10 Policies for Protecting Patient Data in 2015

I recently looked up the origin of the word patient. According to one source, it "comes from the Latin 'patiens,' from 'patior,' to suffer or bear." I found this definition disturbing, because I believe that most patients actively participate in their health care.

Patients have little or no control over the privacy of their data, however, that's the provider's job. That is a whole lot harder than it used to be, given the increase in PHI-related data security incidents.

Strategies for managing incident response have not kept pace with evolving threats and changing regulations, which puts patient data and health at even greater risk.

Here are 10 strategies for both covered entities and their business associates to safeguard patient information in 2015 and beyond:

1. Demand organizational leadership engagement. Workforce training and safeguards alone will not be effective. Organizational leadership must embrace and champion compliance as it would any other compliance throughout the organization by setting expectations and holding all workforce members accountable to the same standards

2. Make incident response management a priority. Organizations must make use of smart and purpose-built software automation for assessing incidents and managing incident response, to better mitigate risks to their patients, reputation, and bottom line.

3. Find and identify your data. Organizations need to know where their data lives, where it travels, and in what form (encrypted, identified, de-identified, etc.)

4. Control PHI workflow and minimize necessary workforce access. Organizations must find ways to better control PHI workflow within the organization, and movement outside the organization. This not only includes safeguarding it from impermissible uses and disclosures, but will also require integration of HIPAA with other health information protection activities to ensure a single point of control within the organization.

5. Assess risks. Organizations must have solid processes in place for assessing risk with new systems, devices, services and partners and determine how best to use their power as purchasers to weed out those that don't meet best security practices.

6. Prioritize third-party vendor management. Organizations will need help with third-party vendor management to strengthen oversight and review processes. Note that smaller Business Associates are particularly vulnerable since they may not have as many resources to devote to security and compliance, and may be more likely to experience a data breach.

7. Get proactive. The healthcare industry needs to take a proactive stance when it comes to regulations to protect patient health information. Companies that go above and beyond baseline protection requirements will be seen as industry leaders, and patients will choose to use their services over others.

8. Make privacy an integral part of new technology adoption. The pace at which new technology is being introduced into the healthcare industry is increasing, with thousands of new health-related mobile applications available this year, devices such as Apple Watch, and the Internet of Things. But we have little evidence that patient privacy or security features are being considered. The healthcare industry and its technology service providers need to dramatically improve how they take advantage of existing technology as well as how they design, construct and deliver new tools.

9. Measure to improve. You can't manage what you can't measure. The healthcare industry needs to get better at determining key metrics to continuously measure and improve security postures.

10. Look for "non-standard" systems as potential PHI data stores. In particular, voicemail systems, customer service call recording systems, and closed-circuit television systems could all potentially be storing PHI, but may not be as carefully safeguarded as traditional IT systems such as EHRs and patient billing.

Content provided by Government Health IT

January 13, 2015 – Rick Kam

6627 Valjean Ave.
Van Nuys, CA 91406

Phone: +888-959-0220
Fax: +818-356-7187

Email: info@camhipaasolutions.com
Website: www.camhipaasolutions.com