Journal of Health Science 4 (2016) 277-282
doi: 10.17265/2328-7136/2016.05.007

EHR Technology: Improvement Review of a Small Rural Hospital

Nancy Norman-Marzella, RN, MSN, NP, CNE
Department of Nursing, Lincoln University, 1570 Baltimore Pike Lincoln Univeristy, PA 19352, USA

Abstract: The focus of this study was to examine the technology improvements in a small rural hospital preparing to implement the first two stages of Health Information Technology for Economic and Clinical Health (HITECH) [1] in their organization. The existing hospital organization's health information technology (HIT) is on a continuum between a traditional system and one that can support evidence-based clinical decisions. A methodology based on hierarchy and experience, is routine and relies upon trial, and error is a traditional approach [2]. Prior experience with Electronic Health Records/Health Information Management Systems (EHR/HIMS) improvements in this hospital lacked a systematic evidence-based approach leading to inoperability and security concerns. Future improvements include adoption of nationally recognized standards for HIT protocols and planning incorporates a process to test improvements and upgrades with feedback from end-users prior to initiating full scale operations.

Key words: Technology, HITECH, Electronic Health Record (EHR), technology improvement.

1. Introduction

The focus of this study was to examine the technology improvements in a small rural hospital preparing to implement the first two stages of Health Information Technology for Economic and Clinical Health [1] in their organization. The existing hospital organization's health information technology (HIT) is on a continuum between a traditional system and one that can support evidence-based clinical decisions. A methodology based on hierarchy and experience, is routine and relies upon trial, and error is a traditional approach [2]. The Organization for Economic Co-Operation and Development (OECD) states "health data constitutes a significant resource to improve population health, and to improve the effectiveness, safety and patient-centeredness of health care systems" (p. 13) [3]. The hospital's strategic plan mandates that the use of health data is consistent with this OECD statement and the Institute of Medicine [4]. Therefore, the hospital will upgrade their information technology across all departments. There are three primary clinical informatics systems including 1) an HIMS hybrid-type general medical-surgical system; 2) emergency area, and 3) Centricity Perinatal® GE for obstetrics and perinatal care. The PACU, OR, ICU are part of the hybrid-type system. Health care workers can use the informatics systems within their respective areas. Each system works well within the individual units. Other hospital programs include: CLINVIEW, CLINDOCS, CREDIT NOTES, ORDER ENTRY, EMAR, MEDHOST (GREENSCREEN), MEDHOST (EDIS), MEDHOST (PHARMACY), MEDHOST (QUICK ADMIT), EMAIL (OUTLOOK), PACS (DOC/TECH/ADMIN), and SINGLE SIGN ON (VERGENCE). However, the systems currently do not interface with each other and data in each system is sporadic.

Two key reasons the hospital has undertaken the process of upgrading and centralizing the Health Information Management System-Health Information Technology (HIMS-HIT) include the mandate by the hospital's strategic plan for health data collection, and to comply with the 2009 Health and Human Services American Recovery Act, specifically, the Health

Corresponding author: Nancy Norman-Marzella, RN, MSN, NP, CNE, associate professor of nursing, research fields: nursing education, technology, genetics/genomics, leadership ethics, and women/children's population health.

Information Technology for Economic and Clinical Health (HITECH) [1].

The goal is to complete implementation of the first two stages of HITECH by spring of 2016. Also, the hospital has hired an informatics nurse who will work from within the Information Systems department and directly with IT to assist the hospital in implementing the objectives for stages one and two of HITECH. The director of Information Technology manages the hospital's system under the leadership of the Administrator for Informational Services. Figure 1 depicts the hospital's current traditional hierarchical model.

2. Design

The stages of development in the life cycle of a clinical information system include: "system conception and planning, identification and analysis of requirements, system design, implementation, and, finally, use and maintenance" (p. 7) [5]. To upgrade, interface, and

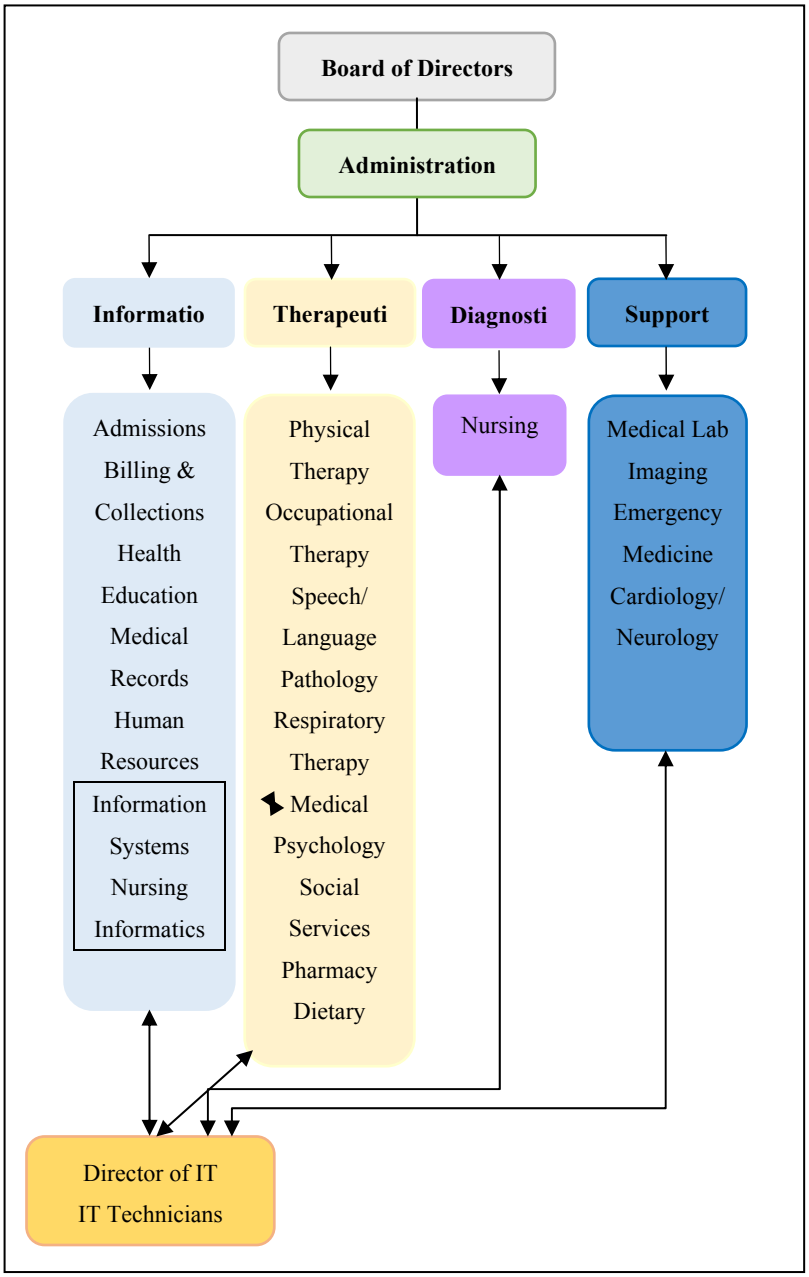

Fig. 1 Hospital's traditional hierarchical organizational chart.

achieve interoperability of the HIMS-HIT, stakeholders from each level of the hospital's hierarchy participated on the HIMS-HIT Taskforce. From the beginning, end users in each department have been involved in planning. The end-users, an ad-hoc group, will take part in test trials throughout the installation and before implementation of the new HIMS-HIT.

Initial funding for the HIMS-HIT HITECH project came from the hospital's capital equipment and administrative project funds specifically designated for HITECH. Budget items include capital equipment, renovations where indicated, full-time employees (FTEs), and training. The Administrator of Informational Systems (comparable to a Chief Information Officer), manages the budget and reports directly to the Chief Financial Officer (CFO). To date, funding has been uninterrupted, and the hospital continues to recruit and hire certified employees in the field of health informatics. Research when comparing capital expenses of HITECH with other interfacing services such as Radiology has shown an improvement in diagnostic accuracy which improved quality care for patients [6].

There is a strong commitment from the entire administrative team, and Board of Directors to the successful implementation of HITECH. Educational funding for employee certification is part of the overall HITECH budget so that current employees with an interest and some experience with health care technology can work in this area. The newly hired Nurse Informaticist is a current employee of the hospital from Critical Care and has recently received an advanced degree and certification in nursing informatics. This position, initially funded as one FTE, will work with the Director of Information Technology. Plans include development of a nursing and medical informatics department with a total of 6 FTEs (3 from nursing and three from medical).

3. Information System Application Implementation

The hospital is in the process of exploring ways to assure the HIT system is legally sound concerning patient health data. The following policies and procedures are currently in place: All new employees submit to drug testing, federal and state security background clearances including verification of licenses and certifications through the respective bureaus. New hires participate in IT training through the Informational Services department. The hospital provides an initial limited access level clearance based on the job description. The access level corresponds to a security data breach code. Training time varies depending upon the job description and level of designated access. In general, training can last from 1-4 weeks in duration. Program specific training takes place in each unit with a department mentor. Department specific training ordinarily consists of an additional 1-4 weeks. Both training events include educational modules with practical application testing. Employees receive their system permanent access code upon completion of both general IT and unit specific training.

Training hours are part of each employee's personnel record along with documentation of additional training for more secure access. Each level of clearance corresponds to a possible security data breach code. The hospital carries cyber/privacy liability insurance to protect patients by the federal health records protection law, Health Insurance Portability and Accountability Act (HIPPA). Also, the organization has an ongoing relationship with Mandiant®, a cyber security agency to monitor threats to its network and system. The system is a virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber-attacks [7].

The Informational Services department plans and trains for contingency operation that can occur for scheduled routine backups and system maintenance or unanticipated events. There are policies and procedures in place to minimize the effect of downtime. Algorithms align with critical system outages or a malfunction. For

example, clinicians and end-users can assign a temporary patient ID number when the system is down that can be easily recognized and reconciled by the system when it is back online. The IT department routinely practices both announced and random downtime drills that include a debriefing to review related policies and procedures, and any problems that occurred. In the event the system is down, clinicians and end-users have copies of policies and procedures at each workstation to continue workflow in a safe and accurate manner. Daily rounds include an update from IT and Informational Systems. During this time, IT briefs department heads on any upcoming IT challenges or changes in the protocol of the department.

Risk management has played a vital role in assuring network security and addressed potential patient confidentiality and ethical concerns by adopting the following HIMS principles to avoid a breach of security in the system. Stated goals include creating a strong security foundation; establishing a security infrastructure to conduct ongoing risk assessments; maintaining vigilance among personnel; and, developing inclusive, comprehensive policies and procedure for network security including sanctions [8]. The security process includes submission of a security form by all personnel requesting computer access (Fig. 2).

Name of Hospital
Information Security Request Form—2015

Accessing information in the hospital requires the use of a login and password. Please fill in the form below with the appropriate information and access request. DO NOT give your password to someone else to use. *Passwords must be kept Private.* (Review the XXXX Password Policy for rules governing passwords and computer access).

This form must be filled out completely (with additional forms if needed). Return this form to the IT Department marked ATTN: Help Desk, Suite XXX, and Address. If the form is not completely filled out, it will be returned delaying account creation/access to systems.

Last Name: _____
Department Name: _____
First Name: _____
Department No: _____
Middle Name: _____
Date of Birth: _____
Job Title/Description: _____
Employee No: _____

Employment Status:
□ Staff
□ Contractor
Union Affiliation:
□ Yes
□ No Contractor Start Date: End Date:

Hospital Access:
□ CLINVIEW □ MEDHOST (GREENSCREEN)
□ CLINDOCS □ MEDHOST (EDIS)
□ CREDIT NOTES □ MEDHOST (PHARMACY)
□ ORDER ENTRY □ MEDHOST (QUICK ADMIT)
□ EMAR □ EMAIL (OUTLOOK)
□ PACS (DOC/TECH/ADMIN)
□ SINGLE SIGN ON (VERGENCE)
□ _____

Form also includes VPN Access: if system needs to be accessed from home. Security Code & Internet Usage Policy Signature and date:_____

Fig. 2 Current security request form for computer access.

4. Conclusions and Recommendations

Although the hospital is small in size (less than 70 beds), the planned technology improvement has momentum and financial support. As a small rural hospital, confidentiality is a high concern. A security upgrade is in progress. However, the current security form does not include all of the electronic health record (EHR) networks and programs in use, for example, Centricity Perinatal GE®. The hospital staff has been writing in additional programs, but this will not be sufficient for planned future HIT initiatives. Designating the hospital HELP desk (staffed with volunteers) to perform this function is inadequate and does not assure official security approval. Unreconciled information with Human Resources and IT will lead to improper employee access.

The organization has several policies and procedures in place to address safety and cyber security, however, missing is a systematic approach to assure electronic health records remain secure. The recommendations by Hardeep, Ash & Sittig [9] explicitly address electronic health record (EHR) safety factors with recommendations according to priority level (Table 1).

Strategies for the Informational Services department/IT include training with the *Final Federal Health IT Strategic Plan Released 2015-2020* [11].

Table 1 Overview of the organization and content of the Safety Assurance Factors for EHR Resilience (SAFER) guides.

Foundational Guides	
High Priority Practices—Recommendations determined to be "high risk" and "high priority". This guide can be used by organizations to help them assess where they should concentrate their EHR safety improvement efforts.	
Organizational Responsibilities—Recommendations related to activities, processes, and tasks that people must carry out to ensure safe and effective EHR implementation and use.	
Infrastructure Guides	Clinical Process Guides
Contingency Planning—Recommendations for preparations that should be completed before the EHR experiences a hardware, software, or power failure.	Patient Identification—Recommendations for creating new patient records in the EHR and patient registration and retrieval of information on existing patients.
System Configuration—Recommendations related to the physical environment in which the EHR will operate, as well as the infrastructure required to run the EHR.	Computerized Provider Order Entry with Decision Support—Recommendations for electronic ordering of medications and diagnostic tests and point-of-care clinical decision support.
System Interfaces—Recommendations for processes that enable the physical and logical connection of different hardware devices and software so they can share information.	Test Results Reporting and Follow-up—Recommendations regarding delivery of test results to the appropriate providers.
	Clinician Communication—Recommendations regarding consultations or referrals, discharge-related communications, and patient-related messaging between clinicians.

Adapted from: Sittig, D. F., Ash, J. S., and Singh, H. 2014. ONC Issues Guides for SAFER EHRs, *Journal of AHIMA* 85 (4): 51 [10].

The Nursing Informaticist working within the Department of Information Technology will need to have a clearly defined role that improves the quality of health care to consumers. The Nurse Informaticist will provide clinical and non-clinical support to nurses and other health care providers [12]. Potential challenges influencing the new Nurse Informaticist role include the need to educate staff during the transition to an institution-wide informatics team of specialists, and compliance with new protocols. Once the new technology is in place, maintaining security, privacy, and confidentiality of data will be the next step in improving technology for the small rural hospital [12].

Acknowledgments

The author wishes to acknowledge Dean F. Sittig, Ph.D.; Joan S. Ash, Ph.D., MLS, MBA; and Hardeep Singh, M.D., MPH for their contribution in use of the (SAFER) Guides; the Hospital IT Department and Nursing Informaticist for providing material about the existing EHR/HIMS, and systematic plan for improving processes, interoperability, compliance, and security concerns.

References

[1] HITECH. (n.d.). *HITECH Answers: HITECH Act Summary.* Retrieved from website http://www.hitechanswers.net/about/about-the-hitech-act-of-2009/.

[2] Ball, M. J., Douglas, J. V., Hinton Walker, P., DuLong, D., Gugerty, B., Hannah, K. J., and Troseth, M. R. (Eds.) 2011. *Nursing Informatics: Where Technology and Caring Meet* (4th ed.). London, England: Springer-Verlag.

[3] Organization for Economic Co-Operation and Development 2013. *Strengthening Health Information and Infrastructure for Health Care Quality and Governance: Good Practices, New Opportunities, and Data Protection Privacy Challenges (Preliminary Report),* 13. Retrieved from http://www.oecd.org/els/health-systems/Strengthening-Health-Information-Infrastructure_Preliminary-version_2April2013. Pdf.

[4] Institute of Medicine 2012. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: The National Academies Press.

[5] Peleg, M. 2011. "The Role of Modeling in Clinical Information System Development Life Cycle." *Methods of Information in Medicine* 50 (1): 7-10. Retrieved from www.methods-online.com on 2012-06-25, IP: 38.102.29.165.

[6] Moodley, I., and Moodley, S. 2015. "A Comparative Cost Analysis of Picture Archiving and Communications Systems (PACS) versus Conventional Radiology in the Private sector. *South African Journal of Radiology* 19 (1): 7, Art. #634, http://dx.doi.org/10.4102/sajr.v19i1.634. http:

//www.sajr.org.za/index.php/sajr/article/view/634/html.

[7] Mandiant®. (n.d.). *One Unified Defense against Cyber-attacks*. (Website). Retrieved from https://www.fireeye.com/company.html.

[8] Healthcare Information and Management Systems 2011. *Privacy & Security Toolkit.* Retrieved from http://www.himss.org/ASP/topics_pstoolkit.asp.

[9] Hardeep, S., Ash, J., and Sittig, D. F. 2013. "Safety Assurance Factors for Electronic Health Record Resilience (SAFER): Study Protocol." *Bio. Medical Central Medical Informatics and Decision Making* 13 (1): 46.

[10] Sittig, D. F., and Singh, H. 2014. "ONC Issues Guides for SAFER EHRs." *Journal of American Health Information Management Association (AHIMA)* 85 (4): 50-2. doi: 10.1093/jamia/ocv060.

[11] U.S. Department of Health & Human Services 2015. *Federal Health IT Strategic Plan 2015-2020*. Retrieved from https://www.healthit.gov/policy-researchers-implementers/he alth-it-strategic-planning.

[12] American Nurses Association 2015. *Nursing Informatics: Scope and Standards of Practice* (2nd ed.). Silver Spring, MD: Author.