SmartFocus on HIPAA Compliance

A **SmartBrief** Education Update

SPONSORED BY BoardEffect

FALL 2016

PROTECTING ePHI ON YOUR BOARD PORTAL

Does your board portal support your HIPAA compliance program? Why it should and how you can make that happen.

While security breaches at retailers grab a lot of the headlines, cybercriminals are actually attacking the health care industry more than any other sector, according to IBM's 2016 Cyber Security Intelligence Index. Last year alone, the study found, more than 100 million health care records were compromised.

The effects of stolen credit card information can be mitigated in a relatively short time frame, minimizing the damage. But Protected Health Information (PHI) and Personally Identifiable Information (PII) are with a person forever, and theft of this sensitive information is far more difficult to resolve. Organizations are required by federal law to report breaches of PHI. The reputational effects of such notification should not be underestimated.

Health care organizations—from small hospitals to universities and nationwide networks and their business associates—gather and store all three kinds of sensitive data. That means it's more important than ever for health care organizations to safeguard this information throughout the enterprise, including board portals.

BOARDS MUST PROTECT SENSITIVE DATA

Boards that handle sensitive and highly personal information, such as Protected Health Information (PHI), often must comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Heath Information Technology for Economic and Clinical Heath (HITECH) Act.

These regulations establish technical, administrative and physical controls for your organization and those you do business with. The regulations specify required controls, including policies for data management and encryption, risk analysis, auditing, and how to respond when a data breach occurs.

Under HIPAA, your organization is also responsible for ensuring compliance by the vendors and contractors with whom you share PHI, including the provider of your board portal. You must have a Business Associate Agreement (BAA) in place with such vendors to document compliance obligations by these outside entities. The penalties for noncompliance can be high.

For example, in March 2016, North Memorial Health Care of Minnesota agreed to pay a $1.55 million fine related to charges of potential HIPAA violations. According to the Department of Health and Human Services, the not-for-profit health care system didn't enter into a BAA with a major contractor and neglected to perform a risk analysis on patient-information security.

Beyond HIPAA and HITECH, the Securities and Exchange Commission holds boards accountable for lax security policies and procedures around PHI and PII. This means that board members must take appropriate risk-management strategies in all areas—credit, operations and cyber.

Customers, stakeholders and shareholders expect more, too. After the data breach at Target in 2013, a proxy firm for shareholders recommended the ouster of seven board members. While the board survived the effort, not all management survived the breach, and the litigation continues to this day. The Target case is one of many that highlight the pressure and responsibilities of the board to reasonably and appropriately protect data.

REAL-WORLD DATA SECURITY IN THE BOARD ROOM

It's particularly important to ensure board compliance with HIPAA because many board portals store PHI, and most board members aren't intimately familiar with the regulations' requirements around handling this sort of data.

These types of sensitive information are frequently included in committee reports, as anecdotal mentions in board books, reviews of medical claims, or even

Data security with BoardEffect

"The health care industry faces an escalating need to ensure data security, especially with the vendors and third parties they trust for their technology services," said Todd Gibby, CEO of BoardEffect.

That's why BoardEFfect underwent a risk analysis. BoardEffect goes beyond the required controls for HIPAA compliance, for example implementing data encryption, one of the more significant controls for any sensitive data.

"This allows customers to align the platform with their specific technical, legal and regulatory requirements to keep ePHI secure," said BoardEffect chief technology officer Michael Scappa.

More than 40% of BoardEffect's customers are health care organizations, from local hospitals with small boards to universities and national health care networks with several boards. This gives the company a unique understanding of the specific regulations and security needs faced by boards in this sector.

And it's why BoardEffect signs Business Associate Agreements required by HIPAA, which few providers of board portals do.

Learn more about BoardEffect's Board Portal at http://www.boardeffect.com/.

> "Safeguarding PHI and PII has never been more important to your patients, your board and your bottom line."

Case Study: Failure to protect PHI results in $2.75 million settlement for The University of Mississippi Medical Center

Officials at the University of Mississippi Medical Center (UMMC) launched an investigation after a password-protected laptop went missing from the hospital's Medical Intensive Care Unit (MICU). They determined an MICU visitor had probably taken the laptop.

A subsequent investigation by the Department of Health and Human Services' Office for Civil Rights (OCR) determined that ePHI stored on a UMMC network drive was "vulnerable to unauthorized access via UMMC's wireless network because users could access an active directory containing 67,000 files after entering a generic username and password," according to the OCR report. Among other data in the directory were 328 files including ePHI of about 10,000 patients, some of it dating to 2008.

The OCR investigation determined UMMC was aware of risks and vulnerabilities to its systems for several years but did not take any meaningful risk-management actions until after the breach occurred. The OCR found multiple alleged violations largely resulting from this "organizational deficiencies and insufficient institutional oversight," including:

- Not implementing policies and procedures designed to avoid, detect, mitigate and correct security violations.
- Neglecting to install physical safeguards to restrict unauthorized use on all workstations with access to ePHI.
- Failing to notify every person whose ePHI was reasonably believed to have been compromised because of the breach

strategic discussions about employee benefits. Even a single piece of PHI requires the same level of compliance as thousands do.

Consider the decision in a case involving Caremark International, In re Caremark Intern. Inc. Derivative Litigation. Casebriefs summarized the finding:

"Directors are potentially liable for a breach of duty to exercise appropriate attention if they knew or should have known that employees were violating the law, declined to make a good faith effort to prevent the violation, and the lack of action was the proximate cause of damages."

Deeper discussion of this case and others is found in Practical Guidance for Health Care Governing Boards on Compliance Oversight, published by the Office of Inspector General, Department of Health and Human Services; the Association of Healthcare Internal Auditors; the American Health Lawyers Association; and the Health Care Compliance Association.

Safeguarding PHI and PII has never been more important to your patients, your board and your bottom line. To deliver the data security required to meet government regulations and patient expectations, make sure the provider of your board portal has developed the appropriate safeguards for HIPAA compliance.

In today's cyber landscape, if you're not discussing data security, liability and risk with your board and your vendors, you're behind the curve. All parties need to know the risks and their responsibilities to protect the data in your board portal. ■

BOARDEFFECT