AMIA

INFORMATICS PROFESSIONALS. LEADING THE WAY.

3A-3: Security

Thomas H Payne, MD, FACMI, FAMIA

University of Washington

Clinical Informatics
Board Review Course

Clinical Informatics Subspecialty Delineation of Practice (CIS DoP)

Domain 1: Fundamental Knowledge and Skills (no Tasks are associated with this Domain which is focused on fundamental knowledge and skills)

Clinical Informatics

K001. The discipline of informatics (e.g., definitions, history, careers, professional organizations)
K002. Fundamental informatics concepts, models, and theories
K003. Core clinical informatics literature (e.g., foundational literature, principle journals, critical analysis of literature, use of evidence to inform practice)
K004. Descriptive and inferential statistics
K005. Health Information Technology (HIT) principles and science
K006. Computer programming fundamentals and computational thinking
K007. Basic systems and network architectures
K008. Basic database structure, data retrieval and analytics techniques and tools
K009. Development and use of interoperability/exchange standards (e.g., Fast Health Interoperability Resources [FHIR], Digital Imaging and Communications in Medicine [DICOM])
K010. Development and use of transaction standards (e.g., American National Standards Institute X12)
K011. Development and use of messaging standards (e.g., Health Level Seven [HL7] v2)
K012. Development and use of ancillary data standards (e.g., imaging and Laboratory Information System[LIS])
K013. Development and use of data model standards
K014. Vocabularies, terminologies, and nomenclatures (e.g., Logical Observation Identifiers Names and Codes [LOINC], Systematized Nomenclature of Medicine --Clinical Terms [SNOMED-CT], RxNorm, International Classification Of Diseases[ICD], Current Procedural Terminology [CPT])
K015. Data taxonomies and ontologies
K016. Security, privacy, and confidentiality requirements and practices
K017. Legal and regulatory issues related to clinical data and information sharing
K018. Technical and non-technical approaches and barriers to interoperability
K019. Ethics and professionalism

The Health System

K020. Primary domains of health, organizational structures, cultures, and processes (e.g., health care delivery, public health, personal health, population health, education of health professionals, clinical research)
K021. Determinants of individual and population health
K022. Forces shaping health care delivery and considerations regarding health care access
K023. Health economics and financing
K024. Policy and regulatory frameworks related to the healthcare system
K025. The flow of data, information, and knowledge within the health system

Domain 2: Improving Care Delivery and Outcomes

K026. Decision science (e.g., Bayes theorem, decision analysis, probability theory, utility and preference assessment, test characteristics)
K027. Clinical decision support standards and processes for development, implementation, evaluation, and maintenance
K028. Five Rights of clinical decision support (i.e., information, person, intervention formats, channel, and point/time in workflow)
K029. Legal, regulatory, and ethical issues regarding clinical decision support
K030. Methods of workflow analysis
K031. Principles of workflow re-engineering
K032. Quality improvement principles and practices (e.g., Six Sigma, Lean, Plan-Do-Study-Act [PDSA] cycle, root cause analysis)
K033. User-centered design principles (e.g., iterative design process)
K034. Usability testing
K035. Definitions of measures (e.g., quality performance, regulatory, pay for performance, public health surveillance)
K036. Measure development and evaluation processes and criteria
K037. Key performance indicators (KPIs)
K038. Claims analytics and benchmarks
K039. Predictive analytic techniques, indications, and limitations
K040. Clinical and financial benchmarking sources (e.g., Gartner, Healthcare Information and Management Systems Society [HIMSS] Analytics, Centers for Medicare and Medicaid Services [CMS], Leapfrog)
K041. Quality standards and measures promulgated by quality organizations (e.g., National Quality Forum [NQF], Centers for Medicare and Medicaid Services [CMS], National Committee for Quality Assurance [NCQA])
K042. Facility accreditation quality and safety standards (e.g., The Joint Commission, Clinical Laboratory Improvement Amendments [CLIA])
K043. Clinical quality standards (e.g., Physician Quality Reporting System [PQRS], Agency for Healthcare Research and Quality [AHRQ], National Surgical Quality Improvement Program [NSQIP], Quality Reporting Document Architecture [QRDA], Health Quality Measure Format [HQMF], Council on Quality and Leadership [CQL], Fast Health Interoperability Resources [FHIR] Clinical Reasoning)
K044. Reporting requirements
K045. Methods to measure and report organizational performance
K046. Adoption metrics (e.g., Electronic Medical Records Adoption Model [EMRAM], Adoption Model for Analytics Maturity [AMAM])
K047. Social determinants of health
K048. Use of patient-generated data
K049. Prediction models
K050. Risk stratification and adjustment
K051. Concepts and tools for care coordination
K052. Care delivery and payment models

Domain 3: Enterprise Information Systems

K053. Health information technology landscape (e.g., innovation strategies, emerging technologies)
K054. Institutional governance of clinical information systems
K055. Information system maintenance requirements
K056. Information needs analysis and information system selection
K057. Information system implementation procedures
K058. Information system evaluation techniques and methods
K059. Information system and integration testing techniques and methodologies
K060. Enterprise architecture (databases, storage, application, interface engine)
K061. Methods of communication between various software components
K062. Network communications infrastructure and protocols between information systems (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP], switches, routers)
K063. Types of settings (e.g., labs, ambulatory, radiology, home) where various systems are used
K064. Clinical system functional requirements
K065. Models and theories of human-computer (machine) interaction (HCI)
K066. HCI evaluation, usability engineering and testing, study design and methods
K067. HCI design standards and design principles
K068. Functionalities of clinical information systems (e.g., Electronic Health Records [EHR], Laboratory Information System [LIS], Picture Archiving and Communication System [PACS], Radiology Information System [RIS] vendor-neutral archive, pharmacy, revenue cycle)
K069. Consumer-facing health informatics applications (e.g., patient portals, mobile health apps and devices, disease management, patient education, behavior modification)
K070. User types and roles, institutional policy and access control
K071. Clinical communication channels and best practices for use (e.g., secure messaging, closed loop communication)
K072. Security threat assessment methods and mitigation strategies
K073. Security standards and safeguards
K074. Clinical impact of scheduled and unscheduled system downtimes
K075. Information system failure modes and downtime mitigation strategies (e.g., replicated data centers, log shipping)
K076. Approaches to knowledge repositories and their implementation and maintenance
K077. Data storage options and their implications
K078. Clinical registries
K079. Health information exchanges
K080. Patient matching strategies
K081. Master patient index
K082. Data reconciliation
K083. Regulated medical devices (e.g., pumps, telemetry monitors) that may be integrated into information systems
K084. Non-regulated medical devices (e.g., consumer devices)
K085. Telehealth workflows and resources (e.g., software, hardware, staff)

Domain 4: Data Governance and Data Analytics

K086. Stewardship of data
K087. Regulations, organizations, and best practice related to data access and sharing agreements, data use, privacy, security, and portability
K088. Metadata and data dictionaries
K089. Data life cycle
K090. Transactional and reporting/research databases
K091. Techniques for the storage of disparate data types
K092. Techniques to extract, transform, and load data
K093. Data associated with workflow processes and clinical context
K094. Data management and validation techniques
K095. Standards related to storage and retrieval from specialized and emerging data sources
K096. Types and uses of specialized and emerging data sources (e.g., imaging, bioinformatics, internet of things (IoT), patient-generated, social determinants)
K097. Issues related to integrating emerging data sources into business and clinical decision making
K098. Information architecture
K099. Query tools and techniques
K100. Flat files, relational and non-relational/NoSQL database structures, distributed file systems
K101. Definitions and appropriate use of descriptive, diagnostic, predictive, and prescriptive analytics
K102. Analytic tools and techniques (e.g., Boolean, Bayesian, statistical/mathematical modeling)
K103. Advanced modeling and algorithms
K104. Artificial intelligence
K105. Machine learning (e.g., neural networks, support vector machines, Bayesian network)
K106. Data visualization (e.g., graphical, geospatial, 3D modeling, dashboards, heat maps)
K107. Natural language processing
K108. Precision medicine (customized treatment plans based on patient-specific data)
K109. Knowledge management and archiving science
K110. Methods for knowledge persistence and sharing
K111. Methods and standards for data sharing across systems (e.g., health information exchanges, public health reporting)

Domain 5: Leadership and Professionalism

K112. Environmental scanning and assessment methods and techniques
K113. Consensus building, collaboration, and conflict management
K114. Business plan development for informatics projects and activities (e.g., return on investment, business case analysis, pro forma projections)
K115. Basic revenue cycle
K116. Basic managerial/cost accounting principles and concepts
K117. Capital and operating budgeting
K118. Strategy formulation and evaluation
K119. Approaches to establishing Health Information Technology (HIT) mission and objectives
K120. Communication strategies, including one-on-one, presentation to groups, and asynchronous communication
K121. Effective communication programs to support and sustain systems implementation
K122. Writing effectively for various audiences and goals
K123. Negotiation strategies, methods, and techniques
K124. Conflict management strategies, methods, and techniques
K125. Change management principles, models, and methods
K126. Assessment of organizational culture and behavior change theories
K127. Theory and methods for promoting the adoption and effective use of clinical information systems
K128. Motivational strategies, methods, and techniques
K129. Basic principles and practices of project management
K130. Project management tools and techniques
K131. Leadership principles, models, and methods
K132. Intergenerational communication techniques
K133. Coaching, mentoring, championing and cheerleading methods
K134. Adult learning theories, methods, and techniques
K135. Teaching modalities for individuals and groups
K136. Methods to assess the effectiveness of training and competency development
K137. Principles, models, and methods for building and managing effective interdisciplinary teams
K138. Team productivity and effectiveness (e.g., articulating team goals, defining rules of operation, clarifying individual roles, team management, identifying and addressing challenges)
K139. Group management processes (e.g., nominal group, consensus mapping, Delphi method)

Core Content Covered

K016. Security, privacy, and confidentiality requirements and practices

K017. Legal and regulatory issues related to clinical data and information sharing

K070 User types and roles, institutional policy and access control

K072. Security threat assessment methods and mitigation strategies

K073. Security standards and safeguards

Key topics

Key elements of the HIPAA Security Rule.

Policy, and technical measures to protect the security of identified patient health information.

Three technical measures (firewalls, VPNs, and encryption) and the security context in which they are used.

Blockchain

Security threats

Definitions, 1

Firewall: A set of hardware components (router, hosts, and combinations) and networks with appropriate software to restrict network traffic to conform to the security policy of the site. [Zwicky 2000]

Virtual private network: A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and other information transmitted between networks. Because a VPN can be used over existing networks, such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. [NIST, 2008]

Definitions, 2
[hhs.gov, 2007]

Encryption: A method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

Security algorithms and terms

Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES)

Hash: A method of cryptography that converts any form of data into a unique string of text. Any piece of data can be hashed, no matter its size or type.

Secure Hash Algorithm (SHA-1, SHA-256), Message-Digest Algorithm (MD5), Hash Message Authentication Code (HMAC)

Public key encryption: A cryptographic system that uses pairs of keys: public keys (which may be known to others), and private keys (which may never be known by any except the owner).

Zero-day: A newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released.

HIPAA Security Rule, 1.
[hhs.gov]

Covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HIPAA Security Rule, 2.
[hhs.gov]

The Security Rule defines “confidentiality” to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI.

Under the Security Rule, “integrity” means that e-PHI is not altered or destroyed in an unauthorized manner.

“Availability” means that e-PHI is accessible and usable on demand by an authorized person.

Changes to US HIPAA Security and Privacy as part of ARRA

Provisions Include Data Restrictions, Disclosure and Reporting Requirements

Limited Data Sets, Restrictions on Disclosures, Marketing, Reporting Security Breaches, Accounting of Disclosures, Charitable Fundraising, Sales of Protected Health Information

Enforcement: Civil and criminal penalties also apply

HIPAA Privacy and Security rules now apply to Business Associates

- Business Associate Agreements may need to be updated
- BAA must demonstrate documented policies and procedures
- BA must notify covered entity and Secretary of HHS of breaches

What is a covered entity under HIPAA?

HIPAA-covered entities include health plans, clearinghouses, and certain health care providers.

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies*	This includes: •Health insurance companies •HMOs •Company health plans •Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Healthit.gov [Privacy and security guide]

What is a business associate under HIPAA?

A BA is a person or entity, other than a workforce member, who performs certain functions or activities on your behalf, or provides certain services to or for you, when the services involve the access to, or the use or disclosure of, PHI.

Examples of Business Associates

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.

Healthit.gov [Privacy and security guide]

An encrypted laptop from your organization containing PHI on 250 research study patients was misplaced at an airport. Which of the following is true?

A. Your organization must report this to the Secretary of HHS.

B. Because fewer than 400 patients were affected, you are not required to report this to the Secretary of HHS.

C. No report to the press or to HHS is necessary.

D. Individuals must be notified within 60 days of discovery.

An encrypted laptop from your organization containing PHI on 250 research study patients was misplaced at an airport. Which of the following is true?

A. Your organization must report this to the Secretary of HHS.

B. Because fewer than 400 patients were affected, you are not required to report this to the Secretary of HH**S.**

C. No report to the press or to HHS is necessary.

D. Individuals must be notified within 60 days of discovery.

Answer C: Because the laptop was encrypted

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Breach Notification

A breach is the unauthorized acquisition, access, use or disclosure of unsecured PHI which compromises the privacy, security or integrity of the PHI. Unsecured PHI is defined as PHI not secured through technology or method specified by the Secretary through guidance.

Must notify individuals within 60 days of discovery

Must resort to public media notification if > 500 records

Must notify the Secretary without reasonable delay of breaches > 500 records

Must provide Secretary annual report of all breaches

Technical measures

Audit trails

Encryption

VPN

Software discipline

System assessment

Individual (strong) authentication of users

Firewalls

Authentication

Authentication is any process of verifying the identity of an entity that is the source of a request or response for information in a computing environment. It is the linchpin for making decisions about appropriate access to health care information, just as it is for controlling legal and financial transactions. Generally, authentication is based on one or more of four criteria:

1. Something that you have (e.g., a lock key, a card, or a token of some sort);
2. Something that you know (e.g., your mother's maiden name, a password, or a personal ID number);
3. Something related to who you are (e.g., your signature, your fingerprint, your retinal or iris pattern, your voiceprint, or your DNA sequence); or
4. Something indicating where you are located (e.g., a terminal connected to a hardwired line, a phone number used in a callback scheme, or a network address).

Authentication = who you are.

Authorization = What you can do

For the Record: Protecting Electronic Health Information [National Academy Press 1997]

Security – Requirements

Layers of protection

Dynamic, moves with changes

Comprehensive

Commensurate with asset classification, value-adjusted, cost-effective

Consistent with institutional mission and operation

Clear, assigned responsibilities

Metrics

Defense in-depth

Slide courtesy of Soumitra Sengupta

Security concepts

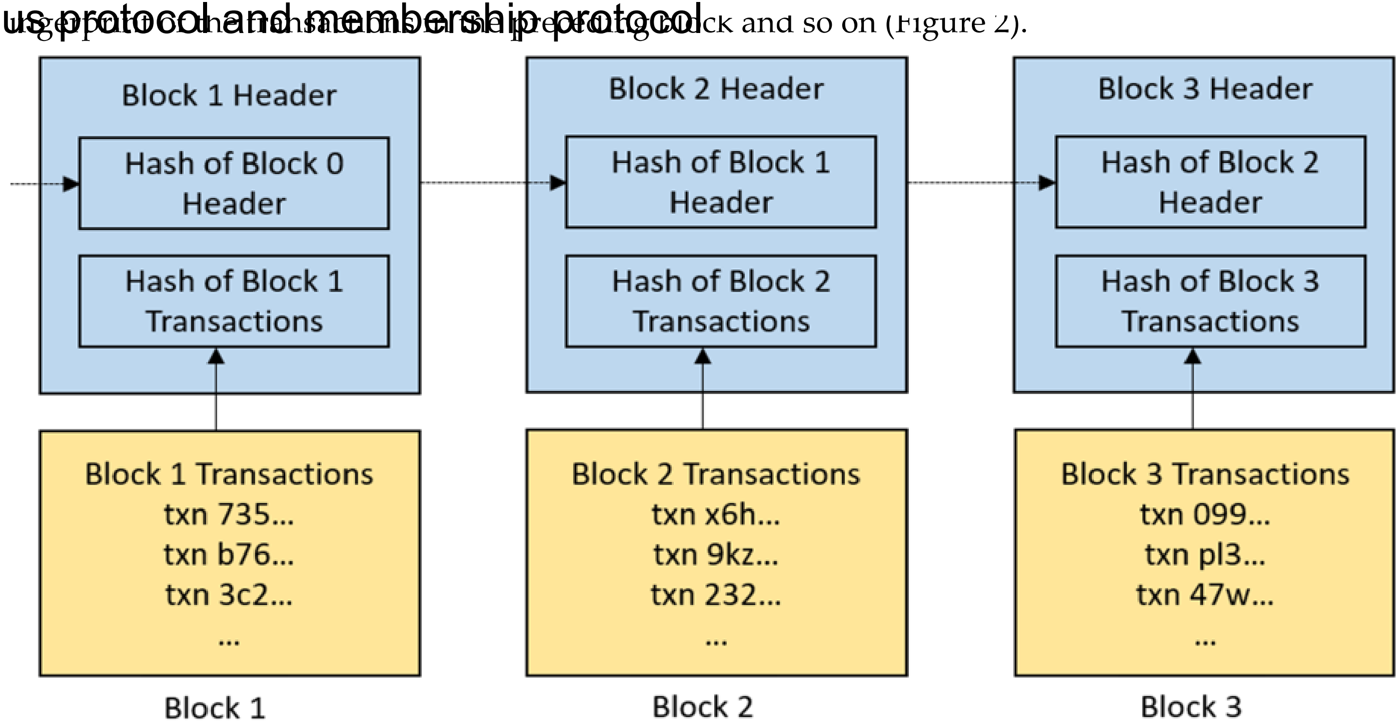
- There are NO perfectly secure information systems
- We have to identify risks specific to an asset based upon possible threats, and then
- Implement and modify security controls to reduce risks, so that
- Residual risks are at an acceptable level.
- Threats may become security incidents, which lead to sanctions and modified security controls

Acknowledge: security controls and ease of access often work against each other

Slide courtesy of Soumitra Sengupta

Blockchain

Hashchain of blocks used to create a distributed ledger in conjunction with a consensus protocol and membership protocol



Agbo 2019

Blockchain in healthcare - Benefits

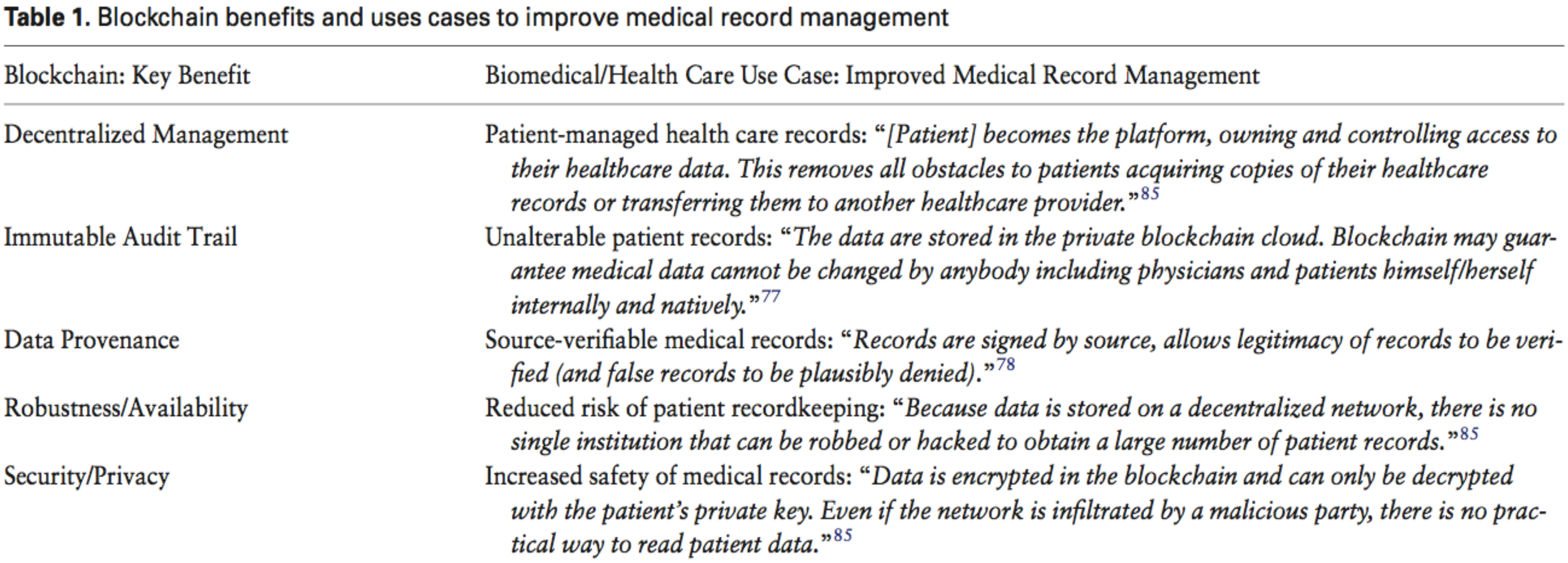


Table 1. Blockchain benefits and uses cases to improve medical record management

Blockchain: Key Benefit	Biomedical/Health Care Use Case: Improved Medical Record Management
Decentralized Management	Patient-managed health care records: "*[Patient] becomes the platform, owning and controlling access to their healthcare data. This removes all obstacles to patients acquiring copies of their healthcare records or transferring them to another healthcare provider.*"[85]
Immutable Audit Trail	Unalterable patient records: "*The data are stored in the private blockchain cloud. Blockchain may guarantee medical data cannot be changed by anybody including physicians and patients himself/herself internally and natively.*"[77]
Data Provenance	Source-verifiable medical records: "*Records are signed by source, allows legitimacy of records to be verified (and false records to be plausibly denied).*"[78]
Robustness/Availability	Reduced risk of patient recordkeeping: "*Because data is stored on a decentralized network, there is no single institution that can be robbed or hacked to obtain a large number of patient records.*"[85]
Security/Privacy	Increased safety of medical records: "*Data is encrypted in the blockchain and can only be decrypted with the patient's private key. Even if the network is infiltrated by a malicious party, there is no practical way to read patient data.*"[85]

Kuo JAMIA 2017 [Link]

Blockchain in healthcare - Limitations

- **Interoperability:** Applications developed by different vendors may not be able to interoperate.
- **Security and privacy:** By linking together sufficient data that are associated to that patient it may be possible to identify the patient. Intentional malicious attacks could compromise the privacy of the patients.
- **Immutability:** Property of blockchain does not augur well with the GDPR's "right to be forgotten"
- **Scalability:** It is not optimal, or even practicable in some cases, to store the high-volume biomedical data on blockchain as this is bound to cause serious performance degradation latency.
- **Engaging patients**: Especially the elderly and the young, management of their data on blockchain may be reduced

Agbo 2019

Security – Controls and Vulnerabilities

Types

- Administrative, Physical, Technical

Administrative examples

- Acceptable Internet Use policy
- Password management policy
- Use & protection of SSN in clinical research data
- Business associate agreement, contracts

Physical examples

- Badge based entry into sensitive areas
- Cameras, RFID based protection in Nursery
- Dual lock system for access to pathogens, access to animal labs
- Essential data center and data closet security

Slide courtesy of Soumitra Sengupta

Security – Technical Controls

Network

- Firewalls
- Intrusion detection and prevention systems (IDPS)
- Network access control (NAC)
- Virtual private networks (VPN)
- Data leakage protection (DLP)

Systems, applications

- Authentication, Authorization, Audit logs (Security Event/Incident Management)
- Patching, up-to-date rules in Anti virus/spyware
- Host based Firewalls, IDPS, DLP
- Encryption, encryption, encryption

Slide courtesy of Soumitra Sengupta

Security Practices Recommended for Immediate Implementation

Technical Practices and Procedures

Individual authentication of users

Access controls

Audit trails

Physical security and database recovery

Protection of remote access points

Protection of external electronic communications

Software discipline

System assessment

Source: For The Record, Institute of Medicine, 1997

Security Practices Recommended for Immediate Implementation

Organizational Practices

Security and confidentiality policies

Security and confidentiality committees

Information security officers

Education and training programs

Sanctions

Improved authorization forms

Patient access to audit logs

Source: For The Record, Institute of Medicine, 1997

Which of the following is usually not part of an organizational security program?

A. Offsite backup with testing of ability to restore

B. Timely patching of device operating systems

C. Creation of Corporate Integrity Agreement

D. External assessment of security vulnerabilities

Which of the following is usually not part of an organizational security program?

A. Offsite backup with testing of ability to restore

B. Timely patching of device operating systems

C. Creation of Corporate Integrity Agreement

D. External assessment of security vulnerabilities

Answer C: Corporate Integrity Agreement

Corporate Integrity Agreements. CIAs impose specific structural and reporting requirements to promote compliance with Federal health care program standards at entities that have resolved fraud allegations.

Security layers

Examples

Physical	Intrusion, fire, power, seismic protection
Network	Firewalls, WEP (wired equivalent privacy)
Social	Phishing, malware, spoofing
Software	Design, updates, authentication
Data	Backup, restore, redundancy

Security Definitions

Malware

Malicious software

Spoofing attack

A person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.

Phishing

A deception perpetrated via email where recipients are enticed into following an attacker's instructions. Following the instructions may take the reader to malicious sites crafted to impersonate valid ones and steal credentials

Denial of service

Attempts to prevent legitimate users from accessing information or services.

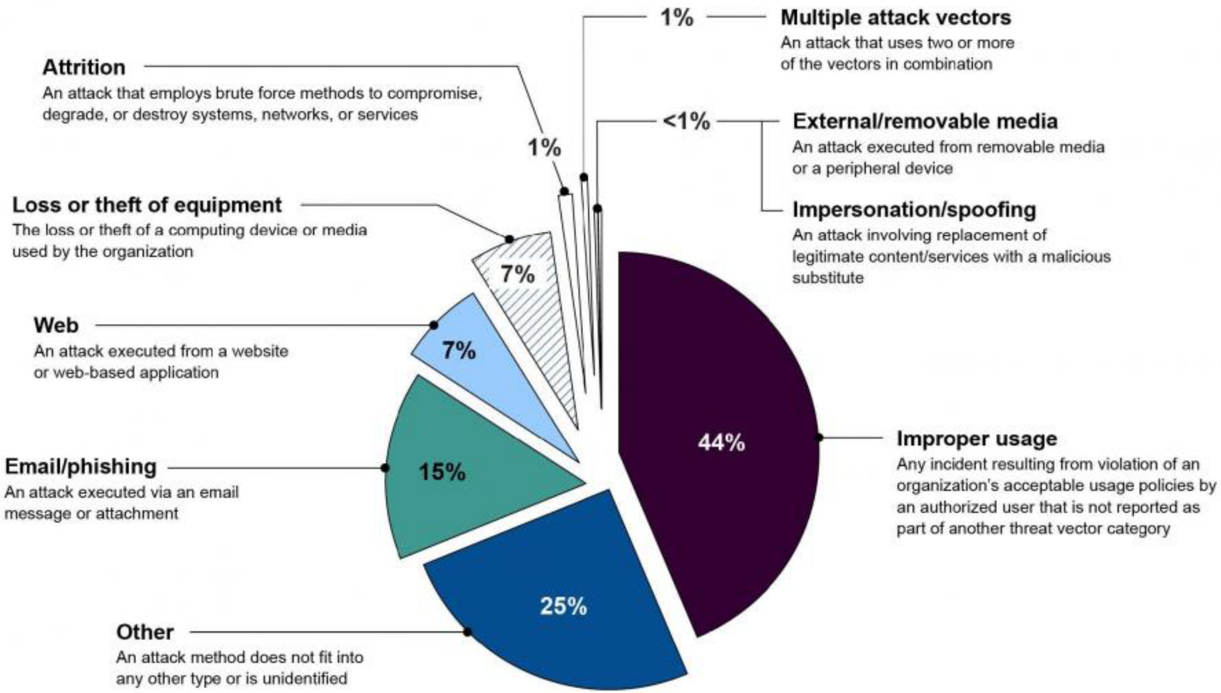
- **Ransomware**

A type of malware that infects computer systems, restricting users' access to the infected systems. Users are told that unless a ransom is paid, access will not be restored.

US-CERT.gov

Evolution of security threats

28,581 total information security incidents



Multiple attack vectors
An attack that uses two or more of the vectors in combination

External/removable media
An attack executed from removable media or a peripheral device

Impersonation/spoofing
An attack involving replacement of legitimate content/services with a malicious substitute

Improper usage
Any incident resulting from violation of an organization's acceptable usage policies by an authorized user that is not reported as part of another threat vector category

Attrition
An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

Loss or theft of equipment
The loss or theft of a computing device or media used by the organization

Web
An attack executed from a website or web-based application

Email/phishing
An attack executed via an email message or attachment

Other
An attack method does not fit into any other type or is unidentified

Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2019.

https://www.gao.gov/cybersecurity

Spoofing is best prevented by:

A. Properly configured firewalls

B. Workforce education

C. Encryption of mobile devices

D. Risk transference programs

Spoofing is best prevented by:

A. Properly configured firewalls

B. Workforce education

C. Encryption of mobile devices

D. Risk transference programs

Answer B: Workforce education

Protection from encryption and firewalls can be overcome by spoofing attacks. Risk transference can mitigate harm, but workforce education is the best preventive measure.

Security Risk Assessment, ARRA

“Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.”

Security threat assessment methods and mitigation strategies

A Threat Assessment is a logical process used to determine likelihood of adverse events impacting your assets and to validate security levels

Identify business needs and changes to requirements that may affect overall IT and security direction. Review adequacy of existing security policies, standards, guidelines and procedures.

Analyze assets, threats and vulnerabilities, including their impacts and likelihood.

Assess physical protection applied to computing equipment and other network components.

Conduct technical and procedural review and analysis of the network architecture, protocols and components to ensure that they are implemented according to the security policies.

Review and check the configuration, implementation and usage of remote access systems, servers, firewalls and external network connections.

Review logical access and other authentication mechanisms.

Review current level of security awareness and commitment of staff within the organization.

Review agreements involving services or products from vendors and contractors.

Develop practical technical recommendations to address the vulnerabilities identified and reduce the level of security risk.

Security Risk Assessment, ARRA

Methods

- Self-assessment of asset owners
- Assessed by internal group
  - Security, Risk management, Internal audit
- Assessed by external group
  - Vulnerability scanners, ethical “white-hat” hackers, external auditors

Measurement

- Qualitative – High, medium, low
- Quantitative – a derived numeric score

Management

- Risk acceptance
- Risk mitigation
- Risk transference

Slide courtesy of Soumitra Sengupta

Security – Incident Handling

- Examples
  - *DMCA violation by students and staff*
  - *VVIP access*
  - *Unencrypted PHI on a desktop*
  - *Malicious user prints identity for identity theft*
- Breach notification process
- Office of Civil Rights (OCR) Audit preparation
  - Risk management portfolio
  - Awareness education
  - Senior management support

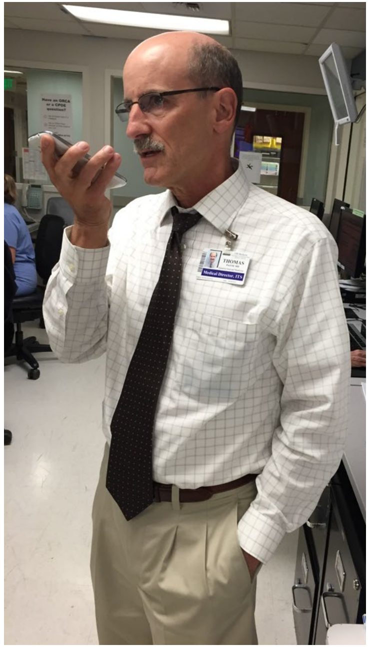
Slide courtesy of Soumitra Sengupta

Bring Your Own Device

Organizations should develop and implement reasonable and appropriate policies and procedures to safeguard health information, including those specific to mobile devices.

Should the organization let providers and professionals use their personally owned mobile devices within the organization?

Should providers and professionals be able to connect to the organization's internal network or system with their personally owned mobile devices, either remotely or on site?



Healthit.gov BYOD

DMARC

Stands for “Domain-based Message Authentication, Reporting & Conformance”

An email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

dmarc.org

Security – Rules & Regulations

JCAHO: Joint Commission on Accreditation of Healthcare Organization – *Information Management*

HIPAA: Health Insurance Portability and Accountability Act – *Information Security of Electronic Protected Health Information. See also references.*

ARRA/HITECH: American Recovery and Reinvestment Act/Health Information Technology for Economic and Clinical Health – *Breach notification, accounting of disclosure, etc.*

Sarbanes-Oxley Act of 2002 – *Audit functions for financial data*

Common Rule (45 CFR Part 46) – *Protection of Human Subjects (Institutional Review Board, GCP)*

21 CFR Part 11 – (FDA) *Data Security, Electronic signatures, etc.*

CDC/NIH/FDA Biological Safety Labs and Bioterrorism, information security

FERPA: Family Educational Rights and Privacy Act – *Medical/Nursing/Dental students' data*

State Laws on HIV and Mental Health Information

State Information Security Breach and Notification Act

State Social Security Number Protection Act

Payment Card Industry Data Security Standard (PCIDSS)

DMCA: Digital Millennium Copyright Act of 1998 – *Copyright violations among immature users*

Key Readings

Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For The Record. Washington, D.C.: National Academy Press, 1997. [Link]

David Chou and Soumitra Sengupta Infrastructure and Security. In Payne TH, (ed). Practical Guide To Clinical Computing Systems. Design, Operations, and Infrastructure. Oxford: Elsevier, 2008.

See also reference list.

References

Agbo CC, Mahmoud QH, Eklund JM. Blockchain Technology in Healthcare: A Systematic Review. Healthcare (Basel). 2019 Apr 4;7(2):56. doi: 10.3390/healthcare7020056. PMID: 30987333; PMCID: PMC6627742. [Abstract]

David Chou and Soumitra Sengupta Infrastructure and Security. In Payne TH, (ed). Practical Guide To Clinical Computing Systems. Design, Operations, and Infrastructure. Oxford: Elsevier, 2008.

Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For The Record. Washington, D.C.: National Academy Press, 1997. [Download]

Dept. of Health and Human Services. Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. Accessed August 9, 2021.

Ford B. Blockchain for Beginners. https://bford.info/log/2016/1102-cybsec-blockchain.pdf Accessed June 27, 2021.

Garfinkel S. Database Nation: The End of Privacy in the 21st Century. Sebastopol: O'Reilly and Associates, 2000.

References (cont'd)

Halamka JD, Lippman A, and Ekblaw A. The Potential for Blockchain to Transform Electronic Health Records. Harvard Business Review, March 3, 2017. [Link]

Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc. 2017 Nov 1;24(6):1211-1220. doi: 10.1093/jamia/ocx068. Review. PMID: 29016974 [Article]

National Institute of Standards and Technology Publication 800-111. Guide to Storage Encryption Technologies for End User Devices. US Department of Commerce, November, 2007. Accessed from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf August 9, 2021.

National Institute of Standards and Technology Special Publication 800-113. Guide to SSL VPNs. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce, 2008. Accessed from https://csrc.nist.gov/publications/detail/sp/800-113/final August 9, 2021.

Taitsman JK, Gromm CM, Agrawal S. Protecting patient privacy and data security. N Engl J Med 2013;368:977-979. [Article]

Zwicky, Elizabeth D., Simon Cooper, D. Brent Chapman. Building Internet Firewalls, 2nd Edition. Sebastopol: O'Reilly Media, June 2000.