


Electronic Prescription Monitoring and IT/Patient Confidentiality Issues

Portland, Oregon
December 5, 2008

Kyle E. Miller, CISSP
Oregon Department of Human Services
Information Security Officer

Visit our website: <http://www.oregon.gov/DHS/admin/infosec>



Information Security


- Protect the information assets
- Availability, integrity, confidentiality
- Identify risks, review threats, determine probabilities
- Develop business processes and technical solutions to:
 - Mitigate risks
 - Transfers risks
 - Accept risks
- **NOT A TECHNOLOGY-ONLY ISSUE!**



Key Concerns


- Compliance
- Transportation of information
- Business Continuity and Disaster Recovery
- Identity Management
- Access Control

Compliance



- Section 10.1
 - ORS 192.581 to 192.529
 - Federal Regulations or Requirements
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Determination of others (i.e., Centers for Medicare and Medicaid Services – CMS)
- Compliance requirements do not have detailed controls
- Other requirements may be cited (i.e., NIST 800-53, PCI)


Transportation of electronic and other media types



- Electronic reporting (4.2.a)
- Other media types (4.2.e)
- Protective measures must focus on the protection of the all information assets regardless of the media type


• NOT A TECHNOLOGY-ONLY ISSUE!

Business Continuity and Disaster Recovery




- Section 4.1: "...be accessible by practitioners and pharmacies, 24 hours a day, seven days a week"
 - If a hosting solution has only one building, there is always the threat of the hosting solution being unavailable or destroyed. The information assets are unavailable until the systems and information are made moved or the building is usable.
 - If the information must be available no matter the cost, technical solutions are available but with higher costs (i.e., mirrored systems).
- Protection and destruction of other media types must be addressed
- Don't forget personnel

Identity Management



- Foundation to provide or gain access to information assets
- Trusted sources and architecture
 - State Identity and Access Management
 - Pharmacy Board
 - Public Health sources
 - DMV sources
- Multiple identities complicate the business processes and individual management of multiple authentications, i.e., user IDs

Access Control



- Mechanisms (business and technical) to request access and authenticate to the information assets
 - Providers (10.2.a): Staff access
 - Patients (10.2.c): Addressing guardianship
 - States (10.2.f): Recommend an information security professional be involved to assist in determination
 - Education, Research or Public Information (10.2.g): Recommend the use of an Institutional Review Board (IRB) to assist in the determination


Security Management Plan



- The development and implementation of a security management plan will allow the commission and board to identify and address the information security risks.

- Remember:
 - **THIS IS NOT A TECHNOLOGY-ONLY ISSUE!**
 - **THIS IS NOT A TECHNOLOGY-ONLY ISSUE!**

Questions



???
