Electronic Medical Records Data Safety & Security

Patient Data is an ASSET

You need to Protect It
EMR Patient Data Scenario-Multiple Inputs

Integrated Clinical Information System

Data In
- Meditech HiSS
- PAS Module
- Labs Module
- Order Commns
- Diagnostic Devices
  - Incl Physiological Monitors
  - Blood gas analysers
  - Ventilators
  - Infusion Pumps
  - Etc., etc., etc.

Data Out
- PICU
  - Automated Charting
- HDU
- Wards
  
  eICPs Care Pathways
  
  Automated Reporting

Ehealth libraries

HL7
Concerns on EMR Data

- Safety & Security of Patient Data
- Confidentiality of Patient Data
- Misuse of Data
- Availability of Data
- Insurance/Regulatory Issues
Some Guidelines

• ASTM American Society for Testing & Materials (Access Control, Authentication & Non-Repudiation)
• HIPAA- Confidentiality and Security
• NABL- Accreditation of Indian Healthcare Providers-Internationally Accepted
• JCAHO (Focus on Patient Care)
Current Scenario

• NABH has some released guidelines for Accreditation of healthcare providers this year in February 2006
• The Guidelines are designed to bring in standardization in healthcare practices
• NABH certification mandates minimum standards for Manpower, Facilities and Maintenance of records
• Example- Reports are to be stored for a minimum period, Reports have to be signed by Authorized Personnel only
• National registries require medical records to be stored for long periods of time
Insurance and Regulatory

1. Access to Medical Record
2. Data Sharing between healthcare providers and the Insurance Cos – Security & Confidentiality
3. Fraud Control – Incorrect Claims
4. Disease Patterns- Statistics & Risk Assessment
5. Digital Signatures- For Electronic Data Transfer
6. Evolving Regulatory Environment- New Rules keeping the Consumer in Focus
Administrative Procedures for Data Security, Integrity and Availability

- Accreditation
- Data back up Plan
- Disaster Recovery Plan
- Access Management Plan
- Maintenance Plan
- Personnel Policy
- Virus Protection Plan
- User Education & Training Plan
Technical Procedures for Data Security, Integrity and Availability

• Access Control
• Accountability (tracking)
• Data Back up and storage
• Role Based Access
• User Identification
• Alarms and Event reporting
• Audit Trail
• Encryption
• Sign Offs
Access Control
-Log In
Log In history
Confidentiality-
Anonymization of Patient Data when collaborating or sharing data
Creation of security groups for Users
Creation of User Profiles for Access of Data - User Specific Profiles
Access Control Management - Administration
Failed Log in record - Track of Access Attempts
Role based access in Managed Clinic Network
- Need based Access
Conclusion

✓ You can protect the confidentiality and safety of patient data in the Electronic Environment

✓ The administration will need to evolve a policy on the access control management, data back up management & Contingency Plan

✓ Systems and controls need to be built for an effective plan to protect the data of the patient and meet the regulatory needs in the electronic platform
Thank You