over three years. Less than two weeks earlier, the Eleventh Circuit Court of Appeals overturned a Florida District Court's decision to dismiss a case against a Florida health plan in a class action lawsuit arising out of the theft of two laptop computers containing unencrypted protected health information of 1.2 million current and former health plan members.

Together with the HHS Office for Civil Right's audit program (click here for my Health Law Alert on subject), these actions demonstrate the increasing attention—and liability—that health plans and their vendors are subject to for their privacy and security practices. Click here for HHS's media release concerning the settlement and click here for the Eleventh Circuit's decision.

HHS Settlement: Massachusetts Eye and Ear Infirmary

In April 2010, the Massachusetts Eye and Ear Infirmary (the Infirmary) reported to HHS a breach or protected health information arising out of the theft of a laptop. Nearly six months later, HHS initiated an investigation of the incident. HHS determined that the Infirmary failed to comply (or failed to demonstrate that it had complied) with a variety of HIPAA Security Rule requirements. Among the findings was that the Infirmary:

- "[D]id not demonstrate that it conducted a thorough analysis of the risk to the confidentiality" and, "[i]n particular, [the Infirmary] did not fully evaluate the likelihood and impact of potential risks to the confidentiality of [electronic protected health information] maintained in and transmitted using portable devices."

- Failed to implement "security measures [that were[sufficient to ensure the confidentiality of [electronic protected health information] that it created,

maintained, and transmitted using portable devices" starting with the compliance date of the Security Rule.

- Failed to "adequately adopt or implement policies and procedures to address security incident identification, reporting, and response from the compliance date of the Security Rule to [the date of the laptop theft]."

- Failed to "adequately adopt or implement policies and procedures governing the receipt and removal of portable devices that access [electronic protected health information] or to provide [the Infirmary] with a reasonable means of knowing whether or what type of portable devices were being used to access its network from the compliance date of the Security Rule to [the date of the laptop theft]."

Thus, HHS made clear that a fundamental Security Rule requirement is that covered entities perform "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information." In addition, HHS determined that the Infirmary either failed to encrypt electronic protected health information or, in the alternative, failed to "implement an equivalent, reasonable, and appropriate alternative measure to encryption that would have ensured confidentiality of its [electronic protected health information] or document the rationale supporting the decision not to encrypt." Thus, HHS demonstrated that it intends to enforce the standard for "addressable" implementation specifications, such as encryption. Under this standard, covered entities (and pursuant to the HITECH Act, their business associates) must either implement an "addressable" safeguard (if reasonable and appropriate under the circumstances) or document why implementing the safeguard is not reasonable and appropriate and implement "an equivalent alternative measure if reasonable and appropriate."[1]

The settlement requires the Infirmary to enter into a corrective action plan that will last for over three years. Under the plan, the Infirmary must review and revise its security policies and procedures, submit them to HHS, incorporate suggestions from HHS and implement the policies and procedures. The provider must train its personnel on the new policies and procedures and contract with an independent monitor (subject to HHS approval) who will monitor implementation of the corrective action plan.

Eleventh Circuit Decision

In *Resnick v. AvMed, Inc.*, the Eleventh Circuit Court of Appeals (Alabama, Florida, and Georgia) held that plaintiffs, representing a class of over 1.2 million individuals whose

[1] If no equivalent alternative measure is reasonable and appropriate, the covered entity (or business associate) may decide not to implement any safeguard for the implementation specification, but it must document its decision.

unencrypted protected health information was on two stolen laptop computers, successfully pleaded a cause of action against AvMed, a Florida insurer. The Court determined that the plaintiffs were entitled to argue that the theft of the laptop was the cause of subsequent identity theft and that the AvMed was liable for damages arising out of the incident under five theories:

(1) Negligence;

(2) Breach of contract;

(3) Breach of implied contract;

(4) Breach of fiduciary duty; and

(5) Unjust enrichment (restitution).

Although the plaintiffs have not yet proven their case, the Eleventh Circuit's decision suggests that entities that maintain protected health information should expect to be held responsible for safeguarding that information. As the Court opined:

> "In this digital age, our personal information is increasingly becoming susceptible to attack. People with nefarious interests are taking advantage of the plethora of opportunities to gain access to our private information and use it in ways that cause real harm. Even though the perpetrators of these crimes often remain unidentified . . . Plaintiffs [in this case] have pled a cognizable injury and have pled sufficient facts to allow for a plausible inference that AvMed's failures in securing their data resulted in their identities being stolen."

* * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or TBixby@tbixbylaw.com

Thomas D. Bixby Law Office LLC
(608) 661-4310 | www.tbixbylaw.com