Meaningful Use or Meltdown: Is Your Electronic Health Record System Secure?

Gib Sorebo
Chief Cybersecurity Strategist
Leidos
@gibsoerebo
High Cost of Healthcare Data Breaches

$13.5 K
Medical Identity Theft Victims
The average spent to restore their credit, reimburse provider for fraudulent claims, and correct inaccuracies in health records.

$2.1 M
Healthcare Organizations
The average spent in the past 2 years to resolve consequences of a data breach (with average of 2,700 lost or stolen records).

$6 B
Healthcare Industry
The estimated annual costs of data breaches (based on 50% of 2-year organizational costs times 90% of U.S. AHA registered hospitals).

73%
Patients Ages 18-34
Percentage of patients who will choose another provider post data breach.

Source: Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute
What is an EMR or EHR?

From the Office of the National Coordinator for Health Information Technology:

*Electronic medical records (EMRs)* are a digital version of the paper charts in the clinician’s office. An EMR contains the medical and treatment history of the patients in one practice. EMRs have advantages over paper records.

*Electronic health records (EHRs)* do all those things—and more. EHRs focus on the total health of the patient—going beyond standard clinical data collected in the provider’s office and inclusive of a broader view on a patient’s care. EHRs are designed to reach out beyond the health organization that originally collects and compiles the information. They are built to share information with other health care providers, such as laboratories and specialists, so they contain information from all the clinicians involved in the patient’s care.
Why use an EHR system?

Meaningful Use is a CMS Medicare and Medicaid program that awards incentives for using certified electronic health records (EHRs) to improve patient care. To achieve Meaningful Use and avoid penalties, providers must follow a set of criteria that serve as a roadmap for effectively using an EHR. (Practice Fusion, Inc.)
Recent Healthcare EHR Vulnerabilities

Disturbing state of EHR Security Vulnerability Reporting
“…my subsequent journey into the world of EHR vulnerability reporting left me deeply concerned that our EHR vendors do not have mature reporting systems in place.”
http://smartplatforms.org/2014/04/ehr-security-vulnerability-reporting/

OIG Finds Vulnerabilities in ONC’s Temporary EHR Testing Program
“The OIG report stated, ‘The process of certifying EHRs is designed, in part, to give providers the confidence to know that patient health information is secure and protected," adding, “Our audit revealed vulnerabilities with the temporary EHR certification program.’”

It’s Insanely Easy to Hack Hospital Equipment
In a study spanning two years, Erven and his team found drug infusion pumps—for delivering morphine drips, chemotherapy and antibiotics—that can be remotely manipulated to change the dosage doled out to patients
http://www.wired.com/2014/04/hospital-equipment-vulnerable/

OIG = Office of the Inspector General
ONC = Office of the National Coordinator
EHR = Electronic Health Record
## Cybersecurity Challenges Presented with Electronic Health Records Systems

<table>
<thead>
<tr>
<th>Topic</th>
<th>Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>Like Enterprise Resource Planning (ERP) tools, EHRs present high levels of complexities, dependencies, and opportunities for undetected errors. This also makes changes particularly risky.</td>
</tr>
<tr>
<td>Vendor Dependent</td>
<td>Patching and other maintenance (including operating system patches) are typically controlled by the EHR vendor, making proactive security more difficult.</td>
</tr>
<tr>
<td>Integration and Interoperability</td>
<td>Like many enterprise applications, EHRs like to be on top. Other applications and devices must conform to the EHR protocols, formats, and workflow processes. Integrating with legacy systems, particularly biomedical devices can be difficult leading to workarounds that often compromise security.</td>
</tr>
<tr>
<td>Identity Management</td>
<td>EHRs must support multiple classes of users (e.g., doctors, nurses, billing professionals, other hospitals and medical practices, patients, insurance companies) with varying levels of familiarity with the system, levels of trust, and radically different roles.</td>
</tr>
<tr>
<td>Change management</td>
<td>Many have sophisticated change management features, including development, test, and production environments and tracking of changes. However, the change management is tied to the vendor’s EHR and may not necessarily track other relevant network changes.</td>
</tr>
<tr>
<td>Availability</td>
<td>Some outages may be permissible depending upon usage. If paper or other backups aren't available, patients' lives could be at risk if treatment history, allergies, or other time sensitive information is not available.</td>
</tr>
</tbody>
</table>
Different Classes of Users

Few systems have as much variety where each is both accessing data and providing input and all are vulnerable to the weakest piece:

PEOPLE
Your medical record is worth more to hackers than your credit card

BY CAROLINE HUMER AND JIM FINKLE
NEW YORK/BOSTON | Wed Sep 24, 2014 2:24pm EDT

(Reuters) - Your medical information is worth 10 times more than your credit card number on the black market.

http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
# So What’s So Valuable?

## Typical Health Record Locator

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Phone Numbers</th>
<th>Email Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Birth</td>
<td>Medical Record #</td>
<td>Social Security #</td>
<td>Driver’s License</td>
</tr>
<tr>
<td>Payment Info</td>
<td>Bank Account</td>
<td>Insurer</td>
<td>Credit Card</td>
</tr>
<tr>
<td>Allergies</td>
<td>Genetic Data</td>
<td>Conditions</td>
<td>Blood Type</td>
</tr>
<tr>
<td></td>
<td>Prescriptions</td>
<td>Symptoms</td>
<td></td>
</tr>
</tbody>
</table>

---

[leidos logo]
# RSAC

Compliance Requirements (Meaningful Use)

| Objective: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities |
| Measure: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process |
| Note: This measure only requires a yes/no answer |

| Numerator: N/A | YES | NO |
| Denominator: N/A | | | |

Risk Analysis | Risk Management | Sanction Policy | Information System Activity Review
Typical EHR Architecture

Client – Usually thick client on desktop or in virtual environment (web browser for limited functionality)

Middleware – application server and related programs

Database
Security Limitations/Concerns for EHRs

- Role Mappings
- Accessibility / Extensibility of Security Logging
- Proprietary Protocols
- Interoperability
EHRs – Where are They Vulnerable

Typical Electronic Health Records System and Its Interfaces

- Desktop & peripherals
- Local Clinical Devices
- Local Instruments
- Bed-side technologies
- Local Imaging & Robotics
- Wireless Carts
- Peripherals, devices, instruments, Management
- Wireless Infrastructure
- External and Legacy Systems Interfaces
- Patients, authorized users, Mobility
- External Service Providers (e.g., Labs)
- Research and HIEs
- Government Oversight and Dashboards
- Insurance Companies
- EHR Data Center Backbone
- Multi-media Storage
- Data Center – Host & EMR Data (backend)
- Data Analytics Storage
- Likely Attack Vectors
- Presentation (frontend)
- Reporting Develop, Security Tools
- Business Continuity & Failover
So How Do You Prevent a Breach?

Pragmatic Cyber Defense for Healthcare

- Each layer gives defenders an opportunity to detect and repel attack
- Each layer’s defense can be somewhat porous – perfection not required
- Defenses get stronger as attackers penetrate further inside
- Goal is to give defenders 2 or more opportunities to catch the attack

General Use Networks: Flexibility and Productivity

Clinical Networks
Very Good Protection

Medical Device Networks: Excellent Protection

Datacenters: Good Protection

Security Systems: Better Protection

Authentication Systems: Best Protection

Clinical Networks
Very Good Protection

Medical Device Networks: Excellent Protection
And Segmentation
Tips and Lessons Learned for Better EHR Security

- Cover the basics first
  - Good hygiene and actions in previous slide
  - Implement vendor recommendations
- More log analysis
  - Review usage over time
  - Consider automated tools and products like FairWarning or Iatric
- Pay attention to roles
  - Audit regularly to identify role changes and user departures
  - Understand what roles are able to do or see
  - Watch non-employee roles carefully
- Know your interfaces
  - Where does data come from and where does it go?
  - Identify the most vulnerable and impactful
But How Much Security is Enough?

The industry norms
- Cybersecurity budgets in all industries tend to range from 3 to 10% of IT budget (Gartner)
- For healthcare, that number is closer to 2-5% (McKinsey)
- For many, 2-5% of revenue is typical for an IT budget
- For EHR systems, security should be at least 5-10% of the operational budget

Criteria for additional expenditures
- Regulatory compliance (as much as 50% of security budget)*
- Requirements to meet business continuity objectives
- Desire to meet industry best practices (such as encryption of all portable storage)
- Changing threat landscape
- Easily exploitable vulnerabilities
- Achieving acceptable risk posture (most subjective & hardest to substantiate)

*Based largely on anecdotal experience with electric utilities and healthcare providers
Apply What You’ve Learned Today

- **Next Week You Should:**
  - Learn about your health system’s EHR system if you haven’t already
  - Review or begin to generate network diagrams showing EHR connectivity & dependencies
  - Complete a complete systems inventory portfolio (current state/planned)
  - Start security discussions with your EHR teams and begin collaboration

- **In the Next Three Months you should:**
  - Conduct a security assessment of your EHR system and related components
  - Begin reviewing access logs and consider use of automated tools to identify anomalous activities (e.g., accesses inconsistent with role, excessive downloads/accesses)
  - Develop a comprehensive Security Plan as a top priority initiative
  - Develop a comprehensive remediation program including strategy, roadmap, implementation
  - Assemble policies and procedures, identify gaps
  - Consider seeking outside assistance for expertise and surge support where needed
In the Next Six Months you should:

- Begin implementing the remediation program, any needed architecture changes, related priorities and harden external interfaces
- Ingest EHR log data or output from anomaly detection tool into your SIEM or other centralized log aggregation tool
- Include EHR components in regular vulnerability scans
- Where feasible, implement two-factor authentication for EHR administrative functions
- Investigate the use of anomaly detection tools to detect suspicious activities
- Investigate the feasibility of application whitelisting for EHR components
Questions

Gib Sorebo
Leidos Chief Cybersecurity Strategist
phone: 703-676-0269
e-mail: sorebog@leidos.com