Using Computers for Intensive Care Unit Research

Nicholas S Ward MD

A computerized clinical information system (CIS) is potentially a very important information tool for research and improving health care processes as well as for optimizing data management and thereby minimizing health care costs. The newest CISs automatically collect patient data from various sources, including monitors, the laboratory, radiology, and patient notes, and make the data highly organized and readily accessible. In the future CISs may be able to conduct signal analysis, assist in care decisions, provide advanced graphical data presentation, and generate warnings to clinicians. Most CIS systems include large databases, and the advent of relational databases has improved data retrieval and manipulation and thus made the data a powerful tool in outcomes research. On the whole CISs collect more frequent and more accurate data than do clinicians using paper-based data collection systems, but research continues on how accurate CIS data is, how to improve that accuracy, and how much data checking and correction is needed. At my institution we have used CIS data to study changes in patients' code status and to evaluate a protocol for arterial blood gas (ABG) testing. The primary challenges to optimizing a CIS are ensuring accurate data entry, learning to query the data so as to avoid misleading conclusions, and to administer and maintain the hardware and software so as to minimize the chance of data loss and system down time. CISs are in a relatively early stage of their development, and engineering improvements will eventually make CIS data highly accurate and easily accessible and queryable so that CISs become even more valuable for research. *Key words: computers, information management, research, data processing, data collection, research methodology, research techniques.* [Respir Care 2004;49(5):518–522. © 2004 Daedalus Enterprises]

Introduction

Computers are becoming an increasingly large part of the practice of critical care medicine. They are now an integral part of all aspects of intensive care unit (ICU) care and monitoring, from ventilators to medication orders to charting. Over the last decade many elements of comput-

Nicholas S Ward MD is affiliated with the Department of Pulmonary and Critical Care Medicine, Rhode Island Hospital, Brown Medical School, Providence, Rhode Island.

Nicholas S Ward MD 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: Nicholas S Ward MD, Department of Pulmonary and Critical Care Medicine, Rhode Island Hospital, Brown Medical School, 593 Eddy Street, Providence RI 02903. E-mail: nicholas_ward@brown.edu.

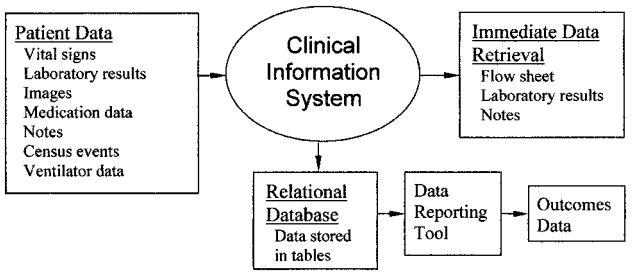


Fig. 1. Schematic of a clinical information system with a relational database.

erized patient data have been linked into *clinical information systems* (CISs). The term CIS, however, is still nebulous. Currently, it is used to describe a diverse array of computer hardware and software that aid in the care of patients. Generally these systems are able to record patient data, either directly, through links with monitoring equipment, or indirectly. A state-of-the-art CIS gets patient data from various sources, such as vital-signs monitors, laboratory data, radiology, and patient care notes, and incorporates those data into a format that is readily accessible and well organized (Fig. 1). These qualities have made CISs increasingly popular in intensive care units, where large amounts of data are generated.

Most CISs today also have features that make them more than just electronic patient charts. A CIS can also incorporate elements such as signal analysis,[1] decision analysis,[2,3] advanced graphical data presentation,[4] and computer-generated warnings that further aid in patient care. In addition, most systems today have large databases. The advent of relational databases has made data retrieval and manipulation much easier. It is the addition of these databases that have made the CIS a potentially powerful tool in outcomes research. An investigator can, theoretically, search for, collect, cross-reference, and analyze tremendous amounts of patient data very quickly.

CIS for Electronic Data Retrieval

One obvious way in which computers can potentially improve research is through gathering, recording, and presenting the tremendous amounts of data generated on patients. This can be a daunting task in the modern ICU where, every minute, data are generated by patient monitors. The ICU also uses laboratory and imaging services more frequently than do other departments. The shortcomings of hand-written patient charts are well documented.[5] The most commonly cited problems with paper charts have been missing records, poor documentation, and illegible writing. A CIS can eliminate handwriting-legibility problems and automatically gather and store all pertinent clinical information, such as medications, vital signs, test results, and narrative notes. Many commercially available CISs today have those abilities.

In terms of gathering physiologic data, a CIS offers 2 potential advantages over other methods. The first is that the CIS theoretically can provide more frequent and accurate data that are more easily stored. This aspect of a CIS seems initially to be nothing but a benefit. Computing and automatic data entry eliminate transcription errors, tabulation errors, and incomplete data, and save time, but, unfortunately, continuous or near-continuous physiologic data entry has some problems: as always, there is the potential for erroneous measurements (eg, when a blood pressure cuff is off the patient's arm) and signal noise, as is common with electrocardiograms. To ensure data accuracy, it is frequently necessary to review data before accepting them into the record. Also, in physiologic data the range of extreme high and low values increases with the frequency of measurement, which can impact the calculation of disease-severity scores.[6]

Another potential advantage of a CIS is the possibility of adding secondary data to the primary data via complex signal analysis. An example of this that is familiar to many is the automatic interpretation of electrocardiogram signals. Many cardiac telemetry systems identify and record events such as ventricular tachycardia through signal analysis. A CIS could potentially record events such as shock and ventilatory failure and analyze them for known patterns by interpreting the primary data. That said, it is unlikely that automatic signal analysis and interpretation by CISs will play an important role in the near future, because the variables of human physiology are so complex.

The CIS Relational Database As a Tool for Research

Much of the current interest in computers for ICU research focuses on databases of clinical information collected during patients' stays. In the early days of CISs the effective use of clinical databases was greatly limited by the technology. More than any other component of a CIS, the database requires a tremendous amount of computer memory. Furthermore, efficiently querying a large database requires a very fast computer. As computer memory and speed have rapidly improved, so have the utility of CIS databases.

The other development that made CISs powerful research tools was the invention of the relational database. A relational database essentially "tags" every piece of data as it is stored, much like a library card catalog. By way of those tags the program can quickly relate a piece of data to other similar types of data without searching the entire database (Fig. 2). A state-of-the-art CIS with a relational database can quickly search years of patient data and re-

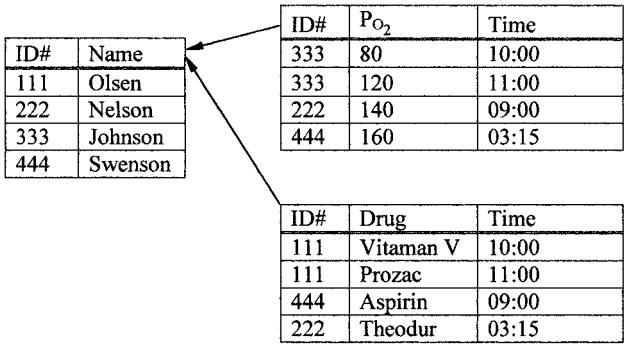


Fig. 2. A simplified example of a relational database showing links between data tables. The patient identification number (ID#) is the key to associating types of data. (Figure courtesy of Steven B Nelson MSc RRT FAARC.)

trieve specific data. Unfortunately, most commercially available CISs either do not have an archived database or have databases that are very difficult or too time consuming to query effectively.

There are 3 fundamental requirements for a database to be useful for outcomes research: accuracy, feasibility, and appropriateness.[7] The problems with accuracy are discussed below. The feasibility of owning and accessing such a database is increasing because the systems are becoming less expensive. The ability to create a large clinical database on site—as is possible with the latest commercially available systems—makes them more appropriate for a given clinician or researcher than most outside databases. Furthermore, outcome data can be analyzed in context with resource utilization data from the same institution. Cowen and Matchett believe this to be perhaps the "greatest ability of a clinical database."[8] In any case, outcomes research on ICU patients should become much more comprehensive and faster to produce with the latest clinical databases.

Problems With Data Accuracy

The potential for data inaccuracy in a CIS is a problem that has not received much attention. Investigators have attempted to determine the accuracy of various commercial and noncommercial databases for measuring specific data such as medications,[9] diagnoses,[10] and patient physiologic data.[11] Wagner and Hogan reviewed 20 studies that compared CIS data accuracy[12] and found that CIS patient data was more accurate than other databases or paper charts. In reviewing this topic Hogan and Wagner helped elucidate the complexity of the problem with computer-based patient records. They divided the concept of accuracy into 2 components: completeness and correctness. Of the 20 studies they reviewed almost all measured only completeness, not correctness.

In addition to that problem most authors who have attempted to validate CIS data accuracy have compared CISs to paper charting. Multiple studies have documented the inaccuracies of handwritten medical records. Instead of being a standard by which to judge CIS data accuracy, handwritten records may be less accurate.[12] A better standard is needed by which to measure data accuracy, but that can be a complex task in a large, comprehensive system.

Examples From a Computerized ICU

At Rhode Island Hospital we have been using a commercially available CIS in our 18-bed medical ICU (MICU) for the last 6 years. In those years we have collected a tremendous amount of data and have used our relational database to answer some important clinical questions. We have also run into many problems. Two topics we have studied with our CIS data include code status and arterial blood gas testing.

Code Status

In order to better understand one end-of-life issue in our MICU, we studied the code status of admitted patients. For the study a row was added to the nursing flow sheet and the nurse was required to pick from a list of code statuses and input the patient's code status at MICU admission (eg, do not resuscitate [DNR], do not intubate [DNI], or full code). On subsequent days, if the patient's code status changed, the nurse was prompted to enter the new code status in the patient flow sheet. The database was queried to determine the numbers and percentages of patients with various code statuses at admission, code-status changes from initial status, and the time to change. The study considered data from a 6-month period. At admission 91.5% of our MICU patients had full code status (no restrictions on advanced cardiac life support or intubation), 4.6% were DNR/DNI, and 3.9% were in the category "other." During MICU stay 25% of the patients' code status changed: 7% to DNR, 11% to DNR/DNI, and 5% to comfort measures only. One percent whose original status was DNR were changed to full code status. Sixty percent of code-status changes were made within 48 hours of MICU admission. Figure 3 shows an example of that type of data.

Arterial Blood Gas Testing Protocol

To evaluate our practices and reduce unnecessary arterial blood gas (ABG) tests in our MICU, we instituted a protocol for ordering them. First we queried our database to determine the daily average number of ABG tests per mechanically ventilated patient. Then doctors and nurses were asked to limit ABG tests to only those situations indicated in the protocol. In the flow sheet the nurse was

Admission Code Status		
	No.	%
Full Code	53	94.6
DNR/DNI	1	1.8
DNR	0	0
CMO	0	0

Change in Code Status				
		Percent Changed During		
No.	%	0–2 days	3–10 days	>10 days
0	0	NA	NA	NA
3	5.4	66.7	33.3	0.0
10	17.9	60.0	30.0	10.0
1	1.8	100	0	0.0

Fig. 3. Data generated by query of patient code status. DNR = do not resuscitate. DNI = do not intubate. CMO = comfort measures only. NA = not applicable.

prompted to choose from a list of reasons the ABG was done. If none of the reasons in the list applied, the clinician could input "other." At the end of the trial period we queried the database to compare ABG ordering before and after implementing the protocol. The protocol decreased the average number of ABG tests per patient per ventilator day from 4 to 2. However, we found that no reason was given (ie, "other" was selected) 92% of the time, indicating poor compliance with the protocol. After further education of the medical staff and eliminating the choice "other," we discovered that a new clinical intervention was the most common reason for conducting an ABG test. Table 1 summarizes the results.

Table 1. Reasons Given for Obtaining an Arterial Blood Gas Measurement After Adjustments

Reason	No.	Percent of Total*
No reason charted	2	> 0.01
Clinical intervention	2201	73.9
Assess P_{CO_2}	54	1.8
New intubation	18	0.6
Other/unexplained	33	1.1
Patient deterioration	156	5.2
Study	89	3.0
Unable to obtain pulse oximeter reading	30	1.0
Ventilator setting change	396	13.3

* Because of rounding, percent values do not total 100%.

Pitfalls of CIS Data

The 2 most common CIS problems are getting quality data into the system and querying the right data. As with any clinical study one must be careful how a question is asked or the resulting data can be inaccurate or confusing. In addition, given that much of the data entered into a CIS is entered or confirmed by human staff, there are limits to how much data can be entered accurately. It has been our experience that the more data entry is asked of the staff, the less accurate and complete the data will be. This makes choosing what data to ask for even more challenging, because quantity impacts quality.

Another major CIS pitfall is technical problems in the hardware and software. At times we have suffered major data losses from our system, from outages of the system and from loss of stored data. Good system administration is a vital component to doing research with a CIS, and the importance of system administration should be emphasized by any group considering implementing a CIS.

Summary

Information gathering via computerized systems is becoming a large part of modern ICUs. These systems offer many advantages over older data gathering systems, including more complete and accurate records. Relational databases enable the study of large volumes of data from various fields and can combine that data quickly and easily. In the future, additional computing capabilities, such as complex signal analysis, could make relational databases even more powerful tools, which should enhance ICU care. Concerns remain about the accuracy of CIS data but in the future the data will probably become consistently accurate enough to facilitate definitive studies.

REFERENCES

1. Goldstein B, Fiser DH, Kelly MM, Mickelsen D, Ruttimann U, Pollack MM. Decomplexification in critical illness and injury: relationship between heart rate variability, severity of illness, and outcome. Crit Care Med 1998;26(2):352–357.
2. Evans RS, Pestotnik SL, Classen DC, Clemmer TP, Weaver LK, Orme JF Jr, et al. A computer-assisted management program for antibiotics and other antiinfective agents. N Engl J Med 1998;338(4): 232–238.
3. Evans RS, Classen DC, Pestotnik SL, Clemmer TP, Weaver LK, Burke JP. A decision support tool for antibiotic therapy. Proc Annu Symp Comput Appl Med Care 1995:651–655.
4. Cole WG, Stewart JG. Metaphor graphics to support integrated decision making with respiratory data. Int J Clin Monit Comput 1993; 10(2):91–100.
5. Sado AS. Electronic medical record in the intensive care unit. Crit Care Clin 1999;15(3):499–522.

6. Suistomaa ME Ruokonen E, Takala J. Lack of standardized data collection causes bias in APACHE II and SAPS scores. Intensive Care Med 1997;23:A545.
7. Pronovost P, Angus DC. Using large-scale databases to measure outcomes in critical care. Crit Care Clin 1999;15(3):615–631.
8. Cowen JS, Matchett SC. The clinical management database. Crit Care Clin 1999;15(3):481–497.
9. Wagner MM, Hogan WR. The accuracy of medication data in an outpatient electronic medical record. J Am Med Inform Assoc 1996;3(3):234–244.
10. Jollis JG, Ancukiewicz M, DeLong ER, Pryor DB, Muhlbaier LH, Mark DB. Discordance of databases designed for claims payment versus clinical information systems: implications for outcomes research. Ann Intern Med 1993;119(8):844–850.
11. Hammond J, Johnson HM, Varas R, Ward CG. A qualitative comparison of paper flowsheets vs a computer-based clinical information system. Chest 1991;99(1):155–157.
12. Hogan WR, Wagner MM. Accuracy of data in computer-based patient records. J Am Med Inform Assoc 1997;4(5):342–355.

Discussion

MacIntyre: What are the HIPAA [Health Insurance Portability and Accountability Act] implications of searching these databases? I realize you're not going to publish patient information, but you are matching things about specific patients to other things without their permission. Are there HIPAA issues?

Ward: Yes, there are. You do need consent from these patients, and approval from your internal review board. Nowadays you're definitely going to need consent if you're going to prospectively collect data that include patient identifiers. If the data is collected only for quality assurance, you don't need consent, but you can't publish it. So that makes it that much harder. At a computer I used to be able in 15 minutes to collect enough data for a report. Now I have to go back and figure out if I need consent and otherwise address data security issues. It's becoming a lot more complicated.

Stewart: If you remove patient identifiers in your database, then you can query that information without it being a HIPAA violation and without needing to have an audit trail of who accessed the information. One thing we've done is to remove patient identifiers and send the clinical information to a central repository. If the data has any patient identifiers, then you have to go through the institutional review board process and have patients' permission to access that information. However, most privacy notices, which patients sign at admission, indicate that the patient allows the use of some information, though the patient can check the restriction clause that reads: "Do not use my medical record for research." It depends on the institution's privacy notice. You can avoid HIPAA problems by having the privacy notice read, "Your clinical information may be used for research."

Pierson:* You touched on quality assurance, and your presentation very nicely showed how data that is primarily generated for one purpose, or maybe a couple of purposes, such as patient management and keeping track of things and billing, can be desirable to use for another purpose such as research. We're all required to do QA [quality assurance] activities and we're often interested in doing research as well.

A commonly done thing is to take this year's departmental QA plan and just write it up and submit it for publication and say, "Look at all this data." From an editor's perspective this has been very problematic. It gets back to exactly what you were saying: "Garbage in, garbage out." You have to design something to be of acceptable rigor for research at the front end before you collect any data if those data are going to be worth anything for research. So a QA activity *can* be valid research if it's designed as that from the beginning. But it's unlikely that if you retrospectively go back to a QA project you've done, that you'll be able to get good enough data to answer the right questions with it to make it fill the needs for research.

Ward: That brings up an interesting point. CISs have been around for about 10 years, depending on where you want to draw the starting line. At the trade shows you hear these vendors describe these systems, and the first thought that pops into my mind is, why aren't researchers around the country cranking out reports on a daily basis if the system could quickly give you perfect data on, say, the rate of ventilator-associated pneumonia in people over 65 who have COPD? I think the fact that we don't see such reports is a tip-off that these systems are not as easy to operate as they are sometimes advertised to be, that the data is not as good as is needed, and that CISs are still in their clunky stage.

Nelson: Correlation does not equal causation. In this data-mining adventure that you described in several of your examples, do you think it's just coincidental that you found those results or was there more than just correlation? Were you able to find causation?

Ward: It depends on which of these things you're talking about. For example, there was a correlation between alcoholism and pneumonia, but that's just a correlation, although some other literature shows that same thing. People in alcohol withdrawal have a very high rate of respiratory failure from pneumonia. Regarding the other stuff

* David J Pierson, MD FAARC, Editor in Chief, RESPIRATORY CARE Journal, Seattle, Washington.

I showed on accuracy, I don't know what to make of that data. I'd chosen 2 commonly used methods for collecting that data, and I compared them and showed there was a difference. And so the question is, which is more accurate? In a number of those cases I'd say my system is more accurate, though I know that's a value judgment. The reason why is that in a couple of those things—not so much with the diagnoses but definitely with things like medications—we are much closer to the point of care than these other systems are. Duration of ICU stay is another example: we're much closer to where the duration of stay decision is made in the hospital computer. So I can't prove that our duration-of-stay data is more accurate than some other institution's duration-of-stay data, but ours is collected by the team taking care of the patient. It's almost as good as if I had a research nurse in my ICU prospectively collecting that data.

Volsko: When you said that your system is more accurate than the hospital's system, especially with your reference to duration of stay, is it really a matter of *accuracy* or is it standardization? I encountered a similar problem when analyzing cystic fibrosis data. I captured my cystic fibrosis duration-of-stay data based on a 24-hour rolling calendar. I looked at date and time of admission, and date and time of discharge, in 24-hour increments. So if you were admitted at 2:00 in the afternoon on April 1, at 2:00 in the afternoon on April 2nd that was 24 hours, whereas the hospital looked at their data on the 24-hour rolling calendar based on the midnight census. Before that problem was corrected it caused disparities and an inability to compare baseline to care path outcomes when duration of stay was calculated. Wouldn't it behoove us to standardize those practices to capture the most accurate reflection of what our patients are doing, and so that we can compare that within and among institutions, to facilitate benchmarking?

Ward: That's exactly right. That form of error came in dramatically in the data for time on the ventilator. I had 2 systems for calculating time on the ventilator in terms of days, which is kind of loose, and they weren't standardized to each other. That *could* reflect some of the difference in duration of stay but, clearly, with differences up to 8 days or more. The point I *thought* you were going to make is that the hospital system is more accurate because the patient really *is* in the ICU for, say, 8 days. One could argue that, too.

Gardner: How did you get the data out of the CareVue [CIS] system into your [Microsoft] Access database?

Ward: All I have to do is launch Access and it accesses the CareVue database through some intermediary software. I have a lot of help with that part by people who understand the system better than I do.

Gardner: But did you do your database searches on a separate desktop computer that *wasn't* on the CareVue system, or *was* it on the CareVue system?

Ward: CareVue operates on desktop computer. The computer in the head nurse's office is configured with Access so that it plugs right into the CareVue database, which I guess is kept in the bowels of the hospital.

Gardner: The reason I ask is that part of the issue you're talking about is data mining and data structures. There would be things that you'd want to do in CareVue, such as you'd want data to come up quickly and have it organized in a different way than you'd want it for the database searches. Many people have 2 or more copies of the database—secondary databases that we call "datamarts." Pharmacy data, for instance, would be in one datamart, data about ICD-9 [International Classification of Diseases, Ninth Revision] codes would be in another datamart, and so on. We use that strategy because there are researchers who query the HELP system [Health Evaluation Through Logical Processes system, at LDS Hospital in Salt Lake City, Utah] and they look at 10 patients and find something interesting and then want to look at the data for last 10 years, which can dramatically impact the speed of the clinical data collection system. So generally you pull that data off to a datamart. I've heard the complaint about CareVue and other systems that the data are very hard to get out of the vendor system to pull off into datamarts.

Ward: There is some sort of datamart intermediary in between Access and the database.

Walker: It really caught my attention that not all of the ventilators interface with your CIS, which necessitates manual data entry. That dovetails into Rob Chatburn's discussion[1] about ventilator manufacturers. I'm not so sure that all the ventilator manufacturers have it as a high priority to interface their ventilators to CISs. At the technology meeting in Washington DC last week, I was assured that there are many standards being discussed and that the vendors are being included, but when I talked to the ventilator manufacturers, I got the impression that that's really not the case.

From a respiratory care standpoint my concern is that our devices might be somewhat left out while all the other devices are electronically interfaced with the CIS. However, at the same time, are we going to have to buy a whole new fleet of ventilators to electronically capture patient data? If we're going to improve our productivity by using these emerging technologies, I think that we have to get the manufacturers to work with us both with regard to the "front end" (the user interface) and the "back end," so that the devices interface with CISs.

REFERENCE

1. Chatburn RL. Computer control of mechanical ventilation. Respir Care 2004;49(5): 507-515; discussion 515-517.

Ward: I agree.

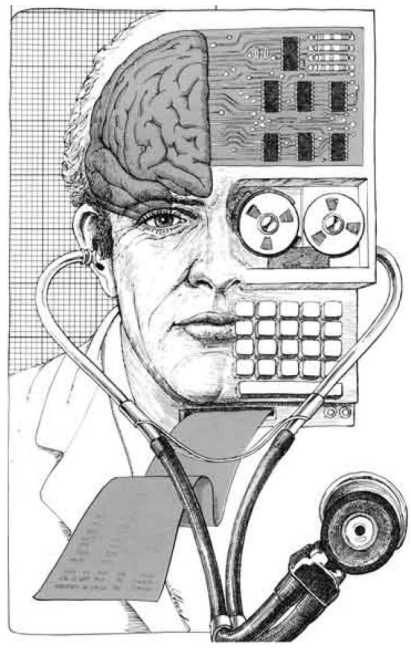
Gardner: There is an Institute of Electrical and Electronic Engineers [IEEE] standard, number 1073,[1–3] and we've been using versions of it for more than a decade. The whole industry, including vendors such as CareVue and manufacturers of bedside monitors and ventilator equipment, has to use it. The standards work, but we've got to get *all* vendors to use them.

REFERENCES

1. IEEE 1073 Medical Device Communications. Available at: http://www.ieee1073.org. Accessed March 4, 2004.
2. Kennelly RJ. Improving acute care through use of medical device data. Int J Med Inf 1998;48(1–3):145–149.
3. Kennelly RJ, Gardner RM. Perspectives on development of IEEE 1073. The Medical Information Bus (MIB) standard. Int J Clin Comit Comput 1997;14(3):143–149.

Walker: Dr Gardner, is that something you could have input into? You're on the leading edge and you make these devices work. Do you see that happening in the near future?

Gardner: Yes I do, and you can too, because the IEEE establishes standards with a consensus process. They're the people who came up with Ethernet and lots of other standards. There's a very active group, and I was involved in the standardization development process for about 10 years.



Artificial Intelligence (Brochure, US Government Printing Office, 1980).
Courtesy National Library of Medicine

Not So Fast! The Dark Side of Computers in Health Care

Steven B Nelson MSc RRT FAARC

There are now computers in numerous health care devices, from thermometers to ventilators, and there are pitfalls to avoid in our increasing dependence on computers. To be useful, information must be delivered in the right context. Computer systems must be protected from worms, viruses, and other harmful code, and they must prevent unauthorized access to data. The source of all underlying decision algorithms must be known and appropriate for the population being served. And there must be contingency plans to mitigate losses caused by system unavailability. *Key words: computers, computer security, medical informatics, software, data security, data protection, patient data privacy, information management, medical errors, medication errors, computer viruses, computer hackers, disaster planning.* [Respir Care 2004;49(5):525–530.

Introduction

This conference has so far extolled the virtues of computerizing nearly every application imaginable in respiratory care. Though that is a commendable goal, there is a "dark side" to computers that extends beyond the sensational headlines on the nightly news warning of the latest virus or identity theft scheme.

The goal of this report is not to support a Luddite mentality regarding technology but to warn of pitfalls that may be encountered before and after the decision to use a computer as a solution. The Luddites were originally a group of displaced textile workers. In the early 1800s steam- and water-powered weaving and spinning frames were being installed in an area of Nottingham, England. By 1811 the workers had banded together under "General" Ned Ludd and formed the "Army of Redressers."[1] Their goal was to destroy the frames and regain their jobs. By 1812 over 800 frames had been destroyed. The movement was crushed after a defeat at Lancashire and the declaration that destruction of a frame was a capital offense.

In the mid-1990s various neoLuddites, including Ted Kaczynski (the "Unabomber") warned that computers were evil and exclusionary. Ironically, they used the very tools they derided to write and spread their message. Though Kaczynski proved to be a murderous madman, he made

Steven B Nelson MSc RRT FAARC is affiliated with Pulmonary Industrial Testing Associates, Overland Park, Kansas.

Steven B Nelson MSc RRT FAARC 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.

Steven B Nelson MSc RRT FAARC is a technical consultant for Sun Microsystems, Santa Clara, California. The opinions in this report are solely those of the author and do not represent the views of Sun Microsystems.

Correspondence: Steven B Nelson MSc RRT FAARC, Pulmonary Industrial Testing Associates, 8314 W 128th Street, Overland Park KS 66213. E-mail: sbn_kc@mac.com.

several cogent points regarding computers and decision-making; he warned of a future where (1) decisions will become so complex that humans won't be able to process all the data, (2) decisions will be made by a small group acting as a "benevolent parent," or (3) decisions will be taken from humans by accident.[2] Those warnings are pertinent to the growing use of computers in health care. This report proceeds on the premise that computer technology should not be avoided but should be considered no more than a tool. I will provide information and opinion on how we can wisely and safely use that tool.

A principle to be aware of is the "rule of unintended consequences," which is illustrated by the use of DDT to control malaria-carrying mosquitoes. The mosquitoes developed resistance to DDT, and the DDT concentrated in the food chain and resulted in weakening of bird eggshells, causing a rapid decline in birds of prey and an increase in rodents. Often people are tempted into what appears to be a quick solution to a problem, and they implement it without proper analysis that could avoid unexpected results and cascading consequences.[3]

There are 7 subjects to address regarding computers and information management: rights, security, reliability, regulations, support, acceptance, and privacy.

Rights

Pharmacists speak of 4 "rights": the right medication, in the right dosage, by the right delivery method, to the right patient. Health care information has a similar set of "rights": the right information, in the right time frame, delivered in the right format, to the right user.

The right type of information is derived from a hierarchy, such as the one in Table 1. Data by themselves are not generally useful. They require a context to become information. Knowledge of the subject matter is needed to determine whether the data are normal or valid. Understanding allows one to create new knowledge to assess the patient. Wisdom is the integration of knowledge from multiple sources and the ability to apply judgment and respond. Many computerized systems are unable to rise above the knowledge level, primarily because of a lack of integrated information. The following example and Table 1 show the hierarchy. Say a respiratory therapist (RT) is given the value "42." By itself that piece of data is useless, because it could be the value of any of several physiologic variables, including P_{aO_2}, P_{aCO_2}, or hematocrit. Knowledge that it is a P_{aCO_2} value would lead the RT to the conclusion that the value is in the normal range. Additional information that the patient is on a ventilator, has acute lung injury, and is supposed to be maintained with permissive hypercapnia might lead to the conclusion that the minute ventilation was too high. As the Mexican novelist Carlos Fuentes said, "The greatest crisis facing modern civilization is going to be how to transform information into structured knowledge."

Table 1. Information Hierarchy

Data	42
Information	FEV_1/FVC, P_{aO_2}, P_{aCO_2}, hematocrit
Knowledge	COPD, hypoxia, normocapnea
Understanding	Change bronchodilator, increase F_{IO_2}
Wisdom	Judgment of correctness

FEV_1 = forced expiratory volume in the first second; FVC = forced vital capacity; F_{IO2} = fraction of inspired oxygen.

Information has a time value. A normal result from a screening spirometry of a patient in an extended care facility may be delivered after many hours. Normal spirometry in a dyspneic emergency-room patient is generally reported within minutes. The findings might be the same, but in the emergency room the information might cause immediate changes in treatment.

Information's format should be appropriate for the device that receives it. It makes little sense to send more than a few seconds of video to a mobile computer such as a personal digital assistant, because those devices do not have large enough displays, enough memory, or fast enough data-transfer, though with engineering improvements that may change.

Information should be delivered to the right user. There are many classes of information in a hospital and many people who provide care for a hospitalized patient. Only the *required* information should be made available. For example, it is probably not necessary for a billing clerk to see an RT's comments about colorful, thick secretions, although a medical records clerk may need that information for diagnostic coding purposes.

Security

Computer security depends on software elements, physical elements, and human elements. Software security involves preventing the running of inappropriate code (eg, worms, viruses, or Trojan horses). A worm is a self-replicating, self-propagating program. Robert Morris at Cornell University wrote the first widespread computer worm in 1988. It exploited a weakness in an e-mail program used by nearly all of the 56,000 computers connected to the Internet at the time. In a matter of hours it had slowed communications to a crawl. Morris soon realized the extent of the damage and tried to send out a message about how to stop it, but many of the systems had already been disconnected from the Internet. It took about 5 days to recover and bring the systems back online. In September 2003 a worm called Sobig.F exploited a weakness in a widely used e-mail program, and it spread to about 150,000,000 computers in a matter of days. It created havoc on the Internet, primarily by the vast number of e-mail messages it was generating. Internet service provider AOL

scans incoming e-mail for viruses, and at the peak of the outbreak they found 23,000,000 copies of the worm during 1 day. Recently worms have been responsible for computer outages in hospitals, government offices,[4] airlines,[5] and nuclear facilities.[6] Even after 15 years of experience that well-known computer exploitation method is still effective.

A computer virus differs from a computer worm in that a virus requires a user action to activate it. Most viruses, such as Melissa and Blaster, take advantage of functions in commonly used desktop-computer applications. A user is enticed to open a file or an e-mail message that appears to be from an acquaintance. Opening the file or message runs a program that can alter files and/or send more e-mail messages to replicate the virus. Viruses are simple to write, using a common scripting language found on nearly every desktop computer. Numerous Internet sources show the basics of writing viruses, and all that is required after writing the virus is to attach it to an e-mail message and send it.

Trojan horses are small programs hidden in larger programs. They can open a "back door" in a computer and thus give access to unauthorized users. One type of Trojan horse is called "spyware," which resides within a program installed by a user and sends information about the user's operating system, memory, hardware, and/or software to the company that wrote the spyware. Spyware can be used to monitor for illegal distribution or for marketing. It may also do nothing more than connect to a company Web site to check for updates. The most prevalent example of spyware is in Web browsers. By setting the Web browser's "cookie" authorization to "prompt" (rather than "accept" or "block"), you can see how many cookies a Web site is attempting to place on your computer and surmise how much information would be passed. (Cookies are small files used to track Web page accesses or transactions.)

Software security measures are simple to implement. Security steps include:

- Do not open attachments in e-mail messages. Attachments are the most common means for spreading viruses.
- Regularly install security patches, which should be obtained only from a known source.
- Install antivirus software in all the computers in your system, including computers that can connect from the outside through a dial-in or virtual private network. The virus scan function should be set to start automatically on a regular basis.
- Keep the antivirus software up to date. Antivirus companies quickly respond to new threats and issue upgrades as viruses are found. The false sense of security offered by outdated antivirus software is probably more dangerous that not having any installed at all.

Physical security concerns access to a computer or a network connection. A computer should be secured to an immovable object to prevent theft. The computer's case should be locked, if possible, to prevent removal of disks or other components. Disks can easily be removed from an unsecured case and the data read on another computer.

No computer should be connected directly between the Internet and an internal network at the same time, because that may allow unauthorized access to restricted information if the system is compromised. Though that configuration may sound rare, consider that many laptop computers include both a wired Ethernet connection and a wireless connection. An improperly configured network card may allow a connection from one source to be bridged to the other source, thereby circumventing normal network access methods.

Implementation of a physical security plan is usually the responsibility of the asset management, security, information technology, and/or networking departments. The appropriate groups should be contacted before connecting any device (wired or wireless) to a hospital information system.

Computer security also includes a human element. The phrase "social engineering" has been used to describe exploitation of a computer user's trust to gain unauthorized access to systems or information. Staff education is the most effective means of prevention. Computer security policies must be included in new-employee orientation and reviewed regularly. Like patient information, information regarding computer systems should never be given to anyone who is not positively known to have the authorization for the information, no matter how authoritative he or she sounds.

Passwords should never be shared. They should be difficult to guess and changed regularly. In many cases a simple "dictionary attack" can identify a password. A simple method for creating good passwords is to select a phrase that is easily remembered and then take the first letter or number of each word and the punctuation to create a string. For example, the phrase "Four score and 7 years ago" could be used to create the password "Fsa7ya", which is secure from a dictionary attack and reasonably easy to remember, even though the characters appear to be random.

Finally, managers should be certain that employee access to all computers is terminated immediately when employment ends, voluntarily or otherwise.

Reliability

Computer reliability depends on starting with a good design. Any project, whether it involves hardware or software, must start by defining the problem to be solved, what is available at present, and what needs to be done to reach the goal.

Software reliability is critical to maintain a functional computing environment, but unfortunately, software is far

from perfect. Almost every program of any length has errors, as anyone who has seen a computer freeze with the "blue screen of death" or "general protection fault" can testify. Industry estimates predict 1–5 software defects per 1,000 lines of code. Even attaining Six Sigma levels of quality (99.9999% accuracy) allows 38 defects per million lines of code. Current estimates of the economic impact of faulty software are in the range of $60 billion per year.[7]

In extreme cases software defects have caused injury and death. The most widely publicized case of death due to software involved a cancer-treatment radiation device, the Therac-25, which was manufactured by Atomic Energy of Canada Ltd[8] between 1985 and 1988 and was used for cancer treatment at several centers in the United States. It was designed to deliver a radiation dose of 10–200 rads, but if a certain sequence of keystrokes was entered, a software bug prevented proper control of the beam intensity and the device could administer 1,000 to over 4,000 rads. Six patients died from radiation exposure or complications. The only clue that something was wrong was an error message: "Malfunction 54." The malfunction codes were to be used by Atomic Energy of Canada Ltd to determine problems, but that particular error code did not even exist, according to the company's documentation.

Hardware reliability can be measured in terms of "uptime" (percentage of time the system is operational vs nonoperational) and response time. The up-time and response time influence the *service-level agreement*, which is an agreement between the user and the computer system's support staff. It specifies contact information, maintenance periods, and expected availability. The service-level agreement may be included as part of the hospital-wide information system plan, but it may be necessary to obtain a separate agreement if the respiratory care department's management information system is a stand-alone system apart from the hospital-wide information system. A service-level agreement might, for example, state that one goal is to have 99% of all new or changed orders sent from the floor to a respiratory care management system in under 10 min. That might require timely logging of the order at or near the patient, a network connection from the terminal to the hospital information system, translation of the order information by a common data dictionary, then formatting for a respiratory care management information system.

Factors that commonly affect system availability are the mean time between failures and the mean time to repair. Hardware and software vendors should know those values. If the basic components are not reliable enough to provide the desired reliability or service, different architectures are available that have better reliability.

Information technology is fragile, and our increasing dependence on it has left us susceptible to large-scale disruptions. A recent example was well documented.[9–11] A simple file-sharing search created a chain reaction of events that led to a 4-day system outage at Beth Israel Deaconess Medical Center (Boston, Massachusetts) in November 2002. The chief information officer was very forthcoming with the event details, in order to help other hospitals assess their exposure and plan for similar occurrences. One of the benefits of the outage was that it caused the institution to develop the ability to isolate systems during subsequent e-mail worm attacks and thus prevent other extended outages. When the SQL Slammer worm struck in January 2003, it caused only a short outage of 6 hours. When the W32.Blaster worm struck in August 2003, they were able to stop it before it even entered the system. Other institutions were not so well prepared and wasted thousands of hours in removing the virus.[12]

The best method to reduce risk is to minimize equipment and software. For example, there is little reason to have a floppy disk drive on a networked computer. Eliminating floppy disk drives prevents outside disks from being used, reducing the chance of a virus entering via that route. Software should be limited to only what is required for the tasks to be conducted on that computer. The most widely used desktop software has unfortunately been shipped and installed with a number of usually unneeded services turned on. These may provide an avenue for unauthorized access. The information systems team should be consulted to make sure that only required network ports are open and other services are shut down.

Loading multiple versions of software can cause problems with licensing and software piracy. The alternative is centralized application servers that distribute only authorized applications to authorized smart terminals (known as "thin clients") that do not have local hard drives or local software, thereby reducing support costs. They can also be configured so that information follows the user. For example, an RT can check a master schedule from any terminal. Use of "smart cards" allows information to follow the RT from unit to unit so that he or she does not need to repeatedly log in, access the schedule page, then log out. The card provides authentication and a central server remembers what was being viewed and displays it in the new location.

Medical computer systems should strive for the same reliability that users of the telephone system have come to expect. Computer system administrators should work toward making the systems robust enough to provide critical information even in the event of power failures or natural disaster. Identification of critical systems needs to be an institution-wide effort. The institution's business continuity plan should delineate what will be done during computer system failure.

Corporate longevity is also an issue. Many software companies did not survive the recent economic depression. To mitigate the risks from companies going out of business, proprietary software source code should be held in escrow so that if the company fails, the source code can be

used for creating replacement software. Companies are frequently bought and sold, and support needs to be available regardless of who is the current owner of the company, so support contracts should cover the possibility of corporate successors. Also it is wise to minimize proprietary components. For example, if information exchange depends on a specific widget from a single vendor, failure of that vendor could jeopardize access to information.

Regulations

The Food and Drug Administration (FDA) specifically recognizes as "medical devices" software products used by blood banks in their collection, maintenance, and distribution of blood and blood components.[13] In addition, the FDA's Center for Devices and Radiological Health has issued guidelines for premarket submission of medical device software.[14] The extent of the software review required is proportional to the severity of injury that a device could permit or inflict. Those guidelines establish requirements for software development, traceability, validation, verification, and testing. It also requires a list of all unresolved software anomalies (bugs) and their impact. Hardware must be described and tested in a similar manner. In general, software that is written for a single purpose and not further distributed does not fall under the regulations of the FDA and Center for Devices and Radiological Health. However, it is the software author's responsibility to make sure that the same procedures are followed for due care and diligence.

Support

Software support is simple with purchased software products: you simply pay for the level of support you require. Support for custom-made applications is more difficult. If an RT writes a program that becomes an essential part of everyday operations, there is the risk that if that person leaves the department, he or she may no longer be able or willing to support the software. In most cases it is unwise to depend on a single individual to write and support a critical software element.

Acceptance

Before final acceptance of a system there are several questions to ask. The purchase agreement should state whether you are purchasing the software itself or only a license to use the software and, if the latter, what is the period of use. Any information classification or diagnostic algorithms should be based on current best practices and references must show the source of medical authority. If the algorithms are not applicable to your institution, you must determine whether they can be changed and whether practice changes required by evidence-based medicine are reflected in new versions of the software.

Privacy

In the words attributed to Sun Microsystems' Chief Executive Officer Scott McNealy, "You have no privacy: get over it!" Though the Health Insurance Portability and Accountability Act provides safeguards to protect health information, many people unknowingly sign away their privacy when they fill out credit applications, insurance forms, and other forms, most of which include explicit permission to release health information. Whether access to that information is actually *needed* remains debatable. There are 2 medical data bureaus that catalog all information submitted by health care providers to insurance companies. By aggregating disparate bits of information from numerous sources a complete health profile might be reconstructed.

Summary

A computer should be recognized as nothing more than a tool, no greater in importance or mystique than a chain saw. As such, proper training is required for safe use. Information must be delivered only to authorized users as it is needed. Systems need to be protected from software threats, such as viruses, and from hardware threats, including unauthorized access and theft. Employees need to know security policies and how to prevent system compromise. Technology will break down; plan for that and identify methods for mitigation.

One hundred and sixty years ago Henry David Thoreau warned of the dangers of technology becoming our master when he said, "We do not ride upon the railroad: it rides upon us."[15] Rob Chatburn provided more optimistic advice about 20 years ago, which is still relevant today: "Whether we use or are used by computers. . . depends on how well we understand them."[16]

REFERENCES

1. Charnwood Borough Council. History of Charnwood. February 2003. Available at: http://www.charnwoodbc.gov.uk/charnwood/history.htm. Accessed February 27, 2004.
2. Kaczynski T. Industrial society and its future. 1997. Available at: http://www.time.com/time/reports/unabomber/wholemanifesto.html. Accessed February 27, 2004.
3. Joy B. Why the future doesn't need us. April 2000. Available at: http://www.wired.com/wired/archive/8.04/joy_pr.html. Accessed February 27, 2004.
4. Computer worm wiggles way into beacon hill network. August 13. 2003. Available at: http://www.thebostonchannel.com/news/2403530/detail.html. Accessed February 27, 2004.
5. Lemos R. 'Good' worm, new bug mean double trouble. August 19, 2003. Available at: http://zdnet.com.com/2100–1105-5065644.html. Accessed February 27, 2004.

6. Poulsen K. U.S. warns nuke plants of worm threat. September 3, 2003. Available at: http://www.securityfocus.com/news/6868. Accessed February 27, 2004.
7. The economic impact of inadequate infrastructure for software testing. Gaithersburg MD: National Institute of Standards and Technology; May 2002.
8. Leveson N, Turner CS. An investigation of the Therac-25 accidents. IEEE Computer 1993;25(7):18–41.
9. Bednarz A. Hospital sounds alarm after 3-day struggle. November 25, 2002. Available at: http://www.nwfusion.com/news/2002/1125bethisrael.html. Accessed February 27, 2004.
10. Kilbridge P. Computer crash—lessons from a system failure. N Engl J Med 2003;348(10):881–882.
11. Weise G. Emergency surgery on a hospital computer system. March 1, 2003. Available at: http://www.spectrum.ieee.org/WEBONLY/wonews/mar03/bhosp.html. Accessed February 27, 2004.
12. IT department works its magic. Aug 29, 2003. Available at: http://mercy.winningit.com/news/news8–29-03.asp. Accessed February 27, 2004.
13. Zoon KC. Letter to computer software manufacturers. Software used in blood establishments (3/31/94). Section 201(h) Federal Food, Drug, and Cosmetic Act (the Act) [21 U.S.C. 321(h)].
14. U.S. Department of Health and Human Services, Food and Drug Administration. Guidance for FDA reviewers and industry guidance for the content of premarket submissions for software contained in medical devices. May 29, 1998.
15. Thoreau HD. Thoreau, Henry David. Walden and civil disobedience. Thomas O, editor. New York: W W Norton & Co; 1966:62.
16. Chatburn RL. Dynamic respiratory mechanics. Respir Care 1986; 31(8):708–711.

Discussion

Gardner: The FDA regulates software under the 1976 Medical Devices Act and they classify and regulate software as a "contrivance." They regulate devices such as the Therac-25 radiation therapy device,[1] but the only medical-records software they've regulated so far is that used for blood banks. The American Medical Informatics Association and other groups I've been involved with have published on the topic.[2] Clearly, devices such as implantable pacemakers and defibrillators need to be regulated. I'm not sure that Microsoft Word, WordPerfect, or Excel files need to be regulated. At this point the FDA is not doing that.

REFERENCES

1. Leveson NG, Turner CT. An investigation of the therac-25 accidents. IEEE Computer 1993;25(7):18–41.
2. Miller RA, Gardner RM. Recommendations for responsible monitoring and regulation of clinical software systems. J Am Med Inform Assoc 1997;4(6):442–457.

Nelson: I think you're correct up until your last sentence, that Microsoft Word and Excel files don't need to be regulated. Several people at this conference have said that they use Excel spreadsheets to make clinical decisions. If you can't depend on Excel having an audit trail that shows everything has been tested and if you're not absolutely sure that it works as expected, you shouldn't be using it. If you're assuming that because it came from Microsoft it's bug-free and all the calculations are correct, you're probably making conclusions that shouldn't be made. The other thing about software is that the FDA doesn't exactly regulate software per se, but the software in a handheld spirometer *is* regulated.

Gardner: Yes, that's a medical device.

Nelson: Right. If you move the information that's displayed on the handheld spirometer's screen from one line to another line, then you need to resubmit the device to the FDA, because it's a change in the device. So whether it's software, hardware, or the system, that's where the fuzziness comes in as far as the FDA is concerned. I agree with you on that.

Gardner: I would just point out that Microsoft Excel will do a lot better than most physicians or parents in calculating medication doses for children. Vilma Patel[1] did some very interesting research on how people guess at what should be done. There have been jokes about people swallowing suppositories, but that really happens. I would still disagree with you.

REFERENCE

1. Patel VL, Kaufman DR, Arocha JF. Emerging paradigms of cognition in medical decision-making. J Biomed Inform 2002; 35(1):52–75.

Nelson: And that's why the two of us got sued for $98 million for testing computerized spirometers a decade ago.

Giordano:* You said not to use Microsoft Outlook. What do *you* use?

Nelson: There are other e-mail programs available, such as Eudora and Mulberry, which come pre-configured with automatic opening of attachments turned off, with all the other things that Outlook assumes that you want to do and turns on for you by default. I'm not saying you shouldn't use Outlook, but if you use it, be aware that those functions are turned on and that bad things can happen without your knowledge. Of course you can always get a Macintosh computer. I noticed that with the mannequin that Dr MacIntyre showed us in his presentation, all the slides appeared to have come from a Macintosh, so apparently they're using a Macintosh to control that quarter-million-dollar mannequin.

* Sam P Giordano MBA RRT FAARC, Executive Director, American Association for Respiratory Care, Irving, Texas.