Respiratory Care in the Computer Age

Karen J Stewart MSc RRT

Computerization in health care is rapidly advancing and is improving patient safety (eg, computerized physician order entry decreases the frequency of medical errors) and practitioner effectiveness and efficiency. Computerization and other developing technologies raise concern about the privacy of health information. In 1996 Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which included privacy provisions that went into effect in April 2003. HIPAA has important impacts on health care providers. With the tremendous growth of health care information systems comes the need to standardize the storage and sharing of health information, so there is an initiative underway to develop a National Health Information Infrastructure, which will set standards for health information exchange among consumers, providers, and the public health sector, as well as consolidate the "silos" of health information that are in place today.

Key words: computers, Health Insurance Portability and Accountability Act, HIPAA, medical errors, information management. [Respir Care 2004;49(4):361–364. © 2004 Daedalus Enterprises]

Introduction

In the very near future respiratory therapists (RTs) and other health care providers may have fully integrated software and technology in health care facilities. Wireless systems will allow providers to enter data at the bedside and to monitor the patient from any location in the facility. The increased efficiency will allow providers to spend more time with patients: Leger and Roberts[1] predict that caregivers will spend 85% of their time with patients, rather than the currently estimated 35–45%, and believe that the technological advances and increased clinical attention are already improving patient outcomes.

In addition to giving providers more time at the bedside, the advance of medical information technology is anticipated to improve patient safety, especially with regard to medication errors. "Medication errors due to illegible handwritten prescriptions, overlooked allergies and drug interactions, and incorrect dosages often result in adverse drug events. Consequently, technology-based interventions have been recommended as a key mechanism for reducing the likelihood of medication errors."[2]

Computerized physician order entry is a method that promises the best results to eliminate errors in prescribing and transcription. No longer will RTs, nurses and others waste time attempting to read illegible handwriting. Although few hospitals currently have computerized physician order entry, the reduction in errors can be substantial—a 55% reduction in one report.[3] Future computerized physician order entry systems will include evidence-based decision-support algorithms to assist in decision-making while orders are being placed.

Karen J Stewart MSc RRT is affiliated with the Medicine Services Department, Charleston Area Medical Center, Charleston, West Virginia.

Karen J Stewart MSc RRT presented a version of this report at the 33rd Respiratory Care Journal Conference, Computers in Respiratory Care, held October 3–5, 2003, in Banff, Alberta, Canada.

Correspondence: Karen J Stewart MSc RRT, Medicine Services, Charleston Area Medical Center, 3200 MacCorkle Avenue SE, Charleston WV 25304. E-mail: karen.stewart@camc.org.

Health care systems are moving from paper to electronic medical records, which impacts all providers. The best technology makes information immediately available to all departments, disciplines, and settings. Most systems use point-of-care devices that substantially improve provider effectiveness and efficiency. For RTs the immediate accessibility of clinical information can enhance the use of protocols and clinical practice guidelines. Decision-support algorithms that use branching logic and rules engines will allow RTs to create and implement computerized protocols and put needed information at the bedside.

The ease of accessing electronically-stored health information has raised concerns about confidentiality and privacy. "In response, governments around the world are developing safeguards for privacy, such as the European Union's Directive on Data Protection and the United Kingdom's Data Protection Act."[4] In the United States, the Health Insurance Portability and Accountability Act (HIPAA) became law in 1996. Its original intent was to protect workers from losing their health insurance should they change jobs. A privacy rule was added to deal with the possible consequences of loss of privacy of health information, which could include "embarrassment, job discrimination, or even the loss or denial of health insurance. Such uncertainty could undermine the relationship between provider and patient, making patients less forthcoming about their health care concerns, and thereby threatening the quality of the care they receive."[5] The privacy provisions went into effect April 14, 2003.

Overview of the HIPAA Privacy Provisions

The regulations provide privacy protections for patients by limiting the way that health plans, pharmacies, hospitals, and physicians can use a patient's personal health information. All forms of medical records (paper, electronic, and verbal) are protected.

Organizations and other entities covered by HIPAA regulations are required to provide a notice (an example of which can be found at http://www.camc.org/privacy/nopp20030407.htm) to their patients regarding his or her rights and how personal health information can be used. Patients are typically asked to sign an acknowledgment that they have received the information.

Under the regulations patients have the right to see and obtain copies of their medical records, restrict who has access to their records, obtain an accounting of who accessed their records, and request that errors in the records be corrected. The covered entity that possesses the records has 30 days to provide access to the records and may charge for the cost of copying and/or mailing the records. Health care providers must understand the regulations and the restrictions on how records are handled.

Under the law, "protected health information"[6] is any information that is entered, created, or received by health care providers that relates to the past, present, or future physical or mental health of any individual or to the provision of health care to that individual and that identifies the individual. Protected health information in any form (written, spoken, e-mailed, faxed, or stored on a computer) must be protected. Protected health information can be any of:

- Name of the individual
- Name of the employer or relatives
- Address, including street, city, state, zip code, or e-mail
- Telephone or fax numbers
- Dates such as birth date, admission date, discharge date, or date of death
- Age
- Social security number
- Other personal numbers such as medical record number, health plan number, account number, driver's license number, or vehicle identification number
- Fingerprints
- Photographs
- Medical device numbers and implant numbers

All health care providers must respect the patient's right to privacy. All patient medical records are confidential and should only be accessed if the provider has a need to know the information to perform his or her job. Providers should actively protect patient information from those who do not have the right and need to know. Passwords to computer systems must not be shared under any circumstances, and most employers have discipline policies to deal with those who inappropriately share passwords.

Covered entities must create audit trails to track those who access protected health information, and they will perform random audits. If necessary, most covered entities will provide information pursuant to government subpoenas to aid in investigations and prosecutions.

There are both criminal and civil penalties for disclosing protected health information. Criminal penalties imposed by the Department of Justice are:

- Knowingly obtaining or disclosing protected health information results in up to a $50,000 fine and 1 year of imprisonment.
- Obtaining protected health information under a false pretense results in up to a $100,000 fine and 5 years of imprisonment.
- Obtaining protected health information with the intent to sell or transfer for commercial gain, personal gain,

or malicious harm results in a fine of up to $250,000 and 10 years of imprisonment.

In addition to the criminal penalties, civil penalties can be imposed by the Health and Human Services Office for Civil Rights. Fines are up to $100 per violation, with a maximum fine of $25,000 per year per specific violation.

National Health Information Infrastructure

Although there has been tremendous growth in health care information systems, there is not yet an agreed system that would allow all the health information systems to work together. Secretary of Health and Human Services Tommy G Thompson said at the National Health Information Infrastructure meeting in July 2003:

> Although there is tremendous growth in health care information systems, there remains a need to create a foundation so all systems can work together. We must improve the systems in which our hard working, dedicated health care professionals provide care and services. To do so we should focus on increasing the use of informatics and other tools, enhancing communication between frontline caregivers and all members of the health care team, and using evidence-based interventions in medical care and health promotion. One of the keys to changing the health system—and improving care, reducing errors and, over the long-term, saving money—is to incorporate information technology fully into the health care delivery system.[7]

The initiative to develop a National Health Information Infrastructure is, according to the United States Department of Health and Human Services, a national effort to build "a comprehensive, knowledge-based system capable of providing information to all who need it to make sound decisions about health. Such a system can help realize the public interest related to disease prevention, health promotion, and population health."[8] It will improve the overall quality of health care by creating a network of systems that address, "clinical, public health, and patient health care information."[9] A system that encompasses comprehensive health information will improve decision-making by providing fast easy access for those who need the information.

The initiative is developing standards that can be followed by all health care sectors and providers. The initiative is not intended to be a form of government regulation nor a centralized repository of medical records. Participation in the initiative is voluntary. The objectives are to:

- Improve patient safety
- Improve health care quality
- Create the ability to detect patterns that could be related to bioterrorism
- Provide better information to health care consumers, empowering them to make better personal health decisions

The National Health Information Infrastructure addresses 3 types of information: personal health, health care delivery, and public health (Fig. 1). "The functions of the National Health Information Infrastructure can be illustrated by exploring 3 interactive and interdependent dimensions that are defined by what they encompass, whom they serve, how they are used, and who has the primary responsibility for content and control."[8] Three primary groups of end users are identified: consumers (patients), providers (clinicians), and public health organizations.

For the health care consumer dimension one of the objectives is to enable the individual health care consumer to manage his or her own wellness by providing the information needed to make personal health decisions. The individual health care consumer will have access to his or her personal health records and will have the ability to maintain and control those records, track his or her self-care, and obtain information such as directories regarding health care and access to public health care providers.

For the health care provider dimension the National Health Information Infrastructure initiative is intended to improve patient safety by providing more access to health information. Providing access to medical data at all times (24 hours per day, 7 days per week) will enable the health care provider to make better, faster patient-care decisions. Information contained in the health care provider dimension includes, but is not limited to, clinical orders, progress and provider notes, decision-support systems, and clinical practice guidelines.

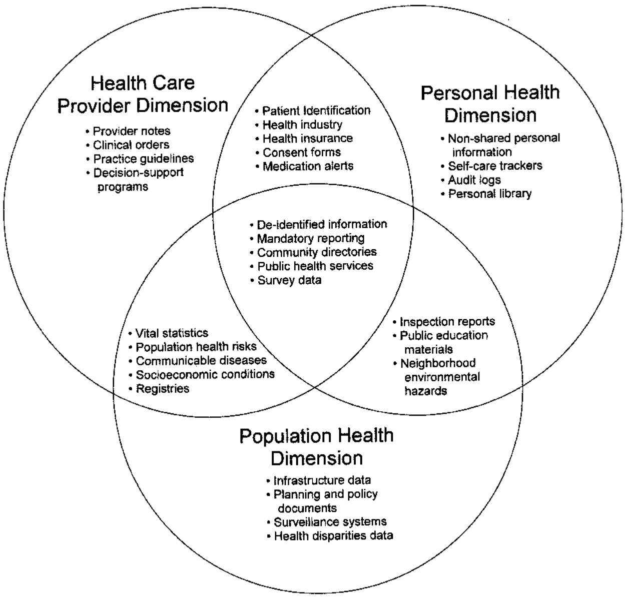

Fig. 1. The National Health Information Infrastructure's dimensions and information types (From Reference 8).

The objective for the population health dimension is to improve information sharing and thus improve the management of disease populations. The data will include vital statistics, population health risks, and disease registries. "The population health dimension makes it possible for public health and other data users at local, state, and national levels to identify and track health threats, assess population health, and create and monitor programs and services, including health education campaigns and conduct research."[10]

"The idea behind the National Health Information Infrastructure is to push information and knowledge to the point where all health decisions are made so the right decisions can be made at the right time."[8] But how do we get to the end result? Increasing the use of information technology and adopting standards are two of the first steps. We need to increase collaboration between all of the dimensions in health care. Leadership and funding from the federal government is needed to guide the development of standards and to encourage capital investment in creating technological solutions. To complete the National Health Information Infrastructure initiative we will need research on the effectiveness and efficiency of technology and the improvement of patient safety, cost reductions, and improvements in the quality of and access to health care.

Summary

Computers and new technologies are creating an environment that will give RTs and other providers tools they need at the bedside. There will be improved efficiency, effectiveness, productivity, and patient safety. Most concerns about health-information privacy have been addressed by the HIPAA's privacy and information-security rules.

Over the next 10 years the National Heath Information infrastructure will create an information system that no longer resides in silos of information. The new paradigm will be a format of integrated information that meets the needs of the consumer and the provider of health care and gives public health officials needed information for protecting and improving the public health.

REFERENCES

1. Leger J, Roberts S. Looking ahead: advice on developing a technology master plan. Health Facil Manage 2003;16(5):24–26.
2. Oren E, Schaffer ER, Guglielmo BJ. Impact of emerging technologies on medication errors and adverse events. Am J Health Syst Pharm 2003;60(14):1447–1458.
3. Shane R. CPOE: the science and the art. Am J Health Syst Pharm 2003;60(12):1273–1276.
4. Protecting patient privacy: striking a balance (editorial). Lancet 2001; 358(9282):597.
5. Reed S. Keeping secrets secret: legislation to secure patient privacy and confidentially is still needed. Am J Nurs 2000;100(8):73–74.
6. United States Department of Health and Human Services. Summary of the HIPAA privacy rule. Available at: http://www.hhs.gov/ocr/hipaa. Accessed January 23, 2004.
7. United States Department of Health and Human Services. Health care information technology (remarks by Tommy G Thompson, Secretary of Health and Human Services) July 1 2003; Available at: http://aspe.hhs.gov/sp/nhii/conference03/speechtext.htm. Accessed January 23, 2004.
8. United States Department of Health and Human Service: Information for Health: A strategy for building the National Health Information Infrastructure. NHII Report 2001; Available at: http://aspe.hhs.gov/sp/nhii/documents/nhiireport2001/report3.htm. Accessed January 27, 2004.
9. United States Department of Health and Human Service: Frequently asked questions about NHII. Available at: http://aspe.hhs.gov/sp/nhii/FAQ.html. Accessed January 23, 2004.
10. United States Department of Health and Human Service: Information for Health: Executive Summary. NHII Report 2001; Available at: http://ncvhs.hhs.gov/nhiilayo.pdf. Accessed January 23,2004.

Discussion

Chatburn: Karen, I'm glad we have an administrator to pick on here today. Suppose I worked for you and I came to you as a department manager and told you I needed a stand-alone management information system and gave you the sales pitch that it's going to improve my ability to track productivity and process improvement and improve charge capture, but it's going to cost $200,000 and I'll probably need another full-time employee to manage it. How would you evaluate that kind of a proposal?

Stewart: My method of evaluating that would be to look for a system to enable you but make sure that it had the ability to communicate with other systems. If you can't share the information with other services and departments in the hospital, you will not be successful. The system *has* to be fully integrated. You *have* to have a system that allows other care providers to see the information you've collected.

Ford: Karen, in dealing with manufacturers of information systems the issue of HIPAA compliance comes up. The manufacturer may tell you they are 100% HIPAA-compliant. My assessment is that many aspects of HIPAA compliance are more related to hospital or medical institution policy. From your discussions of HIPAA compliance with information-system manufacturers, do you have any recommendations on what are the top 2 or 3 things we should ensure are incorporated into the system, such as the auditing feature you mentioned?

Stewart: Yes, I think the most important thing for HIPAA compliance when you're dealing with that business associate would be to make sure the system has some form of audit trail. If someone inappropriately or inadvertently releases information, there is both a civil and a criminal penalty to you because you allowed the release of protected information. I would make sure there were audit trails in place—the ability to audit.

Nelson: Is it the responsibility of the information-system vendor to implement standards and practices other than what are required already of the health care providers? Why are you and Rick [Ford] thinking that a vendor has responsibility other than the standard responsibilities that have always been there for health care providers, such as locking the door to the medical records department?

Stewart: I'll use the pulmonary function testing example. A pulmonary function testing system has a computer hard drive that contains personal health information of individuals who underwent pulmonary function testing. If the information-system vendor comes in and finds there's corruption in the data on the hard drive, he'll have to look into some of those personal health records to determine how the corruption occurred. As soon as he opens that record, he has accessed the information. He's in my hospital doing it as a third party, but I don't have governing right over him. It is also possible the vendor would have to take that hard drive out and bring it back to his company and a third person might look at that patient's data. I need to be able to find out, if a patient asks to see an audit trail of everyone who accessed his personal health information, who that third-party vendor was and who looked at that health information. I have to have the names and know why it was accessed to be able to explain it to the consumer.

MacIntyre: I want to switch gears. I'm a clinician and this management stuff is fascinating, but I think the most pressing problem for us right now is patient safety, especially regarding medications. Why is it taking so long to get a relatively straightforward system that prevents wrong doses or drug interactions? I've got a *Physicians' Desk Reference* on my Palm [handheld computer], so all the information is there. The pharmacy has got all the medications programmed so that they can print out the patient's medication list every day, and yet we don't have a system that looks at just dosing and drug interactions and matching it to patient allergies and reaction. Why is it taking so long to get something as simple as that, and why does it seem to be a lower priority than billing, productivity tracing, and national health databases? Preventing wrong doses and adverse drug interactions should be higher on the priority list.

Stewart: At my own organization we are working to implement that kind of system, by using computerized physician order entry. But, frankly, the information-system vendors haven't yet put the time and attention into creating such a product that I can blend and use.

MacIntyre: Is that because you administrators are more worried about productivity and billing than you are about patient safety?

Stewart: Actually, we are looking at it from a patient-safety perspective.

Hess: One of the things that drove that issue in Boston was litigation. There was a very well known case in the popular media around the country. A patient at one of the Boston hospitals died due do a wrong drug dose. That really drove the things that Neil [MacIntyre] is asking for. I think the clinicians were asking for it, but how they got it was when there was a highly publicized case.

Ward: Every time we get a computer fixed—which is extremely often—some outsider, non-health-care-related person has the opportunity to look through personal medical records. What are the rules regarding vendor and technician access to medical records while repairing a clinical information system? Is that a HIPAA violation?

Stewart: It's acceptable for them to see the information, but you have to have an audit trail of who saw it and when, should you have a consumer complaint. So, yes, they can see it. The concern would be if that outsider were to disclose that information to someone else. You need to be able to track where the information is, because part of a HIPAA criminal penalty proceeding is to determine who released the information.

Ward: How are employees of outside companies, including people who fix computers, supposed to know that they are looking at privileged information? It seems that to be in compliance they would have to sign some form to acknowledge that they are going to see privileged information that they're not allowed to disclose.

Stewart: Actually, that's part of what's called a "business associate agreement." Every company you do business with has to sign a business associate agreement, which includes a provision that they have educated their staff about personal health information and how that information can be released and used.

Walker: I'd like to comment about what Dr MacIntyre brought up earlier, from a clinician standpoint. Last week I was fortunate enough to attend the Emerging Technologies and Health Care Innovations Congress in Washington DC. There were several very good discussions on funding of research of technologies by the federal government. As an example, the Veterans Hospital Administration has received $128 million to research those technologies that you had on one of your slides. But from a clinical standpoint I was very disappointed, because this technology research is on the back end, mostly for billing practices and sharing administrative data between all of the veterans hospitals. I was very disappointed that they're not starting at the front end—with the patient—because it seems that the biggest problem we're having in improving patient care is the interface between the equipment and the patient.

It seems that that research isn't happening at present, which may explain why in health care, especially in the clinical arena, we're so far behind that it's easy to say that you're going to interface a pulse oximeter or a ventilator to an information system, but it's not that easy, especially when you're dealing with small infants, because of their physiologic variables. Also, the folks in England who are developing the information system for their national health care system are spending £300–400 million to link up all their hospitals, but they're somewhat discouraged because the technology just isn't there yet. It seems that we're so far behind in bringing the technology forward, because all the funding is for the basic administrative technologies and not for the clinical side. I hope we can change that.

Hopper: Dr MacIntyre, I agree with what you said. I want to ask how you as a physician feel about allowing the machinery to practice medicine to that degree?

MacIntyre: Well, I don't want the machinery to practice medicine. Allan Morris is always trying to teach me about his decision-making system, which Reed Gardner is going to tell us about later on in this conference. The way Allan explains it to me, it doesn't actually *run* the ventilator. It tells you what it thinks *ought* to be done and then allows you to either accept it or reject it. If you reject it, you have to put in a reason why you rejected it. I'm not comfortable enough yet to have the machine make major decisions for me, but I would welcome the machine giving me advice as to what ought to be done.

Nelson: Just like a good *respiratory therapist* should do!

MacIntyre: Just like a good respiratory therapist should do.

Gardner: One of the things the HIPAA legislation did in 1996 was to provide a means for patient identifiers. That may seem like a trivial thing but it was such a politically "hot potato" that it was dropped from the legislation. What is being done to identify patients? That's a serious problem and we can make serious mistakes if we care for a patient lifelong.

Stewart: I think the current initiative for patient identifiers has come out of the Joint Commission on Accreditation of Health Care Organizations, for developing a standard that requires more than one identifier for a patient. And one of those identifiers cannot be the patient's room number. It also requires proof that you have audited your method of patient identification. For example, the patient identifiers in my organization are the patient's full name and full birth date. Those have to be identified before there is any interaction with a patient.

Gardner: The HIPAA regulations concerning privacy are *regulations*, not *legislation*. Dr Donald Lindberg, director of the National Library of Medicine, told us at a conference this summer that the HIPAA regulations occupy 1,500 pages in the Federal Register. By comparison, the whole Medicare/Medicaid law was only about 30 pages. We've kind of gone overboard haven't we?

Stewart: From an administrative perspective it's a little overboard, yeah.

Volsko: Dr MacIntyre, just to build on your comments, I worked as a care manager with the cystic fibrosis population. I worked with our information technology department to establish physician order sets for intravenous and aerosolized antibiotics. We attempted to put in screens that would pop up and warn the physician entering the orders if dosage parameters were violated, but the order-entry system we were working with was fairly archaic and it was very difficult and complex to program the decision-tree for those pop-up screens. We also had some operator opposition. We need to consider the user; if the user is uncomfortable with the technology, you can have the "best laid" system but still have user resistance and noncompliance.

MacIntyre: Terry, I certainly agree, but my concern is more about prioritization. I just think the problems you identified ought to be at the top of our list, rather than administrative problems, which always seem to take priority over patient care stuff.

Belda: I have a question about a comment you made regarding the bedside therapist not understanding what all is involved with this. Do you have a short list of suggestions you could offer for those planning to implement these changes that will help foster the sensitivity necessary for therapists at the bedside to have a good understanding, and so that others might be able to plan for it as well and successfully implement it?

Stewart: Are you talking about the privacy piece? Every organization was required prior to April 14, 2003, to provide that level of education to *every* employee. Now I find, as I travel around the country, that some organizations haven't. I assisted in writing most of the education material for my organization. Also, it's required upon hire and an annual review, so you don't forget.