MEDICAL RECORDS INSTITUTE

Confidentiality and Security for e-Health

C. Peter Waegemann

CEO, Medical Records Institute (MRI)

Chairman and Acting Director, Centre for the Advancement of Electronic Health Records (CAEHR) UK
Chair, Standards Committee ASTM E31 on Healthcare Informatics
Chair, US TAG to ISO TC 215 on Health Informatics
Chair, ISO TC 215 Task Force on Consumer Interests
Vice Chair, Mobile Healthcare Alliance (MoHCA)

What is e-Health?

- Internet-enabled Healthcare Applications
  - Consumer Health Information
  - Personal Health Records
  - Internet-based Services (e-Pharmacy, e-Care (incl. email and e-communication, etc.)
- Electronic Health Record (EHR) Systems
- Administrative and Financial Health Systems

Importance of Healthcare Security

- Confidentiality/Data Security
- What if something goes wrong?
  - System's Failure (Crash or virus causes loss of data)
  - Outside force damages (hacker, other)
  - Disaster
- Design Issues (Signature, authentication, others)
- Compliance Issues

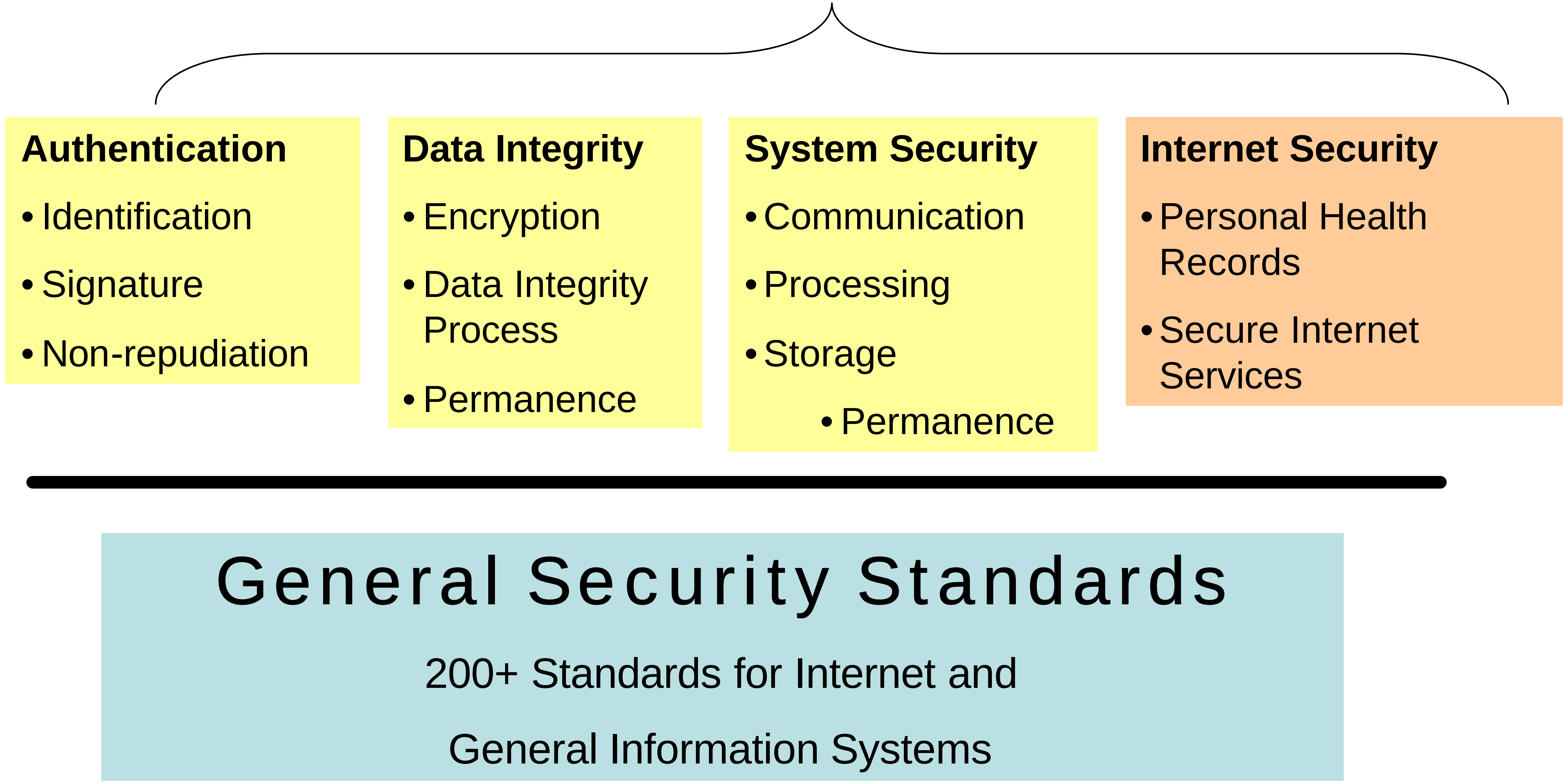
How is Healthcare Security Different From Other Industries?

- Not bilateral conditions
- Regulated (US: HIPAA and other regulations)
- Community interest
- Legal issues

e-Health Security Issues

- Security for (Patient) Confidentiality
- Security that Enables Electronic Health Records
  - Authentication
  - Data Integrity
- Systems Security
  - Secure Transmission
  - Secure Processing
  - Secure Storage
  - Etc.

Healthcare-specific Security Standards



Authentication

- Identification
- Signature
- Non-repudiation

Data Integrity

- Encryption
- Data Integrity Process
- Permanence

System Security

- Communication
- Processing
- Storage
- Permanence

Internet Security

- Personal Health Records
- Secure Internet Services

General Security Standards

200+ Standards for Internet and

General Information Systems

Security on the Internet

- Reliability of Health Information on the Net
- Trust to e-care
- Trust to e-pharmacy

Personal Health Records

- Secure Documentation
- Secure Storage
- Relationship Between the Consumer/Patient and the Website Organization

ASTM E2211

- Data Mining: For IIHI, PCHR suppliers shall allow consumers to choose if and how any personally identifiable information collected from them may be used. These choices shall be presented in a manner requiring that the consumer give specific permission for use of such data.
- Policies: The PCHR supplier shall allow a consumer or other authorized individual easy access at any point in the PCHR application to the policies and standards to which the PCHR supplier site adheres, as well as their associated charges, if any.
- Access: A PCHR supplier shall provide the consumer with the ability to access data within the PCHR in order to verify its correctness or to contest its accuracy and completeness, or both. Access policies shall describe the turnaround time related to such requests (time from request to access), shall specify associated charges, and shall include instructions for contesting and correcting inaccurate or incomplete data.
- Integrity—A PCHR supplier must be able to assure data integrity through audit trails and other security methods and shall disclose its quality assurance policies regarding maintenance of data integrity.
- *Retention*—The PCHR supplier's disclosure statement shall state the length of time that the information will be stored and maintained.

Confidentiality

- Confidentiality is Governed by Local/National Legislation and Provider Policies

E31.17 Privacy, Confidentiality and Access

Chair: *Mary Alice Hanken (mahanken@u.washington.edu)*

Scope: To develop standards that address access, privacy, confidentiality and data security of health information in its many forms and locations.

E 1869 Guide for Confidentiality, Privacy, Access and Data Security Principles for Health Information Including Computer Based Patient Records

E 1986 Standard Guide for Information Access Privileges to Health Information

E 1987 Standard Guide for Individual Rights Regarding Health Information

E 1988 Standard Guide for the Training Persons Who Have Access to Health Information

PS 115 *Provisional Standard Specification for Security Audit and Disclosure Logs for Use in Health Information Systems*

- ***Standards Under Development***
  - **Draft PS 105** *Provisional Standard Guide for Amendments to Health Information*
  - *Draft Standard for Utilization and Retention of Encrypted Signature Certificates*

Security for EHR Systems

- Documentation Method
- Authentication
- Data Integrity
- Systems Security

Mobile Health-care Communication an Computing Device

Any (small) portable and unobtrusive computing and/or telecommunications device that assists in the collection, retrieval or communication of data relevant to medical care

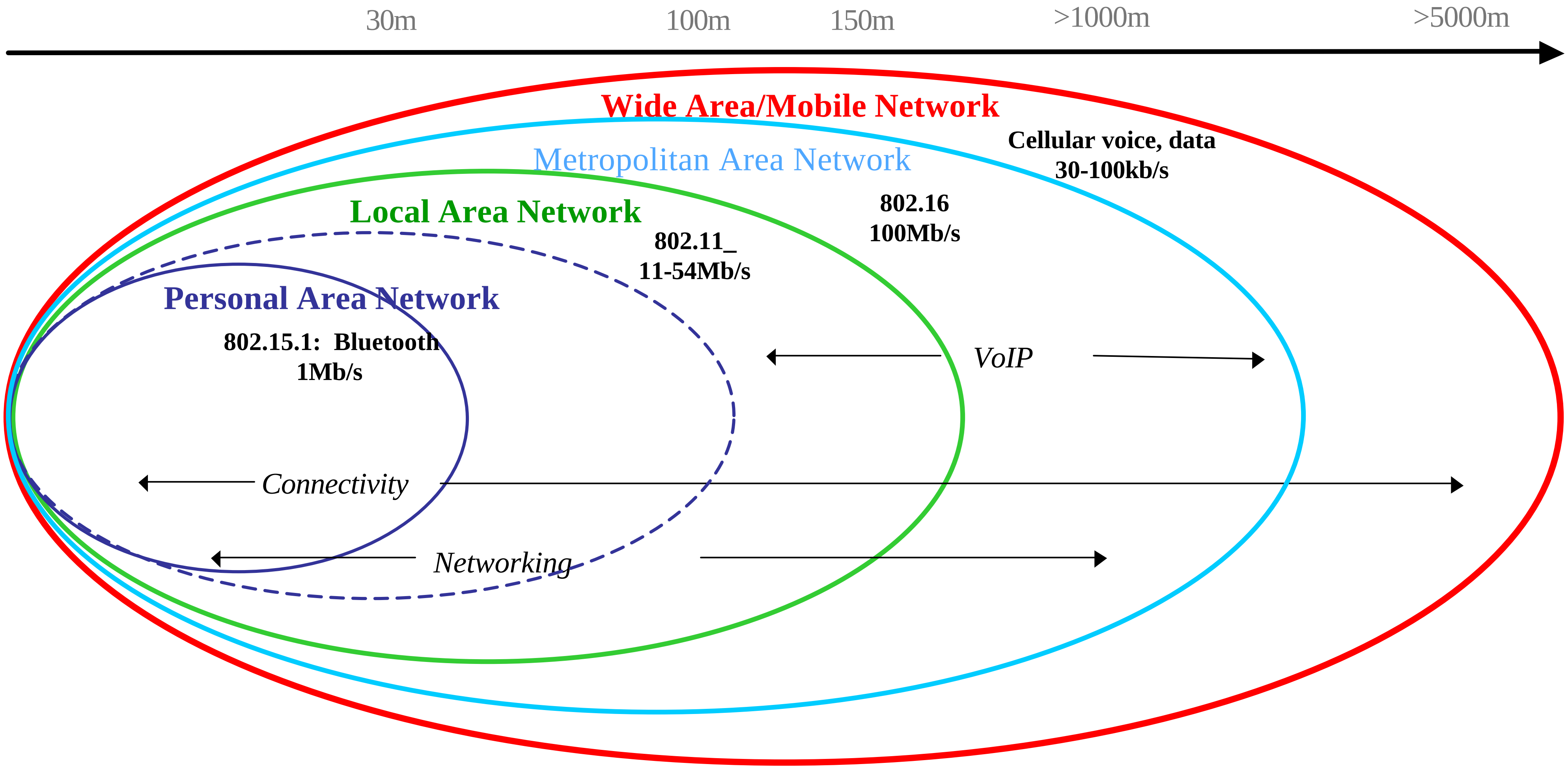
Mobile communications devices and healthcare

- Situation:
  - Mobile wireless devices are entering hospitals and other health care environments
  - Device support applications providing increased productivity and decreased medical errors
  - Past issues with wireless equipment give cause for concern and caution regarding potential issues in their usage
  - Some institutions have issued bans
- What is the appropriate security?
- What security standards are needed?

RF Wireless already seen in hospital

- Paging
- Cellular (incl: Blackberry, RIM)
- Wireless LAN (WiFi)
- Wireless Medical Telemetry System (WMTS)
- Bluetooth
- Radio/TV stations

Wireless technology/application



What Are General Mobile Health Computing (MHCD) Applications?

A. Handheld (Point-of-Care) Information **Accessing** Devices

B. Intermittently Connected Computing Devices

C. Locally (Always) Connected Computing Devices

D. Long-Range Connected Computing Devices

EMI/EMC

- Three Approaches
- Lack of Data on Risk
- Varies by Technology: WiFi not as dangerous
- Ad-hoc Testing

Has the Content Changed Since a Signature Has Been Affixed?

- Need for Determination of Lower Threshold
- Signature is to be Changed When Document is Changed or Deteriorated

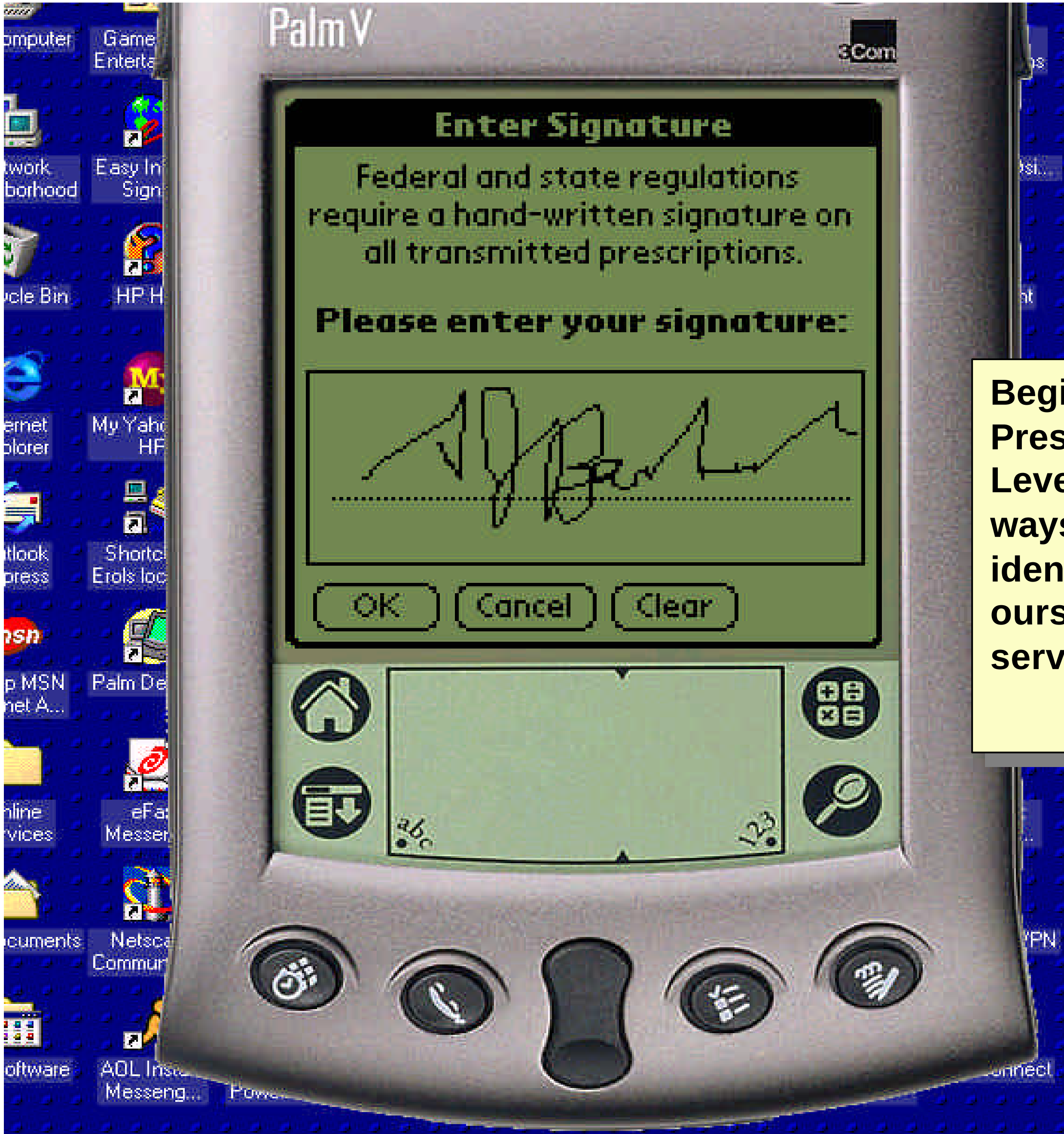
Best

Signature Type	Identification	Encryption	Data Integrity	Signature Action	Document Architecture
Digital Signature	Universally with PKI – Registration Authority – Capture through Token or biometrically	Asymmetric with private and public keys – Certificates from CAs	Hash Function Full guaranteed integrity – full non-repudiation	Conscienscious signing	Binding, compliant with healthcare attributes; amendments managed
Electronic Signature (1)	Bilateral identification with tokens or biometrically	Symmetric encryption	MAC	Conscienscious signing	Binding, compliant with healthcare attributes; amendments managed
Electronic Signature (2)	Bilateral identification with passwords	Symmetric encryption	MAC or less	Conscienscious signing	
Electronic Signature (3)	System/enterprise-wide ID only with passwords or similar	Symmetric encryption	Through audit trail and log-on systems		
Electronic Signature (4)	Passwords				
Electronic Signature (5)	Self-proclaimed			yes	
Electronic Signature (6)	Self-proclaimed			By default	

Least Secure

Biometric Identification

- Identification of Body Parts
  - Fingerprint
  - Retina Scan
  - Face Scan
  - Hand Scan
- Identification of Person-specific Processes
  - Keystroke Recognition
  - Speech Pattern
  - Writing/Signature



Enter Signature

Federal and state regulations require a hand-written signature on all transmitted prescriptions.

Please enter your signature:

Beginning with e-Prescribing. Leveraging better ways of identifying ourselves to other services

Courtesy Andrew Barbash, MD

System Security

- Information Flow (Chain of Trust)
- End-to-End (Point of Origination to Point of Access Security)
- Stewardship Issues
- Accountability
- Audit
- Access Control
- Encryption
- Trusted Data Stores
- Trusted Communications
- Data/Function Classification
- User/Role Clearances
- Non-repudiation
- Signature Architecture
- Back-up/Recovery

Performance

- Response Time
  - Systems failure if practitioner can do it faster and there are no other benefits
  - Dependent on database and technical approaches
    - Database server is bottleneck
- Underlying Technology and Presentation/Navigation Issues
- Scaling

Reliability: Unscheduled Downtime

99.9% Availability → 8.76 unscheduled hours of non-availability

99.999% Availability → 5.25 Minutes per Year

US National Standards

- HIPAA
- E31.20 Data and System Security for Health Information
- E1714-00 Standard Guide for Properties of a Universal Healthcare Identifier (UHID)
- E1762-95 Standard Guide for Electronic Authentication of Health Care Information
- E1985-98 Standard Guide for User Authentication and Authorization
- E2084-00 Standard Specification for Authentication of Healthcare Information Using Digital Signatures
- E2085-00a Standard Guide on Security Framework for Healthcare Information
- E2086-00 Standard Guide for Internet and Intranet Healthcare Security
- E2212-02a Standard Practice Healthcare Certificate Policy
- E31.22 Health Information Transcription and Documentation
- E1902-02 Standard Guide for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records

Regional and International Standards

- CEN TC 251
- ISO TC 215
- Others

Survey

www.medrecinst.com/resources/survey/survey03/index.shtml

- **There is a notable contrast between sectors regarding inappropriate access to patient records by authorized users within the organization**
  - **IHDSOs are very concerned**
  - **Solo/Small practices are much less concerned**
- **The greatest concern of the Solo/Small practices is ‘Access to patient record information by unauthorized users’**
- **The Ambulatory sectors are less concerned about ‘Violations of data security policies and practices’**

Data Security Guidelines, Standards, or Features Implemented or Planned

- **In general, the use of data security protections is fairly high for:**
  - **Access control methods**
  - **Protection of data over networks**
  - **Protection of data within the enterprise**
- **The area where data security protection is least implemented is authentication of users.**

Data Security Guidelines, Standards, or Features Implemented or Planned

- **IHDSOs have significantly higher levels of implementation; Hospitals are slightly above average; Medium/Large practices are about average; and Solo/Small practices fall significantly below average**
- **IHDSOs are especially strong in implementing data security protection within the enterprise (i.e., policies and practices, backup/recovery procedures, and Audit logs)**
- **In contrast, Solo/Small practices are weakest in implementing data security protection within the enterprise**

Summary

- How long will it take to implement a fully operable electronic health record?
  - – A long road ahead
- The same applies to security standards
- Practical security standards needed to cover the current status of EHR developments

Thank you

Attend:
Mobile Healthcare Conference
September 8-10 2003 Minneapolis Hilton

TEHRE 2003 London, England 2-3 December 2003 in conjunction with International ICT Marketplace

Survey on Electronic Health Record Usage and Trends
http://www.medrecinst.com/resources/survey2002/index.shtml

www.medrecinst.com

Copies of these slides may be obtained by emailing peterw@medrecinst.com