December 2014

Hospital Data Breach a Costly Reminder of PHI Responsibilities

An increasing number of state attorneys general are sending a very clear message to holders of patients' medical information (otherwise known as "protected health information" or "PHI"): protect PHI, or be prepared to pay. Although the US Health and Human Service's Office for Civil Rights generally prosecutes HIPAA violations, the HITECH Act empowered state attorneys general to file suit on behalf of their state's residents for HIPAA violations. And since Congress expanded HIPAA enforcement to the states, officials in several states have sued PHI holders following a data breach.

Unencrypted Laptop and Unlocked Door Lead to Trouble

A very instructive example of this extended HIPAA enforcement power surfaced in November 2014, when Beth Israel Deaconess Medical Center of Boston agreed to pay $100,000 to settle a civil suit filed by the Attorney General of Massachusetts following a data breach at the hospital. The Beth Israel settlement stemmed from the May 2012 theft of an unencrypted personal laptop that contained the PHI of nearly 4,000 individuals. The laptop was taken from a physician's unlocked, unattended hospital office. Beth Israel knew of and authorized the physician's use of the personal laptop while at work, which the physician used to store patient records and download emails that contained PHI. Although Beth Israel had a policy requiring the encryption and secure storage of laptops containing PHI, the physician failed to follow the policy on both counts. To worsen matters, Beth Israel failed to notify patients of the data breach within the HIPAA-mandated timeline following the discovery of the theft. In announcing the settlement terms in November 2014, Massachusetts Attorney General Martha Coakley stressed the importance of implementing and enforcing data security policies. In addition to

the $100,000 payment for the breach, Beth Israel also agreed to reeducate its workers on PHI protection and to enact more vigorous encryption compliance policies.

In Massachusetts, the Beth Israel settlement stands as just one of several similar data breach enforcement actions by the State Attorney General in recent years. Since 2012, Massachusetts has reached settlements of $150,000 (Women & Infants Hospital of Rhode Island), $140,000 (Goldthwait Associates), and $750,000 (South Shore Hospital) for the failure to secure PHI.

Increased State Attorney General Enforcement of HIPAA

The HITECH Act permits state attorneys general to initiate a civil suit against alleged HIPAA violators, both to stop data breaches and to obtain damages for harm caused by a breach. Within a year of the law's passage, Connecticut became the first state to use these powers when its Attorney General sued managed care organization Health Net for losing an external hard drive and delaying the required notifications for the data breach. As part of its settlement, Health Net paid $250,000 and agreed to a corrective action plan to improve its security policies. Vermont followed suit, and brought a lawsuit against Health Net in connection with the lost external hard drive, settling for $55,000.

Proactively Working to Prevent a Lawsuit

The lessons embedded in these lawsuits are threefold:

- Develop clear policies about device use, encryption, storage, and protection;
- Enforce those policies; and
- Where a breach may exist, be diligent in promptly notifying the required parties.

State attorneys general have very clearly shown that the failure to protect PHI and timely report data breaches will not be excused — even when theft is involved. PHI holders can proactively protect PHI – and themselves – by developing a strong set of policies to manage data security, by enforcing those policies, and by promptly reporting a breach. Anything short of this invites a costly reminder of the failure of protecting PHI.