monroe plan
FOR MEDICAL CARE

Healthcare Administrative Systems: Security, Privacy, and Safety in the Age of Crisis and Reform

Howard Brill, Ph. D.
Monroe Plan for Medical Care
IEEE Computing Professionals Conference,
April 21, 2010, Montreal Canada

monroe plan
FOR MEDICAL CARE

Introduction

- "Patients at Veterans Affairs health centers around the country were given incorrect doses of drugs, had needed treatments delayed and may have been exposed to other medical errors due to software glitches that showed faulty displays of their electronic health records."

  Associated Press, 1/13/2009

monroe plan
FOR MEDICAL CARE

Introduction

- "… I have also been surprised by the lack of discussion about patient safety concerns when, for example, HIT products are not functioning properly or when they are being used incorrectly."

Senator Charles Grassley (R-Iowa), Letter to Kathleen Sebelius, February 24, 2010

monroe plan
FOR MEDICAL CARE

Introduction

- "industry enthusiasts … need to prepare themselves for some very bad news. I think that [we will experience a failure claiming many lives] … I think it is unavoidable given what we're doing."
- Enrico Coiera, "Dangerous Decade", 3/2010

monroe plan
FOR MEDICAL CARE

Background

- Historically, there has been a major distinction between administrative systems that supported health care delivery and reimbursement processes versus systems, usually embedded, directly involved in treatment.
- Healthcare IT (HIT) represents the movement of administrative systems into clinical decision-making and automated ordering processes.

monroe plan
FOR MEDICAL CARE

Background

- Political rhetoric in the U.S. concerning healthcare reform is much more extreme than the policy discussions, which share significant commonalities between Democrats and Republicans.
- A major commonality is recognition of the potential of Healthcare IT to improve quality and reduce costs.

monroe plan
FOR MEDICAL CARE

Background

- While healthcare in the United States is technologically advanced, the use of IT in healthcare delivery has been very slow.
- Only very recently has outpatient services begun to shift from paper-based systems to electronic systems. There has been little or no sharing of electronic clinical data.

monroe plan
FOR MEDICAL CARE

Background

- HIT is predominantly see as a way of improving patient safety by reducing the errors due to manual processes, uncoordinated care, and inconsistencies in clinician behavior.
- Information Technology professionals, however, recognize that there are risks associated with technology that must be managed and mitigated.

monroe plan
FOR MEDICAL CARE

Federal Defn of HIT

- ARRA – HITECH Act (2009)
  - Incentives for implementation of Electronic Health Record (EHR) systems
  - Definition of Meaningful Use: Operationalizes HIT definition

monroe plan
FOR MEDICAL CARE

Meaningful Use

- Stage 1 (2011)
  - Electronically capture health information
  - Track key clinical conditions
  - Communicate for care coordination purposes
  - Implement clinical decision support tools
  - Report clinical quality measures

monroe plan
FOR MEDICAL CARE

Meaningful Use

- Stage 2 (2013)
  - Computerized provider order entry (CPOE)
  - Electronic transmission of diagnostic test results

monroe plan
FOR MEDICAL CARE

Meaningful Use

- Stage 3 (2015)
  - Decision support of high priority conditions (guideline based care?)
  - Patient Self Management Tools
  - Population Reporting (including race, ethnicity, primary language, and gender information)

monroe plan
FOR MEDICAL CARE

Standards IFR

- HIPAA Transactions and Code Sets
- HIPAA & HITECH Privacy and Security
- Interoperability and Data Exchange
  - SOAP 1.2 / REST
  - HL7 / ASC X12N / NCPDP
  - UCUM / LOINC / SNOMED Vocabularies
- Functional Requirements (e.g.)
  - Drug-drug interaction alerts
  - Reminder/recall messages
  - Check insurance eligibility

monroe plan
FOR MEDICAL CARE

Standards IFR

- Clarified Security Standards
  - Symmetric Fixed Block Cipher (e.g. AES)
  - IPv6 / IPv4 with IPSec
  - Audit Log
  - SHA-1 hash or better
  - XUA / SAML
  - Disclosure logging
- This is a major change from HIPAA, which did not specify implementation standards for security.

monroe plan
FOR MEDICAL CARE

Certification NPRM

- Federal Proposed Standards
  - ISO/IEC Guide 65: 1996 - Product Certification Systems
  - ISO/IEC 17025:2005 - Testing and Calibration Laboratories
  - ISO/IEC 17011:2004 - Accreditation Bodies

monroe plan
FOR MEDICAL CARE

Safety

- Safety standards are conspicuously missing from the IFR and Certification NPRM
  - There are functional standards but not any standards concerning software development processes.
  - There are standards for the qualification of certifying organizations but no standards for the qualification of software development organizations.
  - The Office of the National Coordinator (ONC) held hearings in February and March on patient safety regulation.

monroe plan
FOR MEDICAL CARE

Safety

- Standards do exist for software embedded in Medical Devices. These are codified into FDA regulations.
- ARRA/HITECH regulations do not discuss the use of these standards.
- Are standards suitable for embedded software in medical devices appropriate to HIT? Would they be effective for HIT, even assuming they are effective for medical devices?

monroe plan
FOR MEDICAL CARE

FDA / Medical Devices/HIT

- HIT does fall under the FDA's medical device regulatory authority.
- The FDA has "refrained" from enforcing regulatory requirements for HIT.

monroe plan
FOR MEDICAL CARE

Medical Device Standards

- ISO 14971 (2000) Application of Risk Management to Medical Devices
- IEC 60601 (2000) Programmable Electrical Medical Systems
- ISO 13485 (2003) Medical Devices – Quality Management Systems
- ANSI SW68 (2001) Medical Device Software, Software Life-Cycle Processes

monroe plan
FOR MEDICAL CARE

FDA Software Regulations

- General Principles of Software Validation (2002)
- Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (2005)
- Guidance for Industry, FDA Reviewers and Compliance on Off-the-Shelf Software Use in Medical Devices (1999)
- 21 CFR 820.30 (g) Software Validation

monroe plan
FOR MEDICAL CARE

Software Standards

- FDA Standards reference NIST 500-234 (1996) Reference Information for the Software Verification and Validation Process

monroe plan
FOR MEDICAL CARE

Critique

- The characteristics, use-cases, and risk profiles of administrative systems differs substantially from medical devices and it is unlikely that standards established for medical devices, even if effective in that domain, will be directly applicable or promote HIT policy objectives.

monroe plan
FOR MEDICAL CARE

Policy Objectives

- Policy objectives are in conflict with a classic software safety approach
  - Interoperability
  - Implementation Speed (COTS)
  - Cost-Savings
  - Innovation
  - Spurring organizational change: software as a driver of change

monroe plan
FOR MEDICAL CARE

Sub-texts

- Discussions are hard to follow without understanding the following sub-texts:
  - Manual paper-based systems kill people.
  - Top-down approaches, e.g. coding systems, have proceeded at a glacial pace. There is a push to "get it done" and not create regulatory obstacles.

monroe plan
FOR MEDICAL CARE

Key Differences

- Emphasis on interoperability across a wide-range of web-connected software and data of various purposes versus specific treatment functions, i.e. qualitatively different degree of complex system interactions.
  - Koppel: HIT is an "ecosystem"
  - Porous system / component boundaries
  - Distributed systems
- Major role of organizational and business/work processes in use-cases.
- Prominence of communication failures in risk profile versus direct physical errors.
- Integral and necessary role of "updates" versus controlled update and maintenance processes
  - Dynamic, continuous updates and improvements

monroe plan
FOR MEDICAL CARE

Effectiveness of Medical Device

- Therac—25 is the best documented and theoretically most important case of software generated fatalities in medical devices.
- Yet in 2010 software-generated radiological accidents remain a significant problem of growing rather than diminishing scale.

monroe plan
FOR MEDICAL CARE

FDA and HIT

- Miller and Gardner 1997. "Recommendations for Responsible Monitoring and Regulation of Clinical Software Systems" JAMIA 4:442-457. Position paper of consortium of associations
  - Proposed FDA regulation of clinical software
  - Scaled levels of regulation based on human intervention
  - Regional Councils / Industry Guidelines
  - FDA declined.
  - Grassley reopens discussion in 2010

monroe plan
FOR MEDICAL CARE

AMIA 1997

- Miller and Gardner recognized the potential complexity of HIT systems
- Recognized interpretation / ergonomic errors
- Still emphasized V&V of "standalone" software, rather than implications of systems failures.
- Interesting analogy to IRBs in regional regulation.

monroe plan
FOR MEDICAL CARE

Scenarios

- Network / System Failure
- Interoperability or interpretation Failure
- Software Error
- Data / Configuration Error
- Ergonomic / Human Interface Failure
- Security Breach: Identify Theft/Borrowing

monroe plan
FOR MEDICAL CARE

Scenarios

- Network / System Failure
  - Beth Israel Deaconess
    - Growing complexity of networked systems causes massive system failure, forcing use of paper and runner-based communications.
    - The failure is not due to a specific software breakdown, but impact of growth on network design and configuration.
    - Business continuity plans did not anticipate configuration collapse.

monroe plan
FOR MEDICAL CARE

Scenarios

- Interoperability or interpretation failure
  - "HL7 is an invitation to negotiate."
  - Local and regional differences in interpreting medical coding.
  - Notable lags in coding systems – CPT4 and labs, ICD-9CM and chronic disease

monroe plan
FOR MEDICAL CARE

Scenarios

- Software Error
  - VA EHR
    - Incomplete data reporting/display
    - Data of different patients displayed simultaneously
    - March 1 shutdown due to systemic error – switch to paper/fax/telephonic communication

monroe plan
FOR MEDICAL CARE

Scenarios

- Data or Configuration Errors
  - Drug/Drug interactions
  - Lab data
  - Paradox of update/maintenance risk
  - Implementation configuration
    - Incorrect assignment of underlying codes to "quick pick lists"
    - Implementation typically requires organizational changes also --- it is not just a software validation exercise.

monroe plan
FOR MEDICAL CARE

Scenarios

- Ergonomic / Human Interface failures
  - A common failure mode with medical devices
  - False alarm problem in drug-drug interactions
  - Diversity of users
  - Patient self-management and literacy
  - Transcription software
    - Tennis Elbow = Tennessee Balls

monroe plan
FOR MEDICAL CARE

Scenarios

- Security
  - "Software Assurance" --- What is the impact of security flaws in software? HIPAA security standards address data-at-rest and data-in-motion, but not software security
  - System shutdowns to halt virus/trojans
  - Identity Theft/Borrowing
    - Mixing of different individuals clinical data

monroe plan
FOR MEDICAL CARE

ONC Draft Recommendations

- Facilitate and encourage reporting
- Vendor Alerts
- "the certification process should require vendors to utilize development processes that insure patient safety."
- Patient Engagement
- Implementation and Training Process
- Interoperability Traceability / Audit trails and logs of interface transactions
- Regional Extension Centers disseminate best practices
- JCAHO inclusion of reporting
- "The FDA: *** To be discussed ***"

monroe plan
FOR MEDICAL CARE

Where to do we go?

- Basic science and engineering
  - System/Network Outages
    - There needs to be greater depth in understanding and mitigating catastrophic failures of complex distributed systems
  - Social-Technical Systems
    - How do you stimulate the development of adaptive, recursively improving systems?
  - Cognitive Science
    - Effective presentation of complex information
    - Awareness of cognitive errors/illusions

monroe plan
FOR MEDICAL CARE

Where do we go?

- Aviation Model versus Medical Device Model
  - National database of HIT patient safety errors
  - Layered Accountability for development, implementation and use
  - Independent investigatory arm
- Certification includes software development standards and training
- Implementation and use includes organizational standards for patient safety policies and training (analogous to HIPAA)

monroe plan
FOR MEDICAL CARE

Where do we go?

- Workforce Development – software safety
- The AMIA's analogy to setting up local and regional boards similar to IRBs / PSOs in more recent literature.