Quality and Risk Considerations for Health Information Technology

Published by AAMI
Acknowledgment
AAMI wishes to thank Brian Shoemaker, member of the AAMI Health Software Quality Management Task Group, for his invaluable role as primary editor for this paper.

For additional information on the AAMI Health Software Quality Management Task Group, contact Wil Vargas at wvargas@aami.org.

Published by
Association for the Advancement of Medical Instrumentation
4301 N. Fairfax Drive, Suite 301
Arlington, VA 22203-1633
www.aami.org

© 2016 by the Association for the Advancement of Medical Instrumentation

Permission is granted to distribute or reproduce this report in its entirety for noncommercial and educational purposes. For other uses, or to order reprints of this report, complete the reprint request form at www.aami.org or contact AAMI, 4301 N. Fairfax Dr., Suite 301, Arlington, VA 22203-1633.
Phone: +1-703-525-4890; Fax: +1-703-525-1067.

Printed in the United States
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee Representation</td>
<td>iv</td>
</tr>
<tr>
<td>I. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Scope</td>
<td>2</td>
</tr>
<tr>
<td>Audience</td>
<td>2</td>
</tr>
<tr>
<td>Flexible approach</td>
<td>2</td>
</tr>
<tr>
<td>II. Quality Considerations</td>
<td>2</td>
</tr>
<tr>
<td>An HIT Product Needs Certain Properties</td>
<td>2</td>
</tr>
<tr>
<td>Design of an HIT System Must Focus on Quality and Safety</td>
<td>3</td>
</tr>
<tr>
<td>Implementation and Deployment Are as Important as Design</td>
<td>3</td>
</tr>
<tr>
<td>Understand the Anatomy of Your HIT System</td>
<td>5</td>
</tr>
<tr>
<td>Every HIT System Needs Maintenance</td>
<td>6</td>
</tr>
<tr>
<td>System Obsolescence/Retirement Presents Unique Challenges</td>
<td>7</td>
</tr>
<tr>
<td>III. Risk Management</td>
<td>7</td>
</tr>
<tr>
<td>Minimize Safety Risk During Design</td>
<td>7</td>
</tr>
<tr>
<td>Build in Cybersecurity</td>
<td>7</td>
</tr>
<tr>
<td>Privacy/Confidentiality, Financial Risk, and Other Areas</td>
<td>8</td>
</tr>
<tr>
<td>IV. Quality Standards for HIT</td>
<td>8</td>
</tr>
<tr>
<td>Why Not Use Existing Standards?</td>
<td>8</td>
</tr>
<tr>
<td>Compare: Medical Device Standards</td>
<td>8</td>
</tr>
<tr>
<td>Quality Efforts for HIT Software Have Begun</td>
<td>8</td>
</tr>
<tr>
<td>V. Summary</td>
<td>9</td>
</tr>
<tr>
<td>Resources for Understanding HIT Safety Issues</td>
<td>10</td>
</tr>
<tr>
<td>References</td>
<td>11</td>
</tr>
</tbody>
</table>
Committee Representation

Association for the Advancement of Medical Instrumentation
Health Software Quality Management Task Group

This white paper was initiated by the AAMI Health Software Quality Management Task Group. At the time this document was published, the AAMI Health Software Quality Management Task Group had the following members:

Co-chair: Michelle Jump, Stryker Instruments Division
          John Murray, FDA/CDRH

Members: Michael Attili, Amaxo Inc
          Pat Baird, Baxter Healthcare Corporation
          Todd Cooper, Center for Medical Interoperability
          Richard DeLaCruz, Silver Lake Group Inc
          Sherman Eagles, SoftwareCPR
          Plamena Entcheva-Dimitrov, Regulatory Consultant
          Megan Hayes, Medical Imaging & Technology Alliance a Division of NEMA
          Rob Hyatt, Intermountain Health Care
          Jeremy Jensen, Boston Scientific Corporation
          Michelle Jump, Stryker Instruments Division
          Patty Krantz-Zuppan, Medtronic Inc WHQ Campus
          Mary Beth McDonald, Mary Beth McDonald Consulting
          John Murray, FDA/CDRH
          Khader Saad, Medtronic Inc WHQ Campus
          Rick Schrenker, Massachusetts General Hospital
          Brian Shoemaker
          Mike Willingham, Caradigm USA LLC
          Daidi Zhong, Chongqing University

Alternates: Cheryl Carey, Medical Imaging & Technology Alliance a Division of NEMA
            Jeff Marshik, Boston Scientific Corporation
            Andrew Northup, Medical Imaging & Technology Alliance a Division of NEMA
            Bakul Patel, FDA/CDRH

NOTE—Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.
Quality and Risk Considerations for Health Information Technology

I. Introduction

Federal incentives and pressure to improve care while reducing cost have spurred healthcare providers to adopt a plethora of software applications in the past few years. Much of this software, commonly referred to as health information technology (health IT or HIT), promises substantial benefits, such as:

I. Improving efficiency and coordination of care among different healthcare providers.
II. Advancing delivery of patient-centered medical care.
III. Helping identify and respond to public health threats and emergencies.
IV. Assisting with health-related research.

In response to a federal mandate in the Food and Drug Administration Safety and Innovation Act (FDASIA), the Food and Drug Administration (FDA), together with the Federal Communications Commission and the Office of the National Coordinator for Health Information Technology (ONC), issued FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework in 2014. In the report, the agencies suggested a strategy for ensuring quality and safety in HIT, as well as proposed restructuring compliance requirements in order to reduce regulatory burden for lower-risk HIT products.

The current paper is intended to build on the concepts in the FDASIA report by providing a set of quality and risk considerations that both healthcare providers (who purchase HIT) and software developers (who develop HIT software) should address.

A number of patient safety issues already have occurred, underscoring the need for a framework to ensure quality and safety. Examples of recent incidents include the following:

• A patient with diabetes experienced severe hypoglycemia and died, in part because multiple orders for insulin had been entered into separate prescribing systems used at the hospital.
• A pharmacy technician typed incorrect information into a computer, resulting in the death of a premature baby boy who was injected with excessive amounts of sodium chloride.
• When converting to electronic records, a physician’s office omitted a patient’s aneurysm history from the active problem list. During a medical procedure several years later, the aneurysm burst and the patient died. The specialist had been unaware of the patient’s risk.

Scope

The FDASIA Health IT Report outlines three broad categories of HIT: 1) administrative functions, 2) health management functions, and 3) medical device functions. The report notes that administrative HIT applications (e.g., billing and claims processing, practice and inventory management, scheduling) present little or no patient safety risk (see note). Medical device software (category 3 above) is, of course, already under FDA oversight. Categories 1 and 3, therefore, are outside the scope of the current paper.

NOTE—This breakdown may not consider all risks; the interface of “administrative” systems with critical functions can be a concern. Most organizations think of the EMPI (enterprise master patient index) as an “administrative system” but consider risks from incorrect ADT (admit-discharge-transfer) information and incomplete information coming across the HIE (health information exchange) because of such factors as differing ADT or MPI (master patient index) rules, or the scheduling to orders interface. Often, the ability to accurately create and process “future orders” depends on a financial/billing encounter (or financial/billing encounter creation rules). Errors may present patient safety risks with the available inventory of supplies and medications and proper staffing levels. In general, some scheduling functions and medical supply inventory management would be considered medium risk and in the Health management HIT functions.

This paper focuses on the types of software that implement health management HIT functions, such as:

• Health information and data management.
• Data capture and encounter documentation.
• Electronic access to clinical results.
• Most clinical decision support.
• Medication management (electronic medication administration records).
• Electronic communication and coordination (e.g., provider to patient, patient to provider, provider to provider).
• Provider order entry.
• Knowledge (clinical evidence) management.
• Patient identification and matching.

Audience
The content of this paper is targeted to those whose role can affect, or is affected by, the quality and safety aspects of HIT. These individuals can include:

• Those who develop HIT software.
• Those responsible for evaluating and purchasing HIT software.
• Those who configure HIT software.
• Those who install, operate, and maintain HIT software.
• The body tasked with overseeing HIT software adoption to meet meaningful use criteria.
• The team(s) responsible for quality of HIT software.

If all of these stakeholders recognize the considerations being proposed, the overall safety and quality of HIT can be improved substantially. Buy-in from all interested parties will be needed to create and demand this level of quality, as well as to ensure that the efforts are realized.

Flexible approach
The focus of this paper is on “quality considerations,” which can contribute to increasing the overall quality and safety of HIT systems in the healthcare delivery environment. After the appropriate quality considerations are identified, a quality management system can be built around these concepts.

The list of considerations discussed here is not all-inclusive but is intended to stimulate the critical thinking process necessary to ensuring quality and safety of any HIT system.

II. Quality Considerations
The following subsections describe considerations that should be included in a chosen quality system, standard, or process:

1. An HIT product needs certain properties (i.e., usefulness, data protection, user-friendliness, interoperability)
2. Design of an HIT system must focus on quality and safety
3. Implementation and deployment are as important as design
4. Understand the anatomy of your HIT system
5. Every HIT system needs maintenance
6. System obsolescence/retirement presents unique challenges

An HIT Product Needs Certain Properties
To fulfill its promises, such as improved efficiency and coordinated care, HIT products need to possess specific properties. Several of the more important properties are described below.

Usefulness. The software must meet user needs, provide required features, and perform consistently without reduced performance. Instances in which this level of quality was lacking include the following:

• A drug therapy was ordered, but the respiratory therapy unit (that was to administer the therapy) was not automatically notified.
• A pharmacist ordered the correct start time and date for a drug therapy, but the interface between the pharmacy system and administration system caused the order to default to the next day start time.

Data protection. The HIT software must preserve the integrity, privacy, confidentiality, and availability of patient data. Consider the privacy aspect alone: A recent data breach at a health insurance provider allowed hackers to access the medical information and Social Security numbers of millions of insured individuals.

Usability. The HIT software must be clear to the user and fit with his/her workflow. Numerous examples of data entry error could stem from a lack of clarity in the user interface. A report from the Pennsylvania Patient Safety Authority described issues such as:
• Transposition or transcription errors in entering orders or administration information.
• Entry of incorrect patient parameters, such as weight or blood glucose, triggering calculations of incorrect therapy.
• Entering the wrong physician name, resulting in reports being sent to the wrong recipient.
• Units errors—typically, mistakes in patient weight units (lb versus kg) or incorrect medication dosing units (weight-based dosing [e.g., mg/kg/h] versus non–weight-based dosing [e.g., mg/h]).
• Incorrect input—wrong fields, generally because the user was unfamiliar with the configuration or function of a facility’s electronic health record (EHR) system.

In addition, a user-friendly HIT system must operate in its customers’ normal environment and must be able to adapt to anticipated disruptions of that environment. HIT systems must be adaptable to loss of power, loss of communications, loss of cooling, equipment relocation, as well as software compatibility.

Interoperability. HIT users often note that their applications and the data they process are not “interoperable.” Healthcare providers have expressed a desire that all data for a patient be accessible in his/her EHR, whether generated in the clinical laboratory, measured at bedside, monitored in specific therapy units, or created at another institution. The ONC has published an advisory to promote interoperability standards. However, barriers to interoperability remain.

Design of an HIT System Must Focus on Quality and Safety

Several considerations are fundamental during the design and development process and should always be applied to ensure the quality of the HIT product.

User-centered design is essential: A confusing or cumbersome interface in a healthcare environment, or poor fit with the clinical workflow, can lead to errors and patient harm. Compared with other product design philosophies, user-centered design strives to optimize the product around user needs, understanding, and environment, rather than forcing users to change their behavior to accommodate the way in which a product was engineered. Typical characteristics of products created through user-centered design include the following:

• Workflow is clear and unambiguous, and fits with how the users operate.
• The human-computer interface is configured for optimal usability for different users and environments.
• Context-sensitive assistance is available to provide information about the current task on any screen.
• Error messages convey useful information about what occurred.
• Abnormal or out-of-range results are automatically flagged or distinguished in some way.
• The system assists the caregiver in protection of privacy of data.

Requirements should be clearly written and mutually understood by both software developers and healthcare providers. They must serve as the basis for development and testing. These requirements need to be captured so that they can be reviewed and verified.

Configuration and change management during development should be carefully managed. Changes to software or systems can create ripples that affect other software or systems if not managed. For HIT applications, numerous components need to interact (e.g., pharmacy systems, patient-connected devices, laboratory information systems, patient records); changing a function in one of these, if not managed, could have serious impact on its ability to interact with others.

Risk management considerations, for both patient safety (i.e., potential of direct harm to a patient, through delayed or incorrect therapy) and cybersecurity (i.e., theft/alteration of patient data or breaches that affect performance), are of critical importance for HIT and must be included in design. Neither patient safety nor cybersecurity can be addressed as an afterthought or “bolt-on.” Both considerations are discussed in further detail below.

Validation, by representative users in simulated or real use environments, is the only way a developer can know whether clinical needs and usability goals have been met. (This discussion assumes that the software designers will have conducted the necessary and appropriate verification testing prior to validation in the real use environment.)

Implementation and Deployment Are as Important as Design

HIT products are distinct from, for example, medical devices in that they are not usable “out of the box.” In many cases, considerable effort must go into implementation and deployment in the environment where they will be used. Although the HIT software producer is responsible for the design and development of the application software, the implementation phase becomes a shared responsibility of the software vendor and the purchaser.

For the HIT product to function effectively and safely in its intended environment, consider the following key steps and concerns in successful implementation:
The selection of a software application and vendor is crucial to success. Application selection must be based on a thorough understanding of the clinical workflow and processes that will rely on the application. The workflow and the architectural integration of the application should be the basis for the technical terms of the purchase agreement and set the foundation for implementation planning and management.

Establish key objectives and goals for the new system to define “success.”

The purchaser also should ensure that the vendor has applied clinical safety risk management and security risk management to the development of the application, including the implementation phase.

The purchaser should verify that a well-structured project management methodology is in place for installation, implementation, and deployment of the application. An example of phased project management methodology is described in Figure 1.

![Figure 1. Planning an HIT Implementation](image)

- The quality, safety, and security requirements of the system can be managed within this project management framework, along with all other business requirements. This should include testing of any safety or security risk controls identified in the assessment process.
- A project management plan should be created at the outset to clarify the shared responsibility between vendor and purchaser. This includes detailed roles and responsibilities, communication methods, common terminology, methodology, tools, key deliverables, and accountability for management review and approval.
- Each implementation must account for integrating the application into the purchaser’s HIT. This typically requires specific software configuration or coding to meet the unique requirements of the purchaser. In many ways, the design and development principles in the previous section would apply to these “new” requirements.
- User-centered design (described above) also should be applied to implementation. Ideally, key process owners and workflow users should be integrated throughout the implementation project phases: from planning, to defining requirements, to test planning and execution.
- The vendor should consider initial application training at the outset of the project for key IT and clinical personnel, to ensure that the core project team has a solid baseline understanding of the functionality and configurability of the application. A comprehensive training plan for the various types of users should be included. The safety and security risk management controls should be directly linked to the training plan and content, to ensure that staff are aware of the risks and are given instructions to manage them.
- Finally, the purchaser should clearly define all deliverables and evidence required for approval of application deployment:
  - All documentation and tools needed for system maintenance and upgrade are available.
  - Maintenance agreements with the vendor and key internal support organizations are in place.
  - Appropriate documents and tools are available for future upgrades or if expansion of use to broader areas of the organization is planned.
  - Proper change management processes are in place, to account for future IT and workflow changes that may affect the application system.
  - Support processes are in place and understood by end users, ensuring escalation of any potential patient safety issues caused by the system.
Understand the Anatomy of Your HIT System

HIT Centers manage a collective set of health information systems that are used in a clinical environment to manage patient information. HIT Centers should have a detailed and complete roadmap of all data used, including information on where the data originates, how it changes through use, and which application(s) and users are consumers of the data. Over time, this would help drive standardization, as HIT Centers require developers to meet requirements for the software and hardware that are part of the HIT system. It is important that health service provider organizations (HSPOs) see HIT systems as cohesive and coordinated.

HIT Centers may include many of the software components shown in Figure 2 and will include networks, databases, medical devices, and other hardware or software that are used to enter, store, transmit, or manage patient data.

![Figure 2. Components of an HIT Center](image)

A lack of documentation can result in data incompatibilities, unauthorized changes to data, loss of traceability, and incomplete or incorrect data. These conditions can result in adverse events that elude root cause analysis. Data from a survey of more than 500 nurses revealed that:

- 50% of nurses said they had witnessed an error because of a lack of device coordination.
- 25% surveyed estimated that 25% of medical errors and adverse events might be prevented if devices could share information seamlessly.

Methods for documenting data include data flow diagrams, data structure charts, control flow diagram, business process mapping, and device-to-HIT software interface specifications.

HIT Centers should be the gate keepers of the data they manage by:

- Monitoring and managing data formats.
- Defining where and how the data are used.
- Identifying and documenting the consumers of the data.
- Documenting who is changing the data, as well as the changes that are made.
- Defining valid ranges for the data.
- Working with vendors to adapt to the data formats of the HIT Center.
The data stored in an HIT Center are the lifeblood of the center’s HIT system, regardless of where they reside (e.g., hospital, clinic, pharmacy). HIT Centers should document where data originate, how data change as they move from application to application, and which applications and users are consumers of data (Figure 3). It is important that HSPOs see HIT systems as cohesive and coordinated.

Every HIT System Needs Maintenance

Maintaining (i.e., “care and feeding”) an HIT system is an ongoing process and should address a series of key considerations. Postinstallation behavior of any system, especially one handling health information, is not static; rather, it changes in response to changes in its components. These would include:

- Accumulation of new and different data.
- Monitoring of performance and root cause analysis of errors.
- Upgrades.
- Additions and replacements of the software, underlying hardware, and network.
- Frequency and types of user interaction with the system.

These changes occur throughout the maintenance phase of the HIT product life cycle. They require careful attention by the HSPO to ensure that the system continues to function safely and effectively.

The HSPO should consider the following key factors of a successful maintenance process. Many of these activities are managed by the owner of the HIT Center.

- The owner of the HIT Center should have a process to evaluate and test all planned changes to the system. This includes changes to the computing and network infrastructure, software updates from vendors, and any new capabilities or functional changes as the role of the HIT expands. The evaluation should consider the information flows affected by the change and should apply risk management practices as described below.
- The HSPO needs to monitor the system for unexpected changes. The HIT Center owner should establish a monitoring system during the implementation phase and continue to monitor through the lifetime of the HIT Center. The monitoring system should be able to identify hardware or network failures, data corruption, security breaches, operation outside of the tested bounds of the system, and unanticipated changes in clinical workflow or standard of care.
- The HIT Center owner should have visibility and approval rights to the contracts being signed for products to be added to or modified within the HSPO’s system. It is the responsibility of the vendor to ensure that those contracts, as well as the accompanying instructions and installation guidelines, set clear expectations and requirements for the HIT product.
• The HIT Center owner should establish a **communication channel with the system users**. The HSPO needs a way to notify users of changes to the system and to provide user training when those changes affect their work. Users need a way to report system failures, unexpected or confusing behavior, and use errors so that the HSPO can investigate.

• The HSPO should have a **communication channel with each HIT vendor**. The vendors use that channel to communicate any changes or updates to the product in advance so that the HIT Center owner can be effectively prepared to monitor and test the system, if necessary, to ensure that no unexpected anomalies with other products in the system are created by these changes.

• The HSPO should conduct **periodic reviews**. The reviews examine the evaluation and testing of planned changes to provide smooth system upgrades, the effectiveness of system monitoring to identify unexpected changes, and the quality of the communication with users and vendors to identify issues and prepare for changes.

• When a system failure occurs, the HSPO should perform a **root cause analysis**. That information should be used to correct the source of the failure and to identify and implement preventive actions so that the failure does not recur. If the failure is traced back to the HIT product, the HSPO should have a process for communicating this back to the producer.

**System Obsolescence/Retirement Presents Unique Challenges**

All HIT products accumulate considerable clinical and patient data over time. When a system is retired or converted, as eventually happens with nearly every computerized system, care should be taken to preserve needed data so that they will continue to be available.

When retirement time approaches, the HSPO (or HIT Center owner) needs to consider:

• How data will be moved to a new system (and converted, if necessary).
• The range of data to be moved.
• Legal and risk implications of the historical data.
• How existing data will be preserved.

The owner of the HIT Center needs to ensure that any other systems that depend on the one being retired are appropriately reconfigured. A contingency plan must be put in place in case any step of the retirement goes awry. Often, retiring a sufficiently large HIT product is a project all its own, requiring planning, notification, and scheduling to ensure success.

**III. Risk Management**

Those who design and develop an HIT product, as well as those who purchase and implement the HIT product in its use environment, must consider multiple dimensions of risks, including patient safety, data and system security, and privacy/confidentiality.

**Minimize Safety Risk During Design**

Software often is an integral part of HIT. Establishing the safety and effectiveness for HIT requires knowledge of what the software is intended to do and demonstration that the implementation of the software fulfills those intentions without creating any unacceptable risks.

A risk-based, safety-focused approach is necessary to understand the hazards and harm associated with HIT, in order to ensure that proper levels of safety are established. ONC regulation §170.314(g) requires a safety-enhanced design but does not specify what that means or how exactly it will be achieved. At the same time, the Institute of Medicine states, “The current state of safety and health IT is not acceptable.”

**Build in Cybersecurity**

In the era of digital health, users are demanding access to health and medical data in multiple user environments (e.g., hospital, lab, home, mobile). As a result, medical systems (encompassing medical devices, administrative health products, and health management solutions) are increasingly being connected in networks.

Although this enhances productivity and allows patients to take charge of their information, network availability also makes these systems vulnerable to cybersecurity threats. HIT Centers contain prescriptions, treatment plans, and EHRs and are connected to networks, accessed from various protocols, and stored on clouds and medical devices. This provides a multitude of possible security-related attack scenarios.
As part of product development, cyberthreats must be identified (as early as defining the users/user environment), mitigated (as part of design), detected (as part of verification testing), acted upon (once testing reveals that a vulnerability exists [implement fixes and retest]), and finally, through the design of the HIT product, provide mechanisms for recovery and testing of these recovered systems before final system deployment in the field. After an HIT product is deployed (postmarket release), data on cyberattacks—successful and unsuccessful—should be collected and analyzed (as part of risk assessment) in order to identify compromised data or functionality and implement continued improvements.

Privacy/Confidentiality, Financial Risk, and Other Areas

Even without cyberattacks, risks to patient-related data can exist. Wherever multiple systems share data, controlling the content to be shared is necessary in order to avoid inappropriately divulging protected health information. Where procedure and test information are transmitted to billing systems, errors in the data can result in confusion and financial risk. Continuity of operations can be ensured if appropriate plans are in place. What happens when the power fails? What is the fallback if the computer system goes down? How will operations continue in the event of fire or flood?

IV. Quality Standards for HIT

The consensus today is that appropriate quality management and risk management need to be applied to HIT. However, at the present time, no standard specifically focuses on managing quality and risk for HIT.

Why Not Use Existing Standards?

Applying many existing standards to HIT is considered difficult. Common difficulties include the following:

- Many current standards are device manufacturer centric and do not fit into the HIT Center environment. While the quality system for the medical device manufacturer is focused on how well the device is manufactured and performs its intended use, the HIT Center needs to focus on the device from delivery through use in the HIT Center environment. Like throwing a rock into a pond, the impact of the device has far-ranging ripples to the HIT Center environment and its users—the current standards do not address these considerations.
- Existing quality and risk standards are written in the language of the quality manager. They could be more effective if they were written in the language of the developer, installer, and user. Writing the standard from the implementer’s perspective rather than the management controller’s perspective could be more effective.
- Existing quality and risk standards were created when product quality was “manufacturing” centric in lieu of “design” centric. In many cases, the design portions were added on to existing good manufacturing practices. For HIT, design drives quality while manufacturing plays a much smaller role in the whole quality spectrum for HIT.
- Existing quality and risk standards are written based on the interface and interaction between humans and the manufacturing machine; they would be much more effective if they were written based on interactions among the developer, user, and actual HIT product.

Compare: Medical Device Standards

For medical devices, multiple existing standards address quality management, application of quality principles, design and development control, and risk management:

- ANSI/AAMI/ISO 13485 outlines a quality system framework for medical devices.
- ANSI/AAMI/ISO 14971 maps the steps expected in a medical device risk management process.
- AAMI/IEC 62304 sets out processes and deliverables for medical device software, scaled by risk.
- ANSI/AAMI/IEC 80001-1 describes the application of risk management for IT networks incorporating medical devices.

Quality Efforts for HIT Software Have Begun

Various efforts, with varying primary concerns, are aimed at introducing a quality/safety framework to the HIT software realm.

- ISO/TC 215, Health informatics, and IEC/SC 62A, Common aspects of electrical equipment used in medical practice, have prepared a framework for developing standards for HIT to address safety, efficacy, and security for health software and HIT systems. The development of the envisioned body of international standards is expected to begin in late 2015.
- AAMI has established a new standards committee, the AAMI Health IT Committee, which was initially tasked with developing two new standards: AAMI HIT1000, Risk Management Practices for Health IT, and AAMI HIT2000, Quality System Principles for Health IT. Completion of these standards is targeted for late 2016.
addressing the specific needs and conditions of HIT in the United States, the intent is that these standards also inform the development of corollary internationally standards.


V. Summary

Many current standards are device manufacturer centric and do not fit into the HIT Center environment. While the quality system for the medical device manufacturer is focused on how well the device is manufactured and performs its intended use, the HIT Center needs to focus on the device from delivery through use in the HIT Center environment. The impact of the device or software has far-ranging effects on the HIT Center environment and its users—effects that are not addressed by the current device manufacturer–centric standards.

Rather than providing definitive solutions, the intent of this paper was to provide a starting point for discussion on the quality issues currently being encountered by HIT Centers. Establishing a common set of expectations for ensuring the overall quality of the HIT Center environment is critical and should be a major focus going forward.
Resources for Understanding HIT Safety Issues

- In December 2008\textsuperscript{10} and in March 2015,\textsuperscript{11} The Joint Commission (www.jointcommission.org) published Sentinel Event alerts expressing concern over safe implementation and use of health information technologies. From the 2015 alert: “An analysis of sentinel event reports received by The Joint Commission between January 1, 2010 and June 30, 2013 identified 120 sentinel events that were health IT-related.”

- In December 2012, the Pennsylvania Patient Safety Advisory published an analysis of 8,003 reports between June 2004 and May 2012. An EHR was involved in 3,099 of the reports. Although not all of the incidents involved harm to the patient, a number of issues that could impact patient safety were identified.

- A literature review from 2013 examined the impact of unintended consequences on quality of care resulting from EHR system use.\textsuperscript{12}

- In the ECRI Institute’s (www.ecri.org) top 10 health technology hazards for 2015, “data integrity: incorrect or missing data in EHRs and other health IT systems” appeared as the second greatest hazard.\textsuperscript{13}

- In 2011, the Pharmacy e-Health Information Technology Collaborative published its Roadmap for Pharmacy Health Information Technology Integration in U.S. Health Care, and later updated this roadmap in 2015.\textsuperscript{14}

- In February 2013, the Bipartisan Policy Center published An Oversight Framework for Assuring Patient Safety in Health Information Technology.\textsuperscript{15}

- In 2013, the ONC published Health Information Technology Patient Safety Action & Surveillance Plan.

- The April 2014 ONC report, FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework, followed up on proposals made in the earlier documents.\textsuperscript{2}


- HealthIT.gov provides the SAFER guides (www.healthit.gov/safer/safer-guides), which enable healthcare organizations to address EHR safety in areas such as organizational responsibilities, contingency planning, system configuration, system interfaces, patient identification, computerized provider order entry, test results reporting/follow-up, and clinician communication.
References


5. HIMSS. What is interoperability? Available at: www.himss.org/library/interoperability-standards/what-is-interoperability.


