

September 1, 2010

Key Steps to Protecting Electronic Health Records

Quick Links

Choosing and Protecting Passwords

Attack Simulations

CWC's eDiscovery Services

CWC's Digital Forensics Services

Don't Miss Another Advisory!

Subscribe

The age-old tradition of doctor-patient privilege has been the cornerstone of the privacy of health and medical records for decades. In a society where 99% of all documents are created electronically, maintaining that same level of privacy has become exponentially more difficult.

Electronic data is dynamic and can be disclosed in a matter of seconds to an entire audience via email or any social media channel. The authors of electronic health records ("EHR's") now have the obligation of securing and protecting EHR's from unauthorized use, either per regulation or legal precedent.

An electronic health record (EHR) is an electronic version of a patient's medical history that is maintained by the provider over time. This may include all of the key administrative clinical data relevant to the patient's care including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.[i]

The recent trend has been to digitize personal health records and turn them into EHR's.[ii] This process is creating significant challenges for most organizations, and the primary challenge has been to protect and secure EHR's from unauthorized access. ('unauthorized access' is a sanitized reference to a security breach).

In the past five years, according to the Privacy Rights Clearinghouse (www.privacyrights.org), more than 45 Million electronic records (including EHR's) were either lost, stolen by insiders (e.g., hospital or government employees, health IT vendors, etc.) or hacked from outside. Some of the typical schemes include, but are not limited to the following:

- VIP record snooping (e.g., looking at a movie star's EHR's)
- Co-worker, family member, and neighbor snooping
- Financial identity theft (e.g., stealing a patient's personal data (DOB, SSN) and selling it)
- Medical identity theft (e.g., stealing insurance information to obtain free medical care or obtain RX drugs)

Security breaches are not only costly in terms of remediation and sanctions, but an organization's reputation can be greatly compromised when a breach notification is issued and made public on the 6 p.m. newscast. There are many ways for an organization to protect itself from both internal and external threats, but it is important to take a holistic approach - one that protects people, process, and technology.

Protecting EHR's: Key Security Measures to Consider

If it takes an entire village to raise a child, it will take an entire nation to engage in meaningful collaboration and communication to protect and secure EHR's. Some security measures are listed below to help get the dialogue rolling. Please keep in mind that meaningful security measures need to address both internal and external threats, and adequate protection goes well beyond this list.

- Deploy secure IP and virtual private networks (VPN's).
- Initiate an intrusion vulnerability risk assessment.
- Enforce access controls and network-based admissions.
- Inventory all storage devices (i.e., network, laptops, smart phones, etc.) that contain EHR's.
- Encrypt all laptops.
- Establish and enforce security policies that require the use of a high-grade encryption algorithm.
- Consider deploying security information and event management (SIEM) solutions to monitor and protect your IT infrastructure.
- Encourage collaboration between the privacy and security information management functions of your organization.
- Conduct nationwide background checks on each potential employee.
- Establish and conduct periodic nationwide background checks on employees and vendors who have access to EHR's.
- Employ data leakage end-point protection.
- Add an annual penetration test (a.k.a. attack simulation) to your security strategy.
- Assess your vulnerability to a social engineering attack.
- Monitor and deploy software patch updates in a timely manner.
- Stay up-to-speed on the latest rootkits, botnets, and DoS attacks.
- Use and maintain strong passwords [iii].
- Adhere to the IT security requirements of HIPAA and HITECH.
- Maintain routine vulnerability scanning.
- Filter suspect email attachments at the email gateway.
- Monitor logs for worms and other malware infestations.
- Require all smart phones to possess Blackberry-like security features.
- Regularly review and update your information security policies and procedures.

Need more information? Want to schedule a complimentary Digital Forensics and eDiscovery CLE at your firm? Call Continuum Worldwide at 402-699-2199 or visit us at www.continuumww.com/digital

Footnotes

[i] <http://www.cms.gov/ehealthrecords/>

[ii] In 2004, President Bush issued an Executive Order that requires the Department of Health and Human Services (HHS) to study and develop a national health information network (NHIN). With a ten-year deadline, the task of overseeing the system has been left to a newly created HHS Office: The Office of National Coordinator for Health Information Technology, <http://healthit.hhs.gov/portal/server.pt>. In addition, the 2009 Stimulus Law signed by President Obama calls for a system of electronic health records by 2014. The bill allocates up to \$19 billion to implement adoption of the system. See <http://www.privacyrights.org/fs/fs8a-hipaa.htm>.

[iii] <http://www.us-cert.gov/cas/tips/ST04-002.html>