Achieving Information Security in Healthcare Information Systems:

An essential challenge for the future of Nursing Informatics

Urmita Banerjee, Prashansa Rao, Pratik Tamakuwala and Güneş Koru (PI)

Health IT Lab @ UMBC

https://hit.umbc.edu

hit@umbc.edu

University of Maryland, Baltimore County
Baltimore, MD

July 19, 2018

Outline

- Introduction
  - Background
  - Challenges
  - Aims
- Methods
- Results
- Discussion
- Limitations
- Conclusion

Introduction: Background – Information Security

- **Methodologies** and **practices** designed to protect information and information systems from unauthorized access, use, disclosure, misuse, modification, or destruction (*NIST-SP800-53A, 2012)*
- CIA triad : **confidentiality**, **integrity**, and **availability**, defines important characteristics of information protected by information security (*SariSternGreene, 2006)*
- In healthcare, US Congress incorporated HIPAA provisions (1996) and amendments (2009) to mandate adoption of Federal regulations for protection of identifiable health information
- **Information Technology (IT)** provides opportunities for better care, better health, and reduced costs (*AHRQ, 2014)*
- Increased use of IT has led to **rapid increase of security breaches** in the healthcare industry in recent years
  - Ransomware attacks - *data encrypted, taken hostage and ransom demanded, care giving impacted (CNBC, 2017)*
  - Anthem data breach - *79 million personally identifiable information stolen (anthem, 2017)*
  - Newkirk unauthorized access notification - *unauthorized access to 3.3 million patient data (bcbs, 2016)*
- So overall healthcare organizations need to improve information security

Introduction: Information Security Challenges

- **Broad range and large volume** of confidential health-related data stored and maintained. Eg. SSNs of healthcare beneficiaries, clinical observations, financial data, reimbursement claims, attestations. (*Cadarette, S.M., 2015)*
- **Data volume** keeps increasing with increasing utilization of health information systems (*HealthDataVolumesSkyrocket, 2017)*
- Most **software systems are large and complex** which makes achieving information security difficult (*Fridsma, 2013)*
- **Standards vs Guidelines:** Guidelines are actions adhering to Standards
- **Current lack of adherence** information security standards and guidelines (*Siponen, 2007)*
- **Adoption** of information **security standards** in healthcare often **complex** interdisciplinary work (*Gomes, R.,Lapao, L. V., 2008)*
  - Standards and guidelines are broad and general (*Hone, 2002; Siponen, 2007)*
  - Lack of evidence supporting the utility of these standards in maintaining security in particular settings (Larrat, 2012; Rees, 2003)
  - Rapid changes in technology, policies, and regulations result in differences in adopting the standards (*Larrat, 2012 ; Rees, 2003)*

Introduction: Research Direction

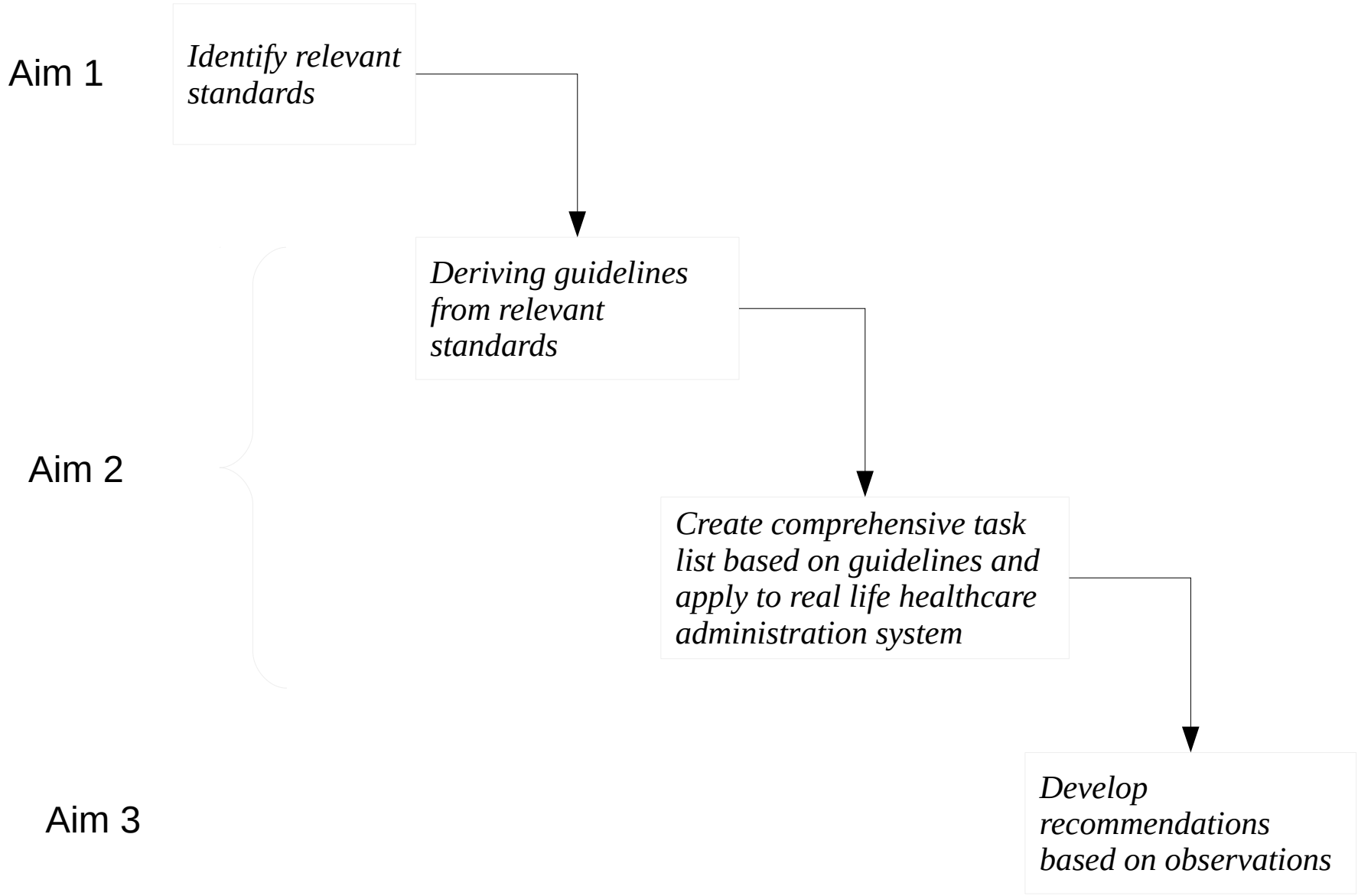
- **Motivation:** Broader adoption of security standards and guidelines can potentially improve the current state of practice in this domain.
- **Gap**: Current lack of evidence about security benefits of adopting standards and guidelines detracts from a broader adoption (*Larrat, 2012; Rees, 2003*)
- **Overarching goal**: Facilitate adoption of standards and guidelines, which, in turn, can help healthcare professionals achieve better security
- **Aims**:

  1. Explore information security **standards** across different industries to identify major standards generally applicable to healthcare sector

  2. Deriving **guidelines** and obtaining **evidence** about their utility by adopting them to improve information security

  3. Provide **recommendations** to improve security of current system being studied and facilitate adoption of security standards and guidelines

Methodological Steps



Methods: Aim 1 – Literature Review

- In-depth review of existing major standards relevant to health information security
- **Purpose**: Ensuring comprehensiveness in the next steps of the study, deriving guidelines and creating a task list
- **Databases** & Search engines used: Google Scholar, EBSCOhost, IEEE Xplore, Science Direct, Elsevier, and PubMed.
- **Keywords** used : information security standards, information security guidelines, information security best practices, IT security standards, IT security guidelines, IT security best practices, health information security, health information privacy, medicaid information security, and medicaid security safeguards.
- In **reviewing titles**, identified articles and papers having informative titles incorporating information like outcome, study design, interventions, etc.
- In **reviewing abstracts**, identified articles and papers providing structured summary providing quick assessment of main idea, validity and applicability of the papers. (*PRISMA, 2013)*
- Based on **eligibility** characteristics such as study question, prime interest and outcomes addressing information security or use of standards for information security, literature was further sorted and reviewed.
- Prominent applicable standards were shortlisted

Methods: Aim 2- Application Context

- A **real-life** government healthcare administration system studied during a year-long security improvement initiative spread over 2016 and 2017
- A **web-based** e-government software application adopted by one of the states in the United States
- **Main purpose**: Collect and approve attestations about compliance with the requirements of a federal incentives program
- Users:
  - Medicaid healthcare providers such as **physicians and hospitals** who received incentives under the program and who provide attestation data as compliance rates
  - State government officials who retrieve, evaluate, and approve attestations
- An **IT vendor** developed the initial system
- System **enhanced later** by second IT vendor in an iterative manner.
- Our study took place while system was being evolved, maintained, and deployed by the second IT vendor.

Methods: Aim 2 – Deriving guidelines

- **Standards identified** through review were examined in detail to derive guidelines by also considering security concerns contextualized to the system
- These **contextualized** security **concerns** serve as requirements in deriving guidelines from the identified standards
- Four main groups of security concerns:
  - **Project**: System size, security budget, organization type, and IT adoption strategy
  - **Process**: Planning, design,implementation, and maintenance
  - **Product:** Functional and non-functional system attributes, hardware and software components, and associated policies, workflows, and physical environment
  - **Information**: Characteristics such as confidentiality, availability, and integrity
- Concerns derived by **understanding** requirements, complexity, dependency on external systems, and communication mechanisms deployed in the **system**.
- **Contextualization** achieved by referring to available **documents** such as system design document as well as on-going verbal and written **communication** throughout the initiative with healthcare professionals and developers.

Methods: Aim 2 – Obtaining Evidence

- A list of **tasks** created from the guidelines.
- **Tasks executed** on the real-life system identified information security problems and directions for improving security
- **Observations** made during this process were noted which provided evidence about effectiveness and efficiency of using standards-based approach.
- **Static Code Analysis** tools such as, Understand TM scitool, FindBugs, OWASP LAPSE project (also known as LAPSE+), and Visual Code Grepper (VCG) used to evaluate the healthcare administration system as part of the tasklist.
- **Static Code Analysis tools** helped :
  - **visualize** and **analyze source code** structure and relationships between different program components, such as packages, classes, and methods.
  - **identify** potential **errors** in source code of the application.
  - **detect** the source and the sink of a vulnerability
  - perform **code review** by identifying bad/insecure code.

Methods: Aim 3 – Providing Recommendations

- Continuous **recommendation & feedback cycle** maintained via email, phone calls, document sharing with healthcare professionals.
- **Source code flaws** making system vulnerable immediately communicated to officials and current developers of system.
- **Technical guidance** provided to immediately patch security problems caused by flaws
- **Final report provided to the officials with suggestions** about future steps that can improve the security of their information system
- **Adopting** relevant security standards to form guidelines about system concerns when applied to the system finds security flaws and helps improve information security

Results: Relevant Standards (Aim 1)

Four major information security standards identified from literature review:

1. **Centers for Medicare and Medicaid Services Acceptable Risk Safeguards (CMS ARS) -** Protects and ensures confidentiality, integrity, and availability (CIA) for all of the CMS' information and information systems.
2. **International Organization for Standardization and International Electrotechnical Commission's Standards (ISO/IEC) 27000 series -** Secures information and provides requirements for establishing, maintaining, and continuously improving information security within an organization. (*ISOStandards, 2016*)
3. **National Institute of Standards and technology (NIST) Special Publication 800 series of Computer Security Publication –** Publishes cyber/information security guidelines, recommendations, and reference materials (*NIST-SP800-100, 2006*). SP 800 series document research efforts in information security by collaborative effort combining work of industry, government, and academic organizations.(*NIST-SP800-30, 2002; NIST-SP800-12, 1995*)
4. **Health Insurance Portability and Accountability Act (HIPAA) Security Rule –** Protects privacy of individuals' health information allowing covered entities to adopt new technologies to improve quality and efficiency of patient care.

Results: Derived Guidelines (Aim 2)

No	Guideline Description	Standards - Referred
1	Examine risk assessment & risk management procedures	HIPAA: 164.308(a)(1)(i), ISO 31000:2009- Risk Management
2	Check identification & authentication of registered users	NIST SP: 800-12, 800-63, 800-73, 800-76, 800 - 78, 800-100, CMS ARS Appendix A (IA)
3	Verify user access management in system	CMS ARS Appendix A (AC), NIST SP: 800-12, 800-100
4	Verify physical and environmental protection	NIST SP: 800-12, 800-100 and CMS ARS Appendix A (PE)
5	Check security awareness and training implemented for the system	HIPAA: 164.308(a)(5)(i)
6	Analyze IT incident response process	HIPAA : 164.308(a)(6)(i), NIST SP: 800-61
7	Analyze contingency planning and procedures	HIPAA : 164.308(a)(7)(i), NIST SP: 800-12, 800 - 34, 800-100
8	Analyze system's media protection policies	HIPAA: 164.310(d)(1), NIST SP: 800-56, 800-57, 800-88, 800-111
9	Check procedures that facilitate implementation of the audit & accountability controls on the system	CMS ARS Appendix A (AU), HIPAA: 164.312(b), 164.308(a)(1)(ii)(D), and 164.308(a)(5)(ii)(C)
10	Examine system's IT security investment and planning	NIST SP: 800-65, CMS ARS Appendix A (SA)
11	Conduct application security testing through source code review and software testing techniques	NIST SP: 800- 115, CMS ARS Appendix A (CA)

Results: Example tasks from the long task list (Aim 2)

No.	Tasks
1	Determine if the system uniquely identifies and authenticates users or processes acting on behalf of the system users.
2	Verify whether risk assessment policies are in place to detect and prevent security violations. Also, determine whether the system has a risk management policy to control uncertainties and risks in a timely manner.
3	Verify and examine whether initial training and awareness provided to the new system maintainers prior to accessing any information in the healthcare administration system. Additionally, verify and examine whether role based security training is conducted.
4	Determine if the system is capable of generating audit records relevant to its security by way of creating logs, error messages, alerts to determine anomalies.
5	Conduct application security testing by applying static code checking tools and perform security testing on the source code
6	……
7	……

Results: Security Problems (Aim 2)

- System **highly dependent** on **external systems** and agencies to function and its authentication functionality is vulnerable
  - Any security vulnerability in the eMedicaid system used for authenticating healthcare administration users automatically **appears** in this system.
- The system is vulnerable to ransomware attack. Healthcare professionals upload word files on the system and **no backup** maintained. All data can get lost with server corruption.
- Documentation for authentication process that should be followed in the system was **unclear and confusing.**
- Important **system reference documents** were found **missing** during security evaluation through formulated security guidelines.
- The system maintainers had **no documentation** for **risk assessment** and **risk management** policies followed for maintaining the system.
- **Physical and environmental documents were incomplete** and poorly documented.
- **No documentation of security training** and awareness programs conducted for the security of the system was maintained
- Information related to **emergency procedures**, such as response procedures, had insufficient information to maintain such a large and complex administration system.

Results: Security Problems – cont'd... (Aim 2)

- System logs for storing error messages were **inefficient** in recording **security-relevant data** required for tracking and investigating security vulnerabilities
- Results from source-code analysis tools prepared **prioritized test plan** to conduct security testing on system's source code base.
- Static code analyzers obtained found several **security vulnerabilities:**
  - **Source code analysis:** No. of files - 1,142 , No. of Program Units - 13,070 , No. of Lines - 257,929
  - **Potential code errors:** Malicious code warnings - 916 , Security warnings – 33
  - **Vulnerability Sources** (points of code that can be source of an attack of untrusted data injection to manipulate application behavior)**:** 82
  - **Vulnerability Sinks** (points of code that can propagate the attack and manipulate application behavior)**:** 16
  - **Code review:** Potential SQL Injection (Critical) - 56 , Operation on Primitive Data Type (High) - 154 , Poor Input Validation (High) – 49, & Potential XSS (High) – 61
  - **Web Parameter Tampering**:
    - **1,600 web URLs** found showing confidential data such as employer identification number, provider address and contact number, etc. publicly by few clicks in the application

Results: Security Problems – cont'd... (Aim 2)

- Testing for URL Manipulation vulnerability **revealed** data about **financial** benefits.
- **Administrator's user account accessible by manipulation of URL**
  - deletion of roles, elevation in access privileges, manipulation of private user information and access to a**pplication without valid login credentials.**

- **Session management vulnerabilities**:
  - Application lacked **renewal of session tokens after successful user authentication** which could lead to **session hijacking**, session fixation, and session puzzling attacks.
  - **Attacker can use a legitimate login** as session ID of an end-user is accessible to him.

- **Reflected XSS attack**:
  - Incorrect data could be entered in HTML tag at login page and cookie details can be accessed from browser via scripts. Hence attacker can generate alerts and pop-ups with messages intended to mislead an unaware end user.

Results: Aim 3 – Recommendations

- The system was in the process of phase two development. **Findings** of the study enabled **second vendor** to substantially **improve** information security.
- Results regarding **applicability of standards** also informed to the officials. The **feedback received was also incorporated in forming the tasks** in the task-list.
- **Source code flaws** or crucial system vulnerabilities were immediately **reported** to government office and current developers and maintainers of the system.
- **Technical assistance** was provided to the developers to **patch** security source code flaws.
- System and its security concerns were identified through **documents** provided by officials and by **direct communication** with them.
- Officials recommended to require thorough **software testing** as part of development process for IT vendors providing software applications.

Discussion

- We provided a **systematic way** of identifying guidelines, creating tasks which detected a large number of security flaws.
- To address security concerns and deliver high-quality healthcare services, certain **policies and regulations are required** (*Chaudhry, 2006*) which need to be identified and applied suiting a specific setting.
- Proper system **documentation** should be maintained by healthcare organizations**.** System in our study lacked system reference documents and documents related to risk assessment, risk management, and contingency plan which made analysis difficult.
- **Security testing** of software should be a mandatory part of software development process. Several malicious source code flaws were discovered which made the system susceptible to security threats like access to cookies , web parameter tampering, etc
- Security attacks have become sophisticated with advancement in IT. Hence, **security patches** must be periodically applied to both software packages and administration systems.
- Healthcare IT needs to **practice heightened vigilance** by complying with federal and state regulations. All parties involved should be made aware of security issues through proper training and education.

Limitations

- Studying one system limits **generalizability** of our initial findings to a wider context.
- On the other hand, some important findings that could be missed during wider analysis were arguably captured in this in-depth study
- The real-life system studied in this research is a **legacy** system and a **lack** of documentation posed some challenges. This was overcome by asking questions and sharing results with the government officials and system maintainers. The feedbacks received helped in overcoming this limitation.

Conclusion

- This study provides useful and interesting **insights** to government officials responsible for implementing and managing healthcare administration systems.
- Government officials should follow **stricter** guidelines for **software** vendors who are developing and maintaining these healthcare administration systems.
- **Ever-increasing** amount of data maintained in healthcare information systems and exchanged with various external entities is subject to a broad range of security **vulnerabilities** (*Appari, 2010*) which can harm individuals and organization in many psychological, physical, or financial ways.
- **Adoption** of relevant Information Security standards and guidelines in a system can help improve its information security. Few examples are:
  - Guideline to check security awareness & training for system
  - Guideline to examine risk assessment and risk management procedures in the system
- **Future research opportunities** may be in form of in-depth case studies, including not only healthcare administration systems, but also other healthcare information systems. Additionally, other topics may be included in this future work such as a) role of government contracts in ensuring security of data; b) role of security standards and guidelines followed by the software vendors; and c)security guidelines followed by the system maintainers.

Questions

- What are the top three information security problems in your organization?
- In what ways would the adoption of standards and guidelines help address these problems?
- What needs to be done in your organization to adopt a systematic approach that follow standards, develop guidelines, and apply tasks to improve information security?

THANK YOU!

Extra Slide

Availability status of documents after conducting security evaluation

No.	Document List	Availability Status
1	Risk assessment and Risk management efforts documents	Unavailable
2	Authentication documents	Incomplete
3	Access-control documents	Incomplete
4	Physical and environmental protection documents	Incomplete
5	Privacy-practices documents	Incomplete
6	Security and privacy awareness documents	Unavailable
7	Response procedures for the IT security incidents documents	Incomplete
8	Continence-planning documents and Emergency power-backup procedure documents	Unavailable
9	Media protection procedure documents	Incomplete
10	Audit and inspection reports and Network access log documents	Unavailable
11	IT investment plan documents	Unavailable