Computerization Can Create Safety Hazards: A Bar-Coding Near Miss

Clement J. McDonald, MD

Increasing numbers of hospitals are implementing bar-coding systems to prevent errors in patient identification. In the present case, a diabetic patient admitted to a teaching hospital was mistakenly given the bar-coded identification wristband of another patient who was admitted at the same time. When a laboratory result that documented the diabetic patient's severe hyperglycemia was entered into the other patient's electronic medical record, the latter patient seemed to have a very high glucose level and was almost given what could have been a fatal dose of insulin. This near miss shows that computer systems, although having the potential to improve safety, may create new kinds of errors if not accompanied by well-designed, well-implemented cross-check processes and a culture of safety. Moreover, computer systems may have the pernicious effect of weakening human vigilance, removing an important safety protection. Researchers should continue to study real-world implementation of computerized systems to understand their benefits and potential harms, and administrators and providers should seek ways to anticipate these harms and mitigate them.

Ann Intern Med. 2006;144:510-516. www.annals.org

For author affiliation, see end of text.

"Quality Grand Rounds" is a series of articles and companion conferences designed to explore a range of quality issues and medical errors. Presenting actual cases drawn from institutions around the United States, the articles integrate traditional medical case histories with results of root-cause analyses and, where appropriate, anonymous interviews with the involved patients, physicians, nurses, and risk managers. Cases do not come from the discussants' home institutions. The physicians and nurse involved in this case were interviewed by a Quality Grand Rounds editor in May 2005.

Summary of the Case

At admission to a large hospital with a sophisticated computer-based physician order entry (CPOE) system that relies on a bar-coding patient identification mechanism, Mr. P., a man admitted for pneumonia who had no history of diabetes, was given the bar-coded patient identification bracelet of Mr. D., a diabetic patient admitted with cellulitis. Mr. P. and Mr. D. were then transferred to separate medical wards in the hospital and became the subjects of a potentially fatal near-miss laboratory error.

The Case

Mr. P., an 80-year-old man with dyspnea, fever, and cough, was seen in the urgent care clinic of an urban hospital. He received a diagnosis of pneumonia and was started on intravenous ceftriaxone and oral doxycycline therapy. At the same time that Mr. P. was being admitted, Mr. D., a patient with diabetes mellitus, was also seen in the urgent care clinic for severe cellulitis, and the decision was made also to admit him to the hospital. He had been given a bar-coded identification wristband as part of the standard check-in procedure. Following standard procedure for admission to the hospital from the clinic, an admitting clerk created a second inpatient bar-coded wristband. As Mr. P. and Mr. D. were being simultaneously admitted, the clerk printed 2 wristbands, 1 for each patient. The clerk inadvertently placed Mr. P.'s wristband on Mr. D.

Mr. D., the diabetic patient, was admitted to a general surgical ward wearing 2 wristbands—the correct one that had been placed when he was in the urgent care clinic and the incorrect one (Mr. P.'s wristband) that had been placed when he was admitted to the hospital. His physician ordered a fingerstick test to obtain a glucose value. The nurse, not noticing that Mr. D.'s 2 wristbands differed, scanned the incorrect wristband (Mr. P.'s), completed the finger-stick test, and downloaded the results into the laboratory's computer system, which then automatically transferred the results into Mr. P.'s electronic medical record.

Meanwhile, while Mr. P. was still in the admitting area, the clerk began to put the remaining inpatient identification wristband on his wrist. At that point, the clerk realized that he had switched the 2 patients' wristbands. He printed a new wristband, placed it on Mr. P.'s wrist, and sent him to the transitional care unit. The clerk then called the general surgical ward, explained that Mr. D. almost certainly had on an incorrect wristband, requested that the nurse remove it, and sent the correct wristband to the general surgical ward. The correct wristband was lost in transit to the general surgical ward and was never placed on Mr. D.'s wrist.

Faithfully Propagated Errors

Although the clerk made a valiant attempt to correct the mislabeling, it obviously was not successful. The strength of bar-coding systems is their easy and reliable

See also:

Web-Only
Appendix
Conversion of figure into slide

Improving Patient Care is a special section within *Annals* supported in part by the U.S. Department of Health and Human Services (HHS) Agency for Healthcare Research and Quality (AHRQ). The opinions expressed in this article are those of the authors and do not represent the position or endorsement of AHRQ or HHS.

transfer of information from a printed document or label to a computer with read error rates of less than 1 in 10 million characters (1). Error rates in keying and typing, in contrast are 3 to 10 per 1000 characters (2, 3). However, bar-code technology is no panacea. It guarantees only that the information recorded on the wristband is transmitted to the computer faithfully. It does nothing to ensure that the information on the wristband—which carries errors of approximately 1 per 1000 admissions—is correct in the first place. Two kinds of errors can lead to wrong wristband information: errors at registration time, such as selecting the wrong patient from a menu of many patients with the same name, or placing a wristband on the wrong patient. Such errors in the wristband content propagate "faithfully" as patient identification errors to any downstream computer system.

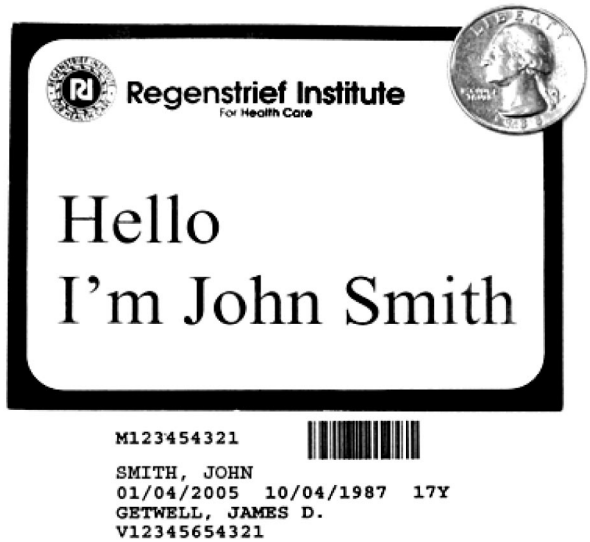
Bar-coded wristbands are most beneficial when institutions also assign bar codes to products, such as medications and blood products, independently from the wristband bar code. In that case, scanning the patient's wristband and the product label at the bedside ensures that the right product is going to the right patient. In fact, the bar-code system, as deployed, would have ultimately uncovered the fact that Mr. D. was wearing Mr. P.'s wristband during the process of checking that wristband against Mr. D.'s delivered medications. The error occurred because the identification for the bedside glucose test result was taken by the testing machine *directly* from the incorrect wristband. Thus, such bedside testing is at special risk for wristband errors.

Hospital personnel may think, "We use bar-coded wristbands, so what could go wrong?" The strength of single-line defenses is always illusory. Recall the Maginot line, France's single defense line, past which Nazi tanks and planes streamed to Dunkirk in 1940. Redundancy is the best defense. Accordingly, the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) (4) requires that 2 identifiers be verified before any blood is drawn or any medication or blood product is dispensed. Asking the patient his or her name counts as 1 identifier. Of course, it always makes sense to ask the sentient patient who he or she is. Asking "What is your name?" rather than, "Are you Mrs. Smith?" yields the most accurate information (5).

Verifying 2 separate wristband identifiers, such as the patient's name and chart number, also satisfies JCAHO's 2 identifier rules. However, reading a wristband challenges visual acuity. The font on 1 vendor's bar-code label is 1/16 of an inch high, a fraction of the font size that meeting managers print on the standard "Hello, I am John Smith" name tags (**Figure**). Larger fonts that can be read as easily at a distance as party name tags should be used for hospital wristbands and other patient labels.

Finally, it is possible that bar codes are not the best technological solution to the problem of incorrectly identifying patients. Bar-code wands can only read what they

Figure. **A typical bar code font (*bottom*), compared with the font size of a typical party name tag (*top*).**



can "see." Therefore, the nurse must move bed covers, turn the patients' wrists, and rearrange medication packages to read the attached bar-code labels. Nurses object to the extra time and effort this requires. They do not like disturbing the patient's sleep at night when they move the patient's arm to scan the wristband and log the hanging of each intravenous bottle (6).

A novel intervention, radio frequency identification (RFID) chips (7), might eliminate the extra time and minimize patient disturbance. These inexpensive radio transmitter chips can be thought of as "talking" labels. They convey the identifying information they carry when close (inches to a few feet) to special interrogating wands. Such identifying chips are used in many industries to track the movement of products from warehouse delivery through cash register checkout. Indeed, Wal-Mart will soon require these chips on all products delivered to its warehouses. The identification badges that open doors when waved in front of a reader also contain these radio frequency identification chips, as do the small theft prevention chips that sales clerks remove from clothing purchases. In theory, 1 wave of a probe could verify that the identifier in the chip attached to the patient's wrist is the same as those attached to the products (for example, medication) without touching the patient or without requiring any special effort by the nurse. Radio frequency identification wristbands and "printers" that will generate, encode, and label them for a particular patient are already on the market, and this technology could replace bar-coded labels in medical applications over time. Some hospitals are already experimenting with them for blood products. The U.S. Food and Drug Administration, however, has some concerns about inter-

ference between wireless physiologic monitors and the radio signal from these chips (8). So, for now, bar coding is the only option for point-of-care verification of dispensing medication. The next few years will probably bring better options.

For years, veterinarians have implanted subcutaneous radio frequency identification chips to locate and track domestic pets and herd animals. Some have proposed implanting such chips in humans, and 1 brave hospital chief information officer has done so publicly (9). Such built-in identifiers would solve the problem of incorrectly identifying a patient once and for all, and would have obvious safety advantages (10). However, privacy advocates have roundly criticized this technology, raising concerns similar to those that ultimately scuttled the universal patient identifier mandated by the Health Insurance Portability and Accountability Act (HIPAA) (11). Fingerprint or other biological patterns (or encrypted versions of the data generated from them) could also be used to identify patients. Thumbprint technology is being used in institutions to verify the identity of users who log on to a computer, and 1 company is marketing a similar product for patient identification. (12) These technologies do not pose a risk for switched identifiers but would require disturbing the patient to a greater extent than do bar-coded wristbands.

The Case, Continued

On routine laboratory review that night, Mr. P.'s resident, Dr. R., noticed that a blood glucose level obtained via fingerstick at the bedside at 9:00 p.m., was recorded at greater than 33.3 mmol/L (>600 mg/dL). This laboratory value was puzzling because Mr. P. had neither a history of diabetes nor symptoms of hyperglycemia and because Dr. R. had not ordered any fingerstick checks. Mr. P.'s intern began to write an order for a sliding-scale insulin regimen, but Dr. R. asked that she first talk with the nurse taking care of Mr. P. to find out why the team had not been notified of this blood glucose level and why it had been checked in the first place.

The nurse, taken aback, stated that she had not checked Mr. P.'s blood glucose level. She agreed to perform a fingerstick check at that time. The value, 5.89 mmol/L (106 mg/dL), further cemented Dr. R.'s suspicion of a mix-up. Dr. R., the patient's resident, stated:

> *What really bothered me about the situation is that it just opened up so many avenues for mistakes, and the mistakes could be really serious medically. For instance, if we had taken that blood sugar at face value, we would have ordered a sliding-scale insulin regimen that would have given this patient over 10 units of insulin, which in a patient of normal blood sugar could have killed him because the blood sugar would drop so low that he could have gone into a coma.*

Ms. F., the charge nurse in the transitional care unit where Mr. P. was admitted, overheard the resident and intern discussing Mr. P.'s high glucose level. Like the physicians, she was concerned about a possible error and started to investigate. She checked Mr. P. and noted that he was wearing the correct wristband. He stated that no one had performed a fingerstick glucose test on him that afternoon. Ms. F. then walked over to the general surgical floor (located next to the transitional care unit) and asked whether they recently had admitted any patients who might have a high glucose level. They identified Mr. D. Ms. F. then went into Mr. D.'s room and checked the identification bracelet. She discovered that Mr. D. was wearing 2 wristbands, the correct one from urgent care, and the incorrect one, which was Mr. P.'s inpatient bracelet.

System-Based Redundancy

This mix-up could have produced dangerous errors of omission and commission. The fact that Mr. D.'s very high glucose level was not entered into his chart could have delayed needed treatment for his diabetes—an error of omission. Because the result did appear in Mr. P.'s chart, he could have been given a bolus of insulin although he was euglycemic—a dangerous error of commission. Neither of these errors occurred because of the many redundant checking and review processes in the system. Indeed, having the right kinds of redundancies is the secret to minimizing errors. Mathematically, we know that if errors occur at a rate of 0.4% at a particular step in a process, we can reduce that error rate to 0.016%—the square of the original error rate—simply by performing that step twice, as long at the repeated step is done independently of the first step. This principle justifies duplicate data entry, such as the "punch and verify" of the card-punch era (3), and the "mod 10" check digit (13), the extra digit in some patient identification numbers that is separated from the other digits by a hyphen. The computer re-computes the check digit according to a standard formula (14) each time a user enters an identification number. It "knows" there has been an entry error when the entered check digit disagrees with the computed digit and requires the user to try again until there is agreement. Check digits uncover the most common typing errors (single, substitutions, and transpositions), and they reduce entry errors by 10-fold or more; therefore, they should be part of every hospital identifier (patient and provider) that must be typed into a computer.

An entire field has developed for detecting and correcting errors through clever application of redundancy, and with enough redundancy, errors may be reduced to any chosen level (15, 16). Computer systems use from 12% to 50% of memory for redundant storage to correct the most common kinds of memory errors. Because modern computer memory is reliable and inexpensive, that tradeoff is easy to justify. In other areas, such as medicine (and the use of double or triple manual checks) or life (air bags, seat

belts, roll bars, speed limits, and asbestos suits such as those worn by racecar drivers), the social and economic costs of these redundancies must be balanced against the increment in safety they provide. There is no "right" balance; to make good choices it is crucial to be explicit about the tradeoffs.

Patient misidentification is an endemic problem in health care institutions. The wrong wristband information is only 1 example. Unconscious patients who arrive at the hospital without identifying information become "John Does" and may not be properly identified for days. Newborn infants are at special risk for being misidentified because they arrive without Social Security number or first name (usually) and cannot say who they are. Mix-ups of Social Security numbers between spouses occur at registration at a rate of 2% to 3% (17). The registration process requires the Social Security numbers of the patient *and* the guarantor, and registration clerks occasionally mis-enter the guaranteeing spouse's Social Security number in the field intended for the patient's Social Security number. Such mix-ups can lead to clinical misidentification when the Social Security number (or part of it) is used to locate the patient's record in the future.

A more important identification error is entering a correct order in the wrong patient's record (paper or computer). This can happen during keyboard entry of patient identification numbers when the operator hits a wrong key (and the identifier does not include a check digit) and during selection of a patient's name from a menu when the cursor slips to the row above or below the intended patient during the mouse click. Mis-entry becomes a special hazard when patients with similar names reside in the same ward or room (18). Such errors in order entry will not be detected by checking the wristband because the identification on the order and the patient will be the same but equally "wrong."

Blood banks use many redundant checks to avoid errors in transfusion. For example, laboratory technologists routinely compare the blood type in the sample with all blood types established by laboratory testing at past visits as far back as records exist. Indeed, the blood bank is often the place where identification errors are first detected. Yet even in blood banking, identification errors occur (19).

Creating a system to ensure fail-safe patient identification is a challenge that requires a thoughtful mix of technologies, provider behaviors, and culture. Overreliance on technological solutions, such as bar coding or perhaps even radio frequency identification, without parallel efforts to institute and enforce appropriate processes of care may only provide the illusion of safety.

Even as we embrace technology-based solutions for important patient safety and quality problems, the physician who knows his or her patient well remains an important defense against medical error. The response of Mr. D.'s resident to the intern: "Talk with the nurse taking care of Mr. P. to find out why the team had not been notified of this blood glucose level, and *why it had been checked in the first place*" [emphasis added], is the appropriate response.

Physicians habitually check new results for consistency against what they already know about the patient, for example, that Mr. P. was not known to be a diabetic, had no symptoms of diabetes, and had no reason to suddenly become hyperglycemic. By instinctively applying Bayesian reasoning, the thoughtful physician identifies suspicious results, as this resident did, and repeats the test for verification. Such consistency checking is part of the physician's thinking process. We cannot overemphasize the importance of this protection to patient safety, and we must guard it carefully as we install new technology and policies. The increasing number of handoffs, for example, from outpatient physician to hospitalist and from admitting resident to the covering resident (driven by residency duty-hours limits), fragments care and could diminish the chance that the physician will really know the patient. This, in turn, compromises the associated protection.

In the current case, Mr. P.'s resident raised the red flag about a possible error and an alert charge nurse with the same instincts followed up on a parallel path. In my institution, physicians complained vigorously about losing the "in lab" signal confirming that their laboratory test orders were actually being processed during a 2-month transition from 1 laboratory system to another. Mr. D.'s physician would have probably noticed and complained about the fact that the glucose result (a fingerstick glucose test) he or she had ordered was not in the chart; however, the nurse who read the results off the glucometer and knew correctly that they were Mr. D.'s probably called them in directly to this physician—yet another link in the chain of events that often characterizes errors in complex organizations.

The Institution's Response

The charge nurse filed an incident report that generated a focused review. The review found that the admitting clerk should have, but failed to, personally confirm that the patient identification wristband had been changed after noticing his mistake; that the registered nurse who checked the fingerstick test should have used 2 identifiers (such as asking the patient his name and checking the wristband) before doing the fingerstick test; and that wristband mix-ups were not unprecedented. The institution subsequently tightened its processes, emphasizing the importance of using 2 identifiers even when the patient has a bar-coded wristband.

Dr. E., medical director of information technology at the institution, stated:

> *The existing policy addresses this [2 patient identifiers requirement] in that the 2 forms of identification [required] before the original wristbands are placed is the critical step here and does need to be reiterated to the people at the frontlines who are placing the*

wristbands when patients are actually next to each other. So this is the critical first step and the downstream issues all relate to educational reminders and training for the staff, as opposed to any changes to the bar codes themselves or in identifiers that are available on the wristband.

Support for the bar-coding system remains strong: Ms. F., the clinical nurse manager, commented:

In general, the system is really a good thing. I think it has dramatically decreased medication errors and it has dramatically decreased patients missing medication doses. [Although] it's not easy to learn and there are a lot of twists in the system that make it difficult for staff nurses . . . and it definitely increases their workload and takes more time away from direct patient care, it's a cost worth paying because of the increased safety to the patient . . . The first thing I recommend is don't install a faulty system, because what will happen is people will figure out a way to work around it. So if your system doesn't work right, or if it's too labor intensive, the staff will find a way to work around.

The physicians also learned a lesson about maintaining an open mind about the possibility of an error involving computerized systems. Dr. R. stated:

The case reinforced the idea that when labs, or some other objective evidence you get from a computer system doesn't quite match with what you are faced with clinically, you as a clinician have to step back and find out how you can put information together. Ask yourself, "Are these not true values?", or is something just not right, and do things need to be rechecked . . . Even in a system that is supposed to work better than previous systems, there are still loopholes, and still things that need to be double-checked.

Dr. E., the institution's director of information technology, broadened the point:

When people discover a discrepancy, it seems to be human nature to believe that there is a problem outside, that the person is wrong, if you will, that it can't possibly be the computer system, but something else. So I think there is, at times, a blind trust that the scanning system must be more accurate than the humans trying to rethink the process. And that's a very interesting phenomenon.

APPLY TECHNOLOGICAL SOLUTIONS WITH CAUTION

Hospital managers tend to accept new systems chosen by their corporate leaders, even when they have their doubts. Although the nurse manager did laud the system in general, she was quick to point out its many negative features, including the fact that it " . . . increases their [nursing's] staff load and takes more time away from patient care." Nursing concerns about bar code systems emerged in another otherwise fawning article as well: "[It] was too slow to respond in emergency conditions" (20).

A direct observational study by Patterson and colleagues (6) goes further, suggesting that some of these systems have serious flaws. For example, when difficulty in achieving intravenous access in 1 patient delayed a critical dose of chemotherapy, the bar-code system refused to accept administration of the medication because the dosing deadline had passed by the time the staff finally placed the line. This example shows a general problem of tight computer control over complicated medical processes. The computer rarely knows all of the relevant facts. Furthermore, at least 1 patient in this study was misidentified with the bar-code system, despite the relatively short observation time of 67 hours. Surprisingly, all of the nurses in Patterson and colleagues' study thought it was faster to type the patient number into the computer than to scan the wristband, even though a major selling point of these systems has been the assumed time savings of scanning. Although meeting specified dosing times has little clinical importance for medications with long half-lives, nurses described dropping important nonmedication-related functions to meet the targets for delivering medication doses at the scheduled times. Scenarios such as these vividly show the potential problems associated with a technological solution that fails to consider all of the realities of clinical care settings.

At least 1 published study shows that bar-code point-of-care systems lower rates of medication errors (21), but the error counts in these studies include minor discrepancies in dispensing times and dosing amounts of limited clinical importance. More important, neither I nor published reviews (22, 23) could find any studies that assessed the nursing time costs, overall cost-effectiveness, patient outcomes, or potential operational side effects, such as a decrease in completion of nonmedicine nursing tasks due to diversion of attention to dispensing medication. Positive identification–dispensing systems, such as bar coding and radio frequency identification chips, have obvious promise, but policymakers need to learn a great deal more before mandating their use—a policy decision recently considered but wisely not taken by JCAHO (24).

Many discussions of technological solutions to the problem of patient identification link bar coding with CPOE, considering them complementary components of a continuum that begins with physician ordering and ends with dispensing the medication. Like bar coding, CPOE has attracted much of the same enthusiasm for mandates (25). Computerizing the prescribing process makes intuitive sense, and the belief that CPOE systems will reduce the high reported numbers of medication errors stokes that enthusiasm. However, it is worth noting that the report of approximately 8000 deaths due to medication errors (26) often cited to justify such mandates actually describes "ac-

cidental deaths due to drugs" (International Classification of Diseases codes E850 to 858, and X40 to 49, which include accidental overdose), most of which occur in young and middle-aged adults with no preexisting diseases reported on their death certificates (27). Eighty-two percent of these deaths are associated with narcotic overdoses (34% methadone and 48% other narcotics) (28), and the remainder are associated with overdoses of other psychoactive drugs. In some instances, the person who died was taking someone else's medications. These are not deaths due to errors in prescription writing, and it is misleading to use them to help justify the investment in CPOE.

It is not just a potentially overstated risk for medication errors that should give us pause before mandating CPOE implementation. A study by Koppel and colleagues (29), which indicated that errors could be induced and prevented by CPOE, raised other questions. Enthusiasts (30–32) criticized Koppel and colleagues for examining only 1 CPOE system, although it is one that has been widely used over a long period. However, Ash and colleagues (33) reported similar problems at another institution; Nebeker and colleagues (34) and Horsky and colleagues (35) point out other problems with CPOE; Han and colleagues (36) reported an increase in mortality rates associated with the installation of a CPOE system; and Hicks and colleagues (37), in a study of more than 500 institutions, found that hospitals with CPOE did not have lower error rates than hospitals that used nurse or pharmacist order entry. In addition, a recent report (38) observed that although all of the important (moderate to severe) errors on handwritten prescriptions were caught before they affected the patient, some similar gaffes on computer-written prescriptions were not because the traditional layers of human cross-checks were less intense. Human checking processes are formidable and should not be dropped automatically simply because the computer is helping with the work.

Reminders to physicians delivered during CPOE do reduce errors of omission and commission (39, 40). However, we do not yet know how important the *physician* entry is to achieving the benefits observed so far, because the computer can apply the same checking logic to orders entered by pharmacists and nurses and deliver reminders to them. Of interest, computer automation of nurse standing orders did produce more inpatient immunizations among eligible patients than reminders with the same purpose delivered to physicians during CPOE (41).

The point is that CPOE is not a magic bullet. We have ample evidence that it improves the care process (42) but as yet have no evidence that it improves patient outcomes (43, 44). This is not to argue against the use of CPOE; it has worked very well in my institution for more than 15 years (45). It offers clear benefits to institutional efficiency and communication (46), with speedier order completion and treatment delivery and opportunities to inform physicians about the benefit, dangers, and costs of their orders. In this way, it shapes physicians' decisions. There are good reasons for institutions to adopt CPOE systems, but they should do so at their own pace and volition. The available evidence does not justify crash programs, mandates, or deadlines. Researchers should be studying the strengths *and* the weaknesses of all these systems to improve them. Furthermore, we should all remember that simple human processes and innovations provide large opportunities for improvement, especially when thoughtfully harmonized with robust technological solutions. Finally, even in a computerized environment, the physician who knows his or her patient well is ultimately the best defense against many kinds of system errors.

Questions and answers from the conference are listed in the Appendix (available at www.annals.org).

From Regenstrief Institute, Indianapolis, Indiana.

Grant Support: This work was supported by grant G08 LM008232 from the National Library of Medicine and grant 510040784 from the Indiana Twenty-First Century Research and Technology Fund. Funding for the Quality Grand Rounds series is supported by the California HealthCare Foundation as part of its Quality Initiative.

Potential Financial Conflicts of Interest: None disclosed.

Requests for Single Reprints: Clement J. McDonald, MD, Regenstrief Institute, 1050 Wishard Boulevard, Indianapolis, IN 46202; e-mail, cmcdonald@regenstrief.org.

References

1. **Pavlidis T, Swartz J, Wang YP.** Fundamentals of bar code information theory. Computer. 1990;April:74-86.
2. **Grudin JT.** Error patterns in novice and skilled transcription typing. In: Cooper WE ed. Cognitive Aspects of Skilled Typewriting. New York: Springer-Verlag; 2003:121-43.
3. **Klemmer ET, Lockhead GR.** Productivity and error in two keying tasks: a field study. J Appl Psych. 1962;46:401-8.
4. **Joint Commission on Accreditation of Healthcare Organizations.** 2005 Hospitals' National Patient Safety Goals Goal: Improve the Accuracy of Patient Identification. Accessed at www.jacho.org/accredited+organizations/patient+safety/05+npsg/05_npsg_hap.htm on 31 October 2005.
5. **Rosenthal MM.** Check the wristband. AHRQ Web Morbidity & Mortality. July 2003. Accessed at www.webmm.ahrq.gov on 31 October 2005.
6. **Patterson ES, Cook RI, Render ML.** Improving patient safety by identifying side effects from introducing bar coding in medication administration. J Am Med Inform Assoc. 2002;9:540-53. [PMID: 12223506]
7. **Want R.** The magic of RFID. ACM Queue. 2004;2(7). Accessed at http://portal.acm.org/citation.cfm?id=1035619 on 31 October 2005.
8. **Brewin B.** FDA mandates bar codes on drugs used in hospitals. Comp World. 2004; 26 Feb. Accessed atwww.computerworld.com/printthis/2004/0, 4814, 90546, 00.html on 31 October 2005.
9. **Halamka J.** Straight from the shoulder. N Engl J Med. 2005;353:331-3. [PMID: 16049206]
10. **Stein R.** Implantable medical ID approved by FDA. Washington Post. 2004; 14 Oct:A01.
11. Health Insurance Portability and Accountability Act of 1996. Accessed at www.hhs.gov/ocr/hipaa on 31 October 2005. Centers for Medicare & Medicaid Services, HHS. HIPAA administrative simplification: standard unique health identifier for health care providers. Final rule. Fed Regist 2004;69:3433-68.
12. Ultra-scan for health care. Accessed at www.ultra-scan.com/ on 31 October 2005.
13. **Wagner NR, Putter PS.** Error detecting decimal digits. Communications of

the ACM.1989;32:106-10.
14. Credit card validation—check digits. Accessed at www.beachnet.com/~hstiles/cardtype.html on 31October 2005.
15. **Gallian JA.** Error detection methods. ACM Computing Surveys. 1996;28:504-17.
16. **MacKay DJC.** Good error-correcting codes based on very sparse matrices. IEEE Transactions on Information Theory. 1999;45:399-431.
17. **Grannis SJ, Overhage JM, McDonald CJ.** Analysis of identifier performance using a deterministic linkage algorithm. Proc AMIA Symp. 2002:305-9. [PMID: 12463836]
18. **Lee AC, Leung M, So KT.** Managing patients with identical names in the same ward. Int J Health Care Qual Assur Inc Leadersh Health Serv. 2005;18:15-23. [PMID: 15819121]
19. **Linden JV, Wagner K, Voytovich AE, Sheehan J.** Transfusion errors in New York State: an analysis of 10 years' experience. Transfusion. 2000;40:1207-13. [PMID: 11061857]
20. **Wright AA, Katz IT.** Bar coding for patient safety. N Engl J Med. 2005;353:329-31. [PMID: 16049205]
21. **Larrabee S, Brown MM.** Recognizing the institutional benefits of bar-code point-of-care technology. Jt Comm J Qual Saf. 2003;29:345-53. [PMID: 12856556]
22. **Oren E, Shaffer ER, Guglielmo BJ.** Impact of emerging technologies on medication errors and adverse drug events. Am J Health Syst Pharm. 2003;60:1447-58. [PMID: 12892029]
23. **Wald H, Shojania KG.** Bar coding (Chapter 43.1). In: Shojania KG, Duncan BW, McDonald KM, Wachter RM, eds. Making Health Care Safer: A Critical Analysis of Patient Safety Practices. Evidence Report/Technology Assessment. Number 43. AHRQ publication no. 01-E058. July 2001. Agency for Healthcare Research and Quality, Rockville, MD. Accessed at www.ahrq.gov/clinic/ptsafety/ on 31 October 2005.
24. **Broder C.** JCAHO drops bar-coding requirement, but could revisit issue. Accessed at www.iHealthBeat.org on 31 October 2005.
25. **Doolan DF, Bates DW.** Computerized physician order entry systems in hospitals: mandates and incentives. Health Aff (Millwood). 2002;21:180-8. [PMID: 12117128]
26. **Phillips DP, Christenfeld N, Glynn LM.** Increase in US medication-error deaths between 1983 and 1993. Lancet. 1998;351:634-44. [PMID: 9500322]
27. **Rooney C.** Increase in US medication-error deaths [Letter]. Lancet. 1998;351:1656-7; author reply 1657. [PMID: 9620737]
28. Increase in poisoning deaths caused by non-illicit drugs—Utah, 1991-2003. MMWR Morb Mortal Wkly Rep. 2005:33-6. [PMID: 1560016]
29. **Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR, Kimmel SE, et al.** Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005;293:1197-203. [PMID: 15755942]
30. **Keillor A, Morgenstern D.** Computerized physician order entry systems and medication errors [Letter]. JAMA. 2005:294:178; author reply 180-1. [PMID: 16014586]
31. **Bierstock S, Kanig SP, Marcus E.** Computerized physician order entry systems and medication errors [Letter]. JAMA. 2005;294:178-9; author reply 180-1. [PMID 16014585]
32. **Levick D, Lukens H.** Computerized physician order entry systems and medication errors [Letter]. JAMA. 2005;294:179-80. [PMID: 16014587]
33. **Ash JS, Berg M, Coiera E.** Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. J Am Med Inform Assoc. 2004;11:104-12. [PMID: 14633936]
34. **Nebeker JR, Hoffman JM, Weir CR, Bennett CL, Hurdle JF.** High rates of adverse drug events in a highly computerized hospital. Arch Intern Med. 2005;165:1111-6. [PMID: 15911723]
35. **Horsky J, Kuperman GJ, Patel VL.** Comprehensive analysis of a medication dosing error related to CPOE. J Am Med Inform Assoc. 2005;12:377-82. [PMID: 15802485]
36. **Han YY, Carcillo JA, Venkataraman ST, Clark RS, Watson RS, Nguyen TC, et al.** Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics. 2005;116:1506-12. [PMID: 16322178]
37. **Hicks RW, Santell JP, Cousins DD, Williams RL.** MedMarx 5th Anniversary Data Report: A Chartbook of 2003 Findings and Trends 1999-2003. Rockville, MD: USP Center for the Advancement of Patient Safety; 2004.
38. **Shulman R, Singer M, Goldstone J, Bellingan G.** Medication errors: a prospective cohort study of hand-written and computerised physician order entry in the intensive care unit. Crit Care. 2005;9:R516-21. [PMID: 16277713]
39. **Dexter PR, Perkins S, Overhage JM, Maharry K, Kohler RB, McDonald CJ.** A computerized reminder system to increase the use of preventive care for hospitalized patients. N Engl J Med. 2001;345:965-70. [PMID: 11575289]
40. **Potts AL, Barr FE, Gregory DF, Wright L, Patel NR.** Computerized physician order entry and medication errors in a pediatric critical care unit. Pediatrics. 2004;113:59-63. [PMID: 14702449]
41. **Dexter PR, Perkins SM, Maharry KS, Jones K, McDonald CJ.** Inpatient computer-based standing orders vs physician reminders to increase influenza and pneumococcal vaccination rates: a randomized trial. JAMA. 2004;292:2366-71. [PMID: 15547164]
42. **Bates DW.** Using information technology to reduce rates of medication errors in hospitals. BMJ. 2000;320:788-91. [PMID: 10720369]
43. **Garg AX, Adhikari NK, McDonald H, Rosas-Arellano MP, Devereaux PJ, Beyene J, et al.** Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review. JAMA. 2005;293:1223-38. [PMID: 15755945]
44. **Koppel R, Localio AR, Cohen A, Strom BL.** Neither panacea nor black box: responding to three *Journal of Biomedical Informatics* papers on computerized physician order entry systems. J Biomed Inform. 2005;38:267-9. [PMID: 15993652]
45. **Tierney WM, Miller ME, Overhage JM, McDonald CJ.** Physician inpatient order writing on microcomputer workstations. Effects on resource utilization. JAMA. 1993;269:379-83. [PMID: 8418345]
46. **McDonald CJ, Overhage JM, Mamlin BW, Dexter PD, Tierney WM.** Physicians, information technology, and health care systems: a journey, not a destination [Editorial]. J Am Med Inform Assoc. 2004;11:121-4. [PMID: 15027445]

47. **Lundsgaarde HP, Fischer PJ, Steele DJ.** Human problems in computerized medicine. Publications in Anthropology 13. Lawrence, KS: University of Kansas; 1981.
48. **McDonald CJ, Overhage JM, Barnes M, Schadow G, Blevins L, Dexter PR, et al.** The Indiana network for patient care: a working local health information infrastructure. An example of a working infrastructure collaboration that linmks data from five health systems and hundreds of millions of entries. Health Aff (Millwood) 2005; 24:1214-20. [PMID: 16162565]
49. **McDonald CJ.** Observation and Opinions: Medical records on a credit card. MD Computing. 1986;3:8-9.

Appendix: Questions and Answers from the Conference

Robert M. Wachter, MD, Moderator: Talk about the tension between redundancy and workarounds. You can build in more and more redundancy, but until the technology gets really good, it may take longer to deliver care. For example, nurse managers will tell you that it takes more time to scan the bar codes.

Clement J. McDonald, MD, Discussant: Technologic replacements for existing human processes always tend to disappoint in their early stages because they do not include subtle but important features of the processes they try to replace. The paper charts that were replaced by one of the earliest medical record systems mixed the handwritten notes of all clinical professionals in one time sequence (47). Notes of physician, social worker, nurses, and pharmacist were intermixed. In the paper version, a user could easily find and follow the thread of one author's, or kind of author's, notes without reading all of the text because the handwriting style, note organization, and ink color provided the visual cues needed to follow the thread. In the computer version of this system, all of these navigational cues were lost, because the text was generated by the computer through a user's menu selection and the differences in note structure, handwriting, and ink color disappeared. Progress, maybe, but also a new inefficiency for providers and an opportunity for error. Today, this problem does not occur because the computerized medical records do usually label and sort notes by the name and type of author.

Dr. Wachter: Explain a little bit about the Indianapolis experiment.

Dr. McDonald: The 5 major hospital systems in Indianapolis—a total of 15 separate hospitals—have joined the Indianapolis Network for Patient Care (INPC) to share much of their electronic clinical data (for example, hospital dictation, laboratory, pathology, radiology, and cardiology reports) with each other for limited clinical care, research, and public health purposes (48). The INPC is responsible for standardizing the data from each of the participating institutions so that information about a given patient from many institutions can be presented as a unified whole as though they came from a single institution. Physicians in Indianapolis emergency departments have been using INPC data to care for emergency patients (450 000 per year) for more than 4 years. When a patient checks into an emergency room (ER), the ER registration system sends a message to INPC, which in response delivers a 1 to 2 page printed précis of the patient's record to the ER registrar's printer for placement on the patient's chart. The INPC also opens access to that patient's full INPC record to ER physicians caring for the patient in the ER. Those physicians can then review the patient's full INPC medical record online for 24 hours. The INPC institutions are implementing a similar approach for inpatients as well, and are working on mechanisms for granting office practitioners access under appropriate circumstances.

Dr. Wachter: One has to assume that at some point you need a system where a patient could go someplace and have their electrocardiogram accessed from across the town or their hospitalization records from across the country. There are privacy tensions there. Do you think there should be a universal record, like the record of your credit card transactions? Or is this something that a patient should carry with them on a card or an implantable chip?

Dr. McDonald: There is no experience in the industry with the sharing of clinical data on a national scale, and the privacy risks associated with such national systems are daunting. Historically such national systems stir political oppositions because they conjure thoughts of Big Brother. Most care is delivered at the community level, and that is where clinical data sharing will have the most advantage. With the development of robust community-based systems, patients might be able to request that their records be forwarded to another community via very safe mechanisms. But the country needs much more experience with community-based systems before moving to this next step.

The idea of a medical record on a patient-carried "smart card" is an old one (49), but it is not a viable stand-alone solution to the problem of medical record data storage, because patients lose their cards, and because many kinds of clinical results—radiology reports, referral notes, laboratory reports—are produced after the patient and the card have left the medical office. Any card-based solution requires some form of centralized and standardized medical data storage from which the patient could download any new results and create new copies of his or her medical record to replace lost or damaged ones. A patient-carried card system could complement a community-based system. The latter would provide the source of clinical data for updating and replacing card content as necessary, and the card would provide a very simple and safe method for providing access to the patient's medical record when traveling outside his or her home community.