Electronic Health Records and Patient Safety

19

Michael S. Victoroff

Pitfalls and Pearls

- When computers are embedded in high-performance systems, they fail just like people do, in sometimes simple but more often complicated ways.
- Blaming adverse events on "computer error" is like blaming them on "human error": These labels have no value in causation or remedy analysis.
- A starting point for the risk analysis of a given system is to look at what it is supposed to do when it works right, and anticipate what will happen when it works wrong.
- A lot of health information technology is designed with almost comical inattention to user experience. Clumsy interfaces are responsible for a large proportion of EHR-related errors. Ironically, users often are the safeguards that prevent errors and injuries from health information technology, rather than the other way around.
- Many design flaws ubiquitous among EHRs stem from their legacy as "cash registers" that create documentation for charge capture. Unfortunately, this business case continues to distort the design of systems, making clinical value a secondary goal.
- There is growing interest in systematically capturing reports of adverse events associated with the use of health information technology. These efforts will eventually produce theories about causes and patterns of EHR-related errors, design considerations, training issues, usability, interactions with users and systems, and other insights that will be useful in building a better generation of products.
- The single greatest concern about current tools for facilitating electronic documentation is their propensity for generating inaccurate records.

M.S. Victoroff, MD
Department of Patient Safety and Risk Management, COPIC Insurance Cos,
5195 E Weaver Dr, Denver, CO 80121, USA
e-mail: michael.victoroff@ucdenver.edu

P.F. Stahel, C. Mauffrey (eds.), *Patient Safety in Surgery*,
DOI 10.1007/978-1-4471-4369-7_19, © Springer-Verlag London 2014

Outline of the Problem

For every function, there is an equal and opposite malfunction.

Health information technology (HIT) has two faces with respect to patient safety. One regards ways HIT solutions can potentially improve almost every aspect of the patient experience, certainly including safety, but also convenience, timeliness, appropriateness, effectiveness and cost of care, as well as furthering research. A growing body of research suggests HIT can improve clinical quality [1–6] and patient safety [7]. These benefits will grow exponentially as HIT proliferates. Just as aviation analogies have been valuable to students of healthcare safety, an analogy with the contribution of technology to aviation safety is perfectly apt. Bright days are ahead.

The other face of HIT is darker. It is a source of errors, injuries, impaired clinician productivity, dilution of effort and diversion of resources from pressing needs, and high costs—now and forthcoming [8]. It is not exaggerating to call the impact of HIT on healthcare prodigious.

This chapter focuses more on risk than benefits of HIT. Although the tone of what follows is cautionary, this imbalance must not be read as a polemic on the evils of automation. On the contrary, the author is an evangelist for EHRs, a former EHR developer and keen advocate of creative information technology. The infancy of any science entails missteps and embarrassments, and we are still in the early days of medical informatics. The pattern in the history of technology is net benefit to human well-being, and HIT will be in the ranks of mankind's most successful inventions.

That said, Newton's Law of Computing states, "*For every function*, *there is an equal and opposite malfunction*." Any combination of hardware, software and humans will produce an undesired result at some point. While the intent of technology is to improve the performance of tasks, information systems in healthcare must be thought of as *medical devices*, and should be developed and tested with the same caution as pacemakers, surgical tools or laboratory equipment.

What Is an EHR?

For this discussion, "Electronic Health Record" (EHR) is the current label for a category of health information technology that automates **clinical documentation**, the transmission of **orders**, **results and messages** and the delivery of **alerts**, **prompts**, **reminders** and other '**clinical decision support**' content to users at the time of care.

There are other ways to define EHRs, and there has been nit-picking over differences between EHRs and EMRs ("Electronic Medical Records") and other labels out of popular favor such as "Computerized Patient Records" "Electronic Patient Records" and even "Personal Health Records" (which are quite different). These nuances are responsible for some of the difficulty practitioners face when shopping for systems. When the American Recovery and Reinvestment Act (ARRA, 2009) [9] began offering subsidies to providers for installing EHRs, it had to define exactly what an EHR was for purposes of reimbursement. But, the discussion in this chapter does not depend on any particular definition and none will be provided beyond that above.

EHRs are merely a subset of a wide range of health information technology that this discussion will not address. Some tangential topics that are seriously important to patients and providers are going to receive less attention than they deserve.

In particular, this chapter largely avoids hazards falling under the rubrics of privacy and security. Although patients can suffer grievous harm from the disclosure of their personal information (and this risk does occupy a great amount of attention in the fields of technology, law and public policy), the dangers contemplated in this discussion are the most tangible kinds, such as bodily harm, disability and death.

Also ignored is much to do with the safety and regulation of medical devices like robots, diagnostic equipment and methods, radiological systems, implanted devices and many other varieties containing software that are not properly classified as "Electronic Health Records." The question whether (or which) software products should be considered "medical devices" for legal and regulatory purposes is currently an active focus of discussions between the U.S. Food and Drug Administration and the vendor community. There is no doubt that the FDA currently has legal authority to regulate software used for healthcare purposes. In the most general sense, the agency foresees software falling into three categories [10]:

1. Subject to regulatory review and standards applicable to medical devices
2. Some form of regulatory oversight is appropriate but not to the same degree as traditional medical devices
3. Regulatory review is not envisioned

What Is Safety?

No medical procedure, device or remedy is safe. For the purposes of this chapter, safety will be understood as the likelihood of a product or system performing as intended, without causing undue or unanticipated risk or harm. Patient safety is entwined with other problems like efficiency, effectiveness, cost and legal liability. There is no effort made here to keep them rigorously separate, although the focus of the current discussion is chiefly preventable risk and harm.

Obstacles

Several obstacles confront any attempt to analyze the impact of Electronic Health Records upon patient safety. First is scarcity of case material. Although EHR users are becoming familiar with a range of hazards, design flaws, malfunctions, inefficiencies and other shortcomings, and increasingly able to share anecdotes about near misses and injuries attributable to EHRs, there are currently few repositories of standardized reports about EHR-related safety events that have enough depth for comparative research. This chapter will touch upon some efforts to standardize reporting and develop a reliable epidemiology of EHR-associated errors.

Second, EHR-related events tend to be complex. Interpreting unanticipated effects typically requires input from both involved users and IT experts. Analyzing the root cause of an HIT event often blossoms into a justifiable exercise in onion-peeling. For example, a seemingly straightforward blunder—ordering the wrong drug through a dropdown-list-off-by-one selection error—should not naively be laid off to "user error." Factors like the font size of the list, the stability of the menu, the dimensions of the selection zone, spacing between items, number of items displayed, number of characters in their names, color, margins, user familiarity with the system, lighting and location of the terminal, sensitivity of the pointing device, and similar usability factors can play critical roles in error rates. As the aviation industry has learned, when "pilot error" falls into a pattern, someone needs to ask whether something in the cockpit might be inducing pilots to make mistakes.

Third, like everything in the field of patient safety, data gathering and review take place under the shadow of potential legal liability. Ironically, misgivings about reporting are a barrier to safety research. This problem is amplified when technology is involved because product liability potentially raises the stakes for damages into a higher range than ordinary malpractice. This risk (and the lack of legal sanctuaries for professional discussion) inhibits developers and vendors from forthrightly addressing (or even sometimes acknowledging) flaws in their own systems, or participating in reporting networks. For this reason, investigators with the best intentions wishing to study HIT hazards face a perverse inhibition. Since public analysis generates discoverable records, some see open discussion as counterproductive because it could draw roadmaps for litigators. On the other hand, from the standpoint of users and patients, there is not enough dialog about hazards of HIT products, some of which exhibit audaciously poor design.

At this writing, relatively few legal claims for patient injuries have been directly attributed to HIT, even when sophisticated analysis points to technology as a contributing factor. But, this may change, as electronic systems play ever larger roles in the way care is provided.

Risk Assessment

What follows is a catalog of safety risks to patients that can be induced by EHRs common in the U.S. today. There is no reason why EHRs in other countries would not be susceptible to the same vulnerabilities. Not every risk applies to every system, because of differences in feature sets, configuration, implementation and myriad other factors that are fluid. Vendors and products are not identified. And, there is no attempt to create a hierarchy of severity. It is well known that trivial errors can give rise to serious harms, and catastrophic failures can be intercepted without causing any harm. Since the stream of reports and issues grows daily, it is impossible to create anything like a comprehensive survey or even a "top ten" list of dangers to watch out for. In fact, every organization's "top ten" EHR risks should differ from the organization's next door. The message for CEOs, CIOs, CMIOs, CNIOs, Safety and Privacy Officers and the rest of the army of Os responsible for EHRs is, "If you are complacent that you've solved the top ten problems in your organization this year, you're going to get blindsided by the eleventh."

There are two ways to build a list of EHR risks: (1) Predicting them from insight into system functions, and (2) by collecting actual event reports.

"Capability Is Vulnerability"

To predict potential hazards of a technology, a good start can be made by examining what its functions are when they operate correctly and imagine them operating incorrectly. The formal exercise of *risk analysis* entails a 360-degree survey of a healthcare provider's information environment and itemizing known and potential hazards to the "confidentiality, integrity and availability" of electronically stored Protected Health Information (Box 19.1) [11].

Box 19.1
Confidentiality: PHI is accessible only by authorized people and processes
Integrity: PHI is not altered or destroyed in an unauthorized manner
Availability: PHI can be accessed as needed by an authorized person

This process is required under the Security Rule which is a component of the Health Insurance Portability and Availability Act of 1996 (HIPAA) [12]. A careful risk assessment will evaluate *vulnerabilities*, *threats*, *risks and impacts* (Box 19.2) [13].

Box 19.2

Vulnerability—A weakness that provides an opening for a harmful event.

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Threat—Something that can cause a harmful event.

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Risk—The likelihood of a harmful event happening.

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Impact—The kind of effect a harmful event would have on people, organizations and property (e.g., legal, operational, reputational, business or financial).

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Parallel with risk assessment is the task of enumerating the *safeguards* in place—and safeguards needed—to defend against vulnerabilities. Safeguards fall into 3 general domains (Box 19.3).

Box 19.3

1. **Physical safeguards**—Locks, doors, keys, fences, ID badges, signs, emergency power supplies, receptionists, guards, etc.
2. **Technical safeguards**—Anti-virus, encryption, passwords, firewalls, software updates, access control lists, offsite backup, etc.
3. **Administrative safeguards**—Training, policies, audits, IT support, credentialing, background checks, disaster plan, etc.

A detailed discussion of information technology risk assessment methods, standards and guidelines is beyond the scope of this chapter. Many resources are available to technology professionals, administrators and end users; a few are listed in Box 19.4.

Box 19.4
Office of the National Coordinator for Health Information Technology (ONC)
- www.HealthIT.gov
- Mobile devices: www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device
- Security and risk auditing: www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- Meaningful Use Security and Privacy Requirements: www.hrsa.gov/healthit/toolbox/HIVAIDSCaretoolbox/SecurityAndPrivacyIssues/howdoicomplywitmu.html

Office for Civil Rights
- Health Information Privacy/HIPAA resources: www.hhs.gov/ocr/privacy/index.html
- Basics of Risk Analysis and Risk Management: www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf
- Guidance on Risk Analysis Under the HIPAA Security Rule: www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

The National Institute of Standards and Technology
- A wealth of information available for download about security and the risk auditing process: http://csrc.nist.gov/
- Guide for Conducting Risk Assessments http://www.nist.gov/manuscript-publication-search.cfm?pub_id=912091

The Agency for Healthcare Research and Quality (AHRQ)
- Standardized reporting formats for patient safety events, including HIT-specific events
- Software and device reporting form: https://www.psoppc.org/c/document_library/get_file?uuid=75912503–7bd1–4e99-a678–5dbb70008e95&groupId=10218
- Hazard Manager: http://healthit.ahrq.gov/sites/default/files/docs/citation/HealthITHazardManagerFinalReport.pdf

Capturing Event Reports

A second way to identify risks is to analyze adverse events that have actually occurred. Among the challenges to research on EHR safety is the lack of a standard taxonomy for classifying types of hazards and adverse events. A number of researchers are actively interested in creating theories, or at least a categorization schema, that would allow the sorting and classification of case reports. One model devised by Sittig and Singh [14] suggests an 8-dimensional "socio-technical" framework for evaluating events involving HIT systems (Box 19.5).

Box 19.5. Sociotechnical Framework
- Hardware and software computing infrastructure
- Clinical content
- The human computer interface
- People
- Workflow and communication
- Internal organizational features (e.g., policies, procedures, and culture)
- External rules and regulations
- Measurement and monitoring

The ECRI Institute [15] used another taxonomy devised by Magrabi et al. [16]. to help analyze over 3,000 reports of HIT-related patient safety events in Pennsylvania occurring 2004–2012.

Under the authority of the Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act) [17] the Agency for Healthcare Research and Quality (AHRQ) coordinates the development of a set of Common Formats for reporting patient safety events to Patient Safety Organizations (PSOs) [18]. One set of CF templates is dedicated to HIT-related events. Using these formats, AHRQ is building a repository of reports from PSOs. Data on EHR-related safety events are also being collected in various formats by the Canadian Medical Protective Association (CMPA), the Physician Insurers Association of America (PIAA), COPIC, Inc. (whose taxonomy has been used in research at the University of Colorado [19]) and other quality and safety organizations. However, as yet there is no central repository where researchers can access a full spectrum of cases.

Limitations of the Current Practice

Medical Documentation Systems

The core of a medical information system is the documentation of physician-patient encounters. Against all intuition, it is difficult to quantify the value of the medical chart strictly in terms of safety. Of course, there are innumerable instances where missing information at the point of care resulted in preventable harm [20]. Malpractice archives (and cemeteries) are full of stories that would have been different, "If only the doctor had known . . ." It would be absurd to deny the importance of records in the process of care. But, the convoluted data gathering rituals that support medical practice generate such redundancy that they function as superior error-trapping mechanisms, so missing information does less harm than might be expected.

Providers are accustomed to untrustworthy information; they are trained to expect it and develop portfolios of techniques to compensate for never having a complete data set for the patient before them. The "Oslerian conceit" is that a skillful practitioner should be able to extract a "complete history" from a patient during the course of an oral interview. The fallacy of this notion should be obvious in the

modern world, in which patients may have only vague and limited technical information about their own care; or whose care has been so extensive that memory is next to useless. Today's medical graduates are accustomed to looking for records to orient themselves to a patient's situation, and using the interview primarily to refine it. But, the fallacy of the latter approach is that the quality and completeness of available documents can be very weak.

Data Loss

Despite these practical shortcomings, it is obvious that better information at the point of care supports better care altogether. Therefore, the definitive risk to the "confidentiality, integrity and availability of electronically stored information" is that of losing it. This can be accomplished in countless ways, of which the simplest is physical destruction. Of course, paper records are vulnerable to the same risk. The great advantage of electronic information is the ease of duplicating it and keeping authentic copies in several locations. Unfortunately, cases still regularly surface from organizations that failed to make adequate provisions for data backup. This is essentially inexcusable in today's technology-dependent world. Both local and offsite copies of critical information are inexpensive and easy to create, and should be cardinal elements of any I.T. infrastructure.

Patients have a right to their records. In one instance, a patient moving out of town filed a state medical board complaint against a doctor who could not give her a copy of her chart. The office EHR had suffered a hard drive failure and some records were permanently lost. The patient argued that this fell below an acceptable standard of practice.

Data Dropped in Transition

The implementation phase of a new electronic system is a time of high risk for data. At least one appellate court case addressed an injury caused when key information from a legacy paper chart (manually summarized) did not make it into the electronic version of the patient record, and necessary treatment was delayed. The court confirmed provider liability, concluding that an organization installing an EHR is responsible to "implement a reasonable procedure during the transition phase" to ensure that data isn't lost [21].

Data Conversion

Transitions in healthcare are not occasional but routine. Patients establish themselves in practices, then move, graduate, get married, change jobs, change insurance, change doctors, retire. Likewise doctors, hospitals and systems are in continuous flux. Today, 25 % of EHRs are being installed to replace a prior EHR, and the pace of this churning will increase over time. Unfortunately, the internal database structures and definitions of each EHR are different (despite serious efforts to create data exchange standards). This makes mass conversion of a dataset from one EHR to another extremely difficult and highly risky from the standpoint of data integrity. The same problem applies to data interchange between institutions. The process of **mapping** information from one system to another is fraught with problems, because no two systems define or store the same data in the same way. A single mis-matched field out of many thousands can set an error in motion in patient care.

Data Deletion

Data loss can occur during normal operations through operator error, routine purging and archiving, import/export and file updating processes, as well as numerous types of software malfunctions. Many systems have provisions for restoring deleted data, but there are instances where retrieved files are older or incomplete versions of the ones lost. The author was involved in a disaster in which 6 months of patient records in a large orthopedic practice were wiped away when a technician reconfigured a drive without knowing what it contained.

Data Corruption

In another case, an EHR software version upgrade corrupted several thousand patient charts in a small practice. The data on individuals apparently remained, but was scrambled into records under different names, and the vendor apparently was not able to find a way to undo the damage. This case was complicated by the fact that the mixup was not recognized until several rounds of backups had been made, so the backups were corrupt, too. (A pre-update copy of the data was not stored.) Although the vendor accepted responsibility for the costs of installing a new system, it did not agree to any liability for the cost of re-creating several thousand charts, or—more concerning to the practice—liability for any consequential injury to patients that might arise from lost information.

Disaster, Malice and Coffee

Among infinite other causes of data loss are power surges and blackouts, flood, fire, storm, untrained users, misplaced devices, mechanical failures, deliberate sabotage by disgruntled employees, hacking, cyber terrorism and every kind of accident. During hurricane Katrina, millions of patient records in New Orleans (paper and electrical) were lost to water damage. Defenses against record loss include physical safeguards (locks, fire extinguishers), technical safeguards (backup, more backup) and administrative safeguards (planning, training).

Cloud Computing

Cloud computing is an arrangement in which patient data (and sometimes the programs that run the data) are kept on secure servers in a remote location, allowing users to access them through a communications network (usually the Internet). This avoids many risks of locally stored data, and reduces expenses of local administration, security, backup, etc. However, if network access becomes unavailable (for example in a storm), or if connectivity fails for technical reasons, all remote data is out of reach.

Data Displacement

Rather than actually being lost, information may simply not be found. Since there is no standard architecture for EHRs, the location of specific types of information is left to the vendor, designer, configurator, and individual user. In one effort to audit about a million patient records with the goal of simply tabulating the occurrence of flu shots, reviewers found they needed to inspect at least 27 different locations in the chart to say confidently whether a shot had been received (Wilson Pace, MD (2010), personal communication). The information might be in the immunization log, or a medication administration record, a nurse's note, a pharmacy order, or perhaps in the medical assistant's comment, "*Patient states flu shot at pharmacy last week*."

If this is a problem with flu shots, how much is the ante raised for items like anticoagulants, near fatal drug reactions, rare diseases, and so on? Many patients have a powerful illusion that EHRs give providers access to "everything" (including things that may not be there at all). But, actual users know that having a giant repository of data is not the same thing as "access." Our ability to collect information far exceeds our ability to retrieve it.

Data Sequestration

The law in its wisdom can mandate things that are technically impossible. With the best intentions, HIPAA allows patients to restrict disclosure of specific portions of their medical records because of sensitivity or other reasons. Some state laws (which generally grant parents the right to view their children's protected health information), nevertheless forbid parental access to some types of minors' information (e.g., treatment of sexually transmitted disease, pregnancy, drug abuse, psychiatric conditions). In spirit, this notion is laudable. However, not only is there currently no technology that can automatically dissect out the bits of information deemed "sensitive," but the very concept of redacting selected threads of data from an integrated body of information without touching the remainder may be a physical impossibility, like taking the flour out of a cake.

From a safety standpoint, even if reliable redaction can committed upon a medical chart, clinicians need to be concerned about mistakes they can make if they rely on the doctored version—particularly if there is no indication that vital facts have been withheld. Sequestration presents particular safety challenges in the fields of—and to clinicians interacting with patients in—behavioral health and addiction medicine. Many drugs and conditions managed by behavioral health specialists have important ramifications for neurology, cardiology, endocrinology, nephrology, and other specialties, which can be missed or misinterpreted if not disclosed.

Data Breach

Potentially more injurious to patients than the loss of their information is the unintended disclosure of it. This can occur by accident (e.g., lost laptops), carelessness (e.g., online postings) or through active intrusion by hackers. Health facilities have become rewarding targets for cyber criminals. At this writing, healthcare data is the chief source of stolen identities in the U.S., as well as an ocean of fraud. Stolen insurance cards allow imposters to obtain services under false identities. Stolen physician credentials can be used to forge prescriptions. Most lucrative of all, patient identities and physician billing information can be combined to submit fraudulent charges to payers, a multi-billion dollar enterprise in which organized crime is deeply invested.

The vulnerability of healthcare operations to cyber-crime is partly due to the great amount of confidential data it distributes across numerous locations, the high volume of healthcare transactions adjudicated without human intervention, and a lesser degree of security-mindedness in the healthcare workforce than other industries that handle confidential information. But, the real dilemma is that the ethical obligations of patient care and safety take priority over privacy when the two conflict. For this reason, privacy and confidentiality are not perfectible goals for healthcare institutions.

Data Quality

A dramatic metamorphosis began to occur in the content of professional notation, as electronic records replaced paper charts. Some of the most powerful advantages and weaknesses of EHRs show themselves in this area.

It was recognized from the time of the first EHRs that the bottleneck was getting physicians to type. A primary design challenge for EHRs from the beginning has been to find ways to make data entry as easy as possible. Dozens of technologies have been incorporated into various EHRs to reduce the pain of documentation. Each of these has opportunities for errors and some can create outrageous errors. Generating notes has never been easier, including notes that are inaccurate and unreliable.

Unreliable Notes

The most serious risk to patient safety presented by EHR documentation is the creation of inaccurate records. While other risks (drug errors, misidentification, etc.) can also be catastrophic, the long-term, insidious accumulation of unreliable documents across entire populations can adversely impact not only individual bedside decisions, but health planning and management for entire populations.

Before electronic records, the most notorious shortcoming of clinical documentation was illegibility. Computer assisted notation has eliminated that terrible problem for all intents and purposes; but in so doing unroofed an abscess of other deficiencies that were certainly present all along. In addition, electronic documentation has enabled a new set of hazards that could never occur in a paper environment. These novel hazards meaningfully threaten patient safety, quality of care, the validity of data aggregated for research, and also weaken the credibility of records used in professional liability claims.

Many providers view note-taking as an unrewarding chore. While everyone appreciates a concise, relevant, well-written, informative note, creating one is an art form. For many reasons, the quality of clinical documentation across health care has never been optimal. Even ignoring the reality of variation among authors in writing skill, today at least two other major factors work against the quality of notes. The first is production pressure, which burdens practitioners with schedules that can be physically and ethically unsustainable. One of the first corners to be cut under time pressure is note writing. Also, medical records have become sustenance for a hoard of secondary consumers of clinical data, with financial, administrative, quality, performance measurement, epidemiology, public health, education and other agendas, each of which imposes its own interests on standards for documentation. Plus, the ever-present shadow of liability risk management hovers over the process. These and other forces—however legitimate—dilute the value of the medical record to practitioners. To be fair, many physicians have never given much attention to record review. But, low expectations for the value of records is not an incentive to improve them; hence the expectation is fulfilled that they aren't very useful anyway.

In the early days of EHRs, the FDA was confronted with the question whether to regulate medical documentation software in the same way as software incorporated in devices like EKG machines. At that time, there was a feeling that electronic notation systems were basically word processors, passively recording input from expert users. Any liability related to content was the responsibility of the author, not the machine designer. This differed from the regulatory approach to black box devices in which

software is embedded in such a way that its operation is not apparent to the operator. However, contemporary EHRs contain numerous automated features that give them capabilities—and vulnerabilities—far beyond any typewriter. Such features can operate outside the control of note-makers, and even against their intentions.

Auto-populated Text

Many technologies allow data fields to be populated with pre-recorded content. Names for these actions vary between systems, but their functions should be familiar to regular computer users (Box 19.6).

Box 19.6

Paste forward: Inserting content from a previous note (or the entire note) into the current note

Templates and macros: Pre-programmed commands invoke a series of actions, which could be to insert a text block, signature, etc.

The ways these features can misfire are fairly self-evident. The final result of a malfunction in documentation is inaccurate documentation.

Spell-Checking

Users of texting apps on smartphones are uncomfortably familiar with errors that can arise when the system substitutes its choice of a word for the one the user intended (and may even have typed correctly). Some word replacements are merely humorous, but some cause serious miscommunication.

Copy-Paste

Most systems allow a block of text to be copied and inserted elsewhere. This function can be manual or automatic, and is heavily used by providers [22] despite generating a high rate of errors [23]. It can be efficient (and more accurate) to copy a complex item from a previous note and drop it into the current one. This prevents transcription errors and insures that critical content receives attention. Used judiciously, this is a valuable feature. Problems occur when it is used to simply avoid creating a new note. In situations (such as multi-day hospitalizations) when lengthy notes are sometimes generated over and over with minimal changes from one to the next, it is tempting simply to enter a copy of the last note and edit it as needed. The potential for creating false documents is so real that the Veteran's Administration has issued policy cautioning providers about the use of this function [24].

Paste Forward

In the extreme form of copy-paste, some systems automatically append the text of the old note at the beginning of the new one. Either way, the obvious danger is incorporating stale or false data into the current note. In some cases practitioners (or juries) have been presented with long threads of records, containing snowballs of accumulated notes that mostly reflect past visits, sometimes with no attempt even to edit them with the current facts.

Pasting a prior entry can be a system function, or a manual process performed by users. In some settings where patients have prolonged stays generating many notes that can be largely similar from one to the next (intensive care, long term care, rehabilitation), providers may choose—or may be encouraged—to copy a previous entry and simply update the bits that have changed. The laws of nature assure that sometimes these necessary edits will not occur.

Templates and Macros

Found in both clinical documentation and also order-entry systems (discussed below), templates have tremendous value in prompting clinicians into remembering important elements of their history collection, differential diagnosis, therapy protocols, patient instructions, and similar packages of information. However, many EHRs exploit this capability by using it to generate highly detailed and seemingly complete (but pre-fabricated) records upon a click of a mouse. The danger arises when the "canned" documentation does not reflect the actual care provided. Also, sometimes it can reflect care that should not have been provided. Both errors mislead everyone later relying on the false record, including subsequent treating providers, researchers, and attorneys trying to reconstruct events for legal purposes.

To an extent, the compulsion to generate extensive documentation arises from the hijacking of the original mission contemplated for EHRs (as clinical support tools) to become cash registers for insurance reimbursement. It would not be wrong to say that EHRs would never have proliferated without a business case that justifies their expense by their ability to generate revenue. In a healthcare economy firmly rooted in the tradition of fee-for-service, provider compensation remains tied in several ways to the completeness of provider records. Another reason EHRs are sometimes built with excessively elaborate checklists is because of a notion that this helps defend against lawsuits. Both ideas are counterproductive.

Completeness is not the same as quality (Box 19.7). Imagine a patient with a sore ankle. According to the byzantine rules of coding, the physician might get better reimbursement if he/she documents an exam of the eyes and ears in addition to the leg. Doing a clinically inappropriate exam is a different ethical violation than documenting an exam that wasn't done (the offense against the patient is worse if a useless procedure was actually performed, but the fraud is worse if it wasn't).

Box 19.7

Name: Person, Edgar T. **MR #:** 34390228
DOB: 1984-06-14 **Sex:** Male

Visit: 2009-08-02
S: Sore R shoulder x 2 months.
O: X-ray – lucency head of R humerus.
A: Lytic?
P: Ortho.

William Osler, MD

Sparse but intelligible documentation

Some templates generate long lists of historical or physical findings that may have no conceivable relevance to a case, and just clutter the record with irrelevant nonsense (Box 19.8). A cluttered record is hard to use, and invites mistakes. Some templated records are so uniform, bland and wordy that clinicians simply don't read them. This defeats the entire clinical purpose of patient data. Secondary uses of the chart (e.g., billing, process measurement) can still proceed with false data, but their integrity is sabotaged.

Box 19.8

HAPPY CLINIC EHR HEALTH DATA RECORD P-21-489660000

Name: Person, Edgar T. **MR #:** 34390228
DOB: 1984-06-14 **Sex:** Male

CHECKIN TIME 14:23:22 | ROOM TIME 14:41:12 | PROVIDER TIME 14:59:16 | RECEPTIONIST: WD | NURSASST: MM | INSURANCE VERIFIED | CONTACT INFO VERIFIED | HIPAA INFO PROVIDED | CONSENT OBTAINED | 234.987-097F.0D-32P ver12.09.87655.

Visit: 2014-08-02

History: Denies parachute accident, bear attack, domestic violence, prior suicide, hallucinogenic mushrooms, family history of Chagas Disease; collects stamps. Sore R shoulder x 2 mos. Confirms: Allergy to potato, plays flute, family history of complications, adopted. ROS: No depression, rash, headache, chest pain, dyspnea, dysuria, dysphoria, paraphilia, erectile dysfunction, hematochezia, scotomata, tinnitus, seizures or chilblains. Likes fruit.

Exam: HEENT normal, CNN I-XIII intact, identifies vanilla, no dysdiadokokinesia, PERRLA, EOMs intact, visual fields full to confrontation, sclerae and conjunctivae WNL, thyroid normal size, firm, no masses, tongue protrudes in midline, teeth show a possible cavity in #12, jugular pulse wave is normal at 45°, PMI is in 4thICS without gallop, murmur or rub, soft 4thheart sound present, lungs present, abdomen present, liver percussion = 216 mm in L mid-clavicular line, spleen approx. 149 gm., genitalia appreciated, limbs x 4, R shoulder pain = 5.2/10, mental status exam deferred. X-ray: Lucency head of R humerus.

Assessment: 354.4, need rule out 170, probably not E906.3 or E845.0; still have to consider 079.9.

Plan: Patient informed of pros, cons, plusses, minuses, advantages, drawbacks and probable and possible consequences of things done, not done, contemplated, foreseeable and unforeseeable in the near and remote future. Agrees, understands and applauds treatment plan. Handouts given for flu shot, vision screening, smoking cessation and vasectomy. All conceivable questions answered in astonishing detail. Ortho referral.

TIME SPENT 00:03:08. DEPARTED 15:06:33 AMBULATORY. ELECTRONICALLY REVIEWED, SIGNED, LOCKED AND LOADED. I CONFIRM THAT I AM NOT COMMITTING ANY KIND OF FRAUD [WO] 2009.08.02:19:44:18 GPS 120798604.3287-986076 USDA CHOICE 2010.01.02

Extensive documentation; but unintelligible and unreliable

Structured vs. Narrative Data

In the older days, computers could not perform many operations on unstructured text. To make it possible to count, sort, tabulate and compute data, it was necessary to encode it into fixed-length fields of carefully defined types. The legacy of this limitation of early data processing is the persistence of the many code sets now in place to capture the vast majority of clinical data. There is at least one (if not a dozen) coding system for symptoms, diagnoses, procedures, tests, results, drugs, devices, outcomes, fees, settings, and practically every type of healthcare information captured, stored or exchanged. Almost all of this data is expected to be encoded by users.

Programmer demand for well-structured data made a marriage with practitioner demand for efficient data entry. The result is now a plethora of interfaces that allow—and also may force—providers to record their findings as items picked from lists. This has created new ways to distort and corrupt data. Structured data is only reliable if fields are defined in standard ways and used with a degree of discipline that may not be achievable by clinicians. Furthermore, reliance on structured data sacrifices nuances of information that can only be captured in natural language. This trend has led to the general impoverishment of clinical records, as authors' vocabularies are constrained to selections provided by programmers. In the contest between the sins of too verbose and too sparse, replacing dictation with "click-tation" is more likely to create a record missing essential facts. Furthermore, while slips of the tongue can (and do) produce false records, slips of the mouse may have a higher propensity, because of the precision they inflict on data entry.

Drop-Down Lists and Checkboxes

In the eternal quest to protect practitioners from keyboarding, most EHRs provide menus that can be managed by pointing devices like mouse and touchscreen. These are susceptible to hand-eye coordination errors, such as "off-by-one" checklist errors, "drag-and-drop-in-the-wrong-location" errors, "double-click-instead-of-single-click" (and vice versa) errors, and similar.

Transcription and Voice Recognition

The astonishing revolution in voice recognition, voice response and natural language processing (NLP) technologies has only begun to be felt in healthcare. It is hard to imagine a more disruptive technology in human history than the ability to speak to and be understood by machines. The sluggish, frustrating and often comic early efforts at machine transcription of voice input have made enormous progress due to increased processor power (and clever science). Voice recognition software is becoming effectively usable and widely used in medical settings.

While human dictation-transcription has been universally accepted for decades, and automated dictation-transcription now offers serious competition, both are subject to production errors. Entire books and websites are devoted to funny malapropisms, freudianisms and other slips attributable to either the speaker or the transcriber, human or otherwise. But, the serious side of transcription error is when actual patient harm devolves from reliance upon false records.

Both human and software transcriptionists are likely to hear correctly a word like "electroencephalogram," even recorded by a person with a heavy accent in a noisy room. Whereas, both humans and machines are more likely to miss small words like "no," "not," and "doesn't." A radiologist dictated, "*I don't believe the lesion in the right upper lobe merely represents scarring from the prior procedure . . .*" The final report read, "*I believe the lesion in the right upper lobe merely represents scarring from the prior procedure . . .*" Consequently, a lung cancer went without investigation for 18 months.

That error involved an automated system, but a human could have made the same mistake. However, human transcriptionists vigorously point out that they have a superior ability to question (as well as intelligently correct during transcription) obvious slips, and will highlight words they can't interpret for later correction. Thus output errors can be intercepted during transcription, or can be appreciated and compensated for by later readers, who knowledgeably re-interpret obvious flubs. No harm, no foul. But, occasionally a discrepancy in output will mislead a clinician or patient, causing harm.

This brings up an unresolved legal conundrum for providers using any kind of transcription. There is an irreducible minimum error rate for any method of data entry, but explaining this to an injured party is problematical. There is no explicit norm for an accepted percent of "complications" caused by erroneous information. There is no comfortable cultural acceptance that sometimes records are wrong and sometimes this can cause harm. Patients (and juries) may have a general (but unachievable) expectation of zero defects. Some dictation systems append a disclaimer to their work product like, "*Dictated but not read*." It isn't clear that such a notice has any legal force. Furthermore, even if providers try (or are mandated) to proofread their documentation product, this would not result in perfect notes. Every editor knows the fallacy of authors proofreading their own writing. And, duplication of effort markedly reduces data entry efficiency. Knowing that perfect documentation is impossible sharpens our questions about how much we depend on medical record accuracy, for all purposes. One safety-minded approach to an inherently fallible process is to layer it inside another process with different failings. A defense against imperfect medical documentation is having many readers; another is taking every record with a bit of salt.

Multi-media

The difference between electrical and paper records is most apparent in a radically expanded definition of "information." Most EHRs today have the ability to incorporate virtually any kind of data into the record, including photography, graphics, audio, video, digital images, device outputs, large documents and special effects reminiscent of Hollywood. Multimedia and diagnostic images attached to medical records can powerfully improve patient care. Their greatest hazard is becoming attached to the **wrong** records.

Identity Management

Few incidents in the patient safety literature create more consternation than "wrong patient" events, and EHRs play a part in generating them. The ease of moving

information (creating, copying, importing, exporting, transmitting, etc.) also makes it easy to move it where it doesn't belong. Paper charts become contaminated with pages that stick together, faxes that are mislabeled, sticky notes that wander across desktops, and reports on patients with similar names. EHRs can commingle records through mis-clicking, mis-dragging, mis-typing, etc., and also have a serious potential for mis-identifying patients because of their dependence upon imperfect lists.

Every master patient index contains duplicates, misspelled names, former names, married names, nicknames, aliases, homonyms, middle initials, middle names and names from cultures that don't fit the pattern of "last, first, middle." An office may receive a prostate biopsy report on James Jones. The medical assistant might have to make a judgment whether to attach it to the record of "Jones J.," "Jones Jim," "Jones James T.," "Jones James [looks like a T might be an F]" or some other incarnation. Data incoherence, co-mingling, splitting, detachment and similar defects form a kind of electronic rubbish in information systems. This sort of corruption proliferates when data are exchanged automatically among systems.

Since the invention of EHRs, there has been contention between forces promoting a national system of unique patient identifiers, and forces concerned about the threat to privacy this could represent. The de facto standard of Social Security numbers has long been known to be hopelessly flawed, but in the U.S. no politically palatable alternative seemed possible to find. However, the need for authentication (and widespread use) of identities for various online activities may finally give birth to a solution, in the form of the National Strategy for Trusted Identities in Cyberspace (NSTIC) [25]. This is a 2011 White House initiative assigned to the National Institute of Standards and Technologies (NIST) that envisions, "Individuals and organizations [will] utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

Its guiding principles are:

1. Identity solutions will be privacy-enhancing and voluntary
2. Identity solutions will be secure and resilient
3. Identity solutions will be interoperable
4. Identity solutions will be cost-effective and easy to use

There is reason to think this effort will succeed in creating a trusted, national, user-centered "identity ecosystem" that will be of considerable value in reducing both misunderstandings and crimes related to patient mis-identification.

Record Alteration

When we catch a mistake in a medical record, there are accepted practices for correcting it. In paper charts, the custom is to cross out the error without making it unreadable, and enter the right information with a notation of the date and the identity of the person who made the edit. There is no implication of deception, and subsequent readers can recognize and rely on the corrected information in its context.

In contrast, in some EHRs corrections are much more difficult to make, and can induce errors. In the infancy of EHRs, legal consultants were concerned about fraud, impersonation, and unattributed entries. A fetish evolved for electronically signing, stamping and sometimes even locking notes so they couldn't be edited after saving. This satisfied a perceived legal need for strong assurance about record authorship and provenance. Except in very ancient systems, these practices are now redundant to the database technology that routinely captures *meta-data* about transactions like "create," "save," "view," "print," "edit," "delete," and so on; which are typically linked (with timestamps) to the login credentials of the user who performed them. Meta-data logs may also include details like the port number of the network connection used for access, the location of the terminal, and other arcane facts of interest to technicians.

An incidental effect of EHR meta-data is to add wrinkles to the process of legal discovery involving electronic information of all types.

From the standpoint of user-experience, meta-data renders obsolete the older-than-Egypt need for signatures on official documents, and merely adds an annoying, unnecessary step in requiring users to "sign" notes. But, record-locking becomes a safety issue when corrections need to be made. In some EHRs, it is frankly impossible to edit a saved note, no matter what errors it contains. (It is far from uncommon to insert a long, complex note into entirely the wrong chart. Being unable to delete a note on the wrong patient creates both a safety hazard and a privacy violation.) The more rigid systems only allow the user to write an "addendum" to the original, erroneous note, and in the worst examples, the addendum may be separated in some way from the original. In some systems, it is hard to tell looking at the erroneous note that an addendum needs to be hunted down; and it may not be evident what exactly is wrong. For example, if the note on June 12th incorrectly lists "warfarin" as a current medication, and this is corrected with a supplement on June 19th, a reader of the June 12th note in some EHRs might have no way of knowing where to look for the correction. At very least, keeping bad data alongside the good requires extra steps by users, creating yet another potential error pathway.

Personal Health Records

The task and challenges of clinical documentation have traditionally fallen to practitioners, with the patient record always being tethered to the provider's practice or facility. EHRs for the first time open the possibility of making patient records portable across sites, which is not shocking to providers, or even putting them in the custody of patients themselves, which is quite shocking indeed. The term "Personal Health Record" is not well defined, but refers to clinical information in the custody and control of patients, usually organized in a kind of summary format.

One profoundly underused safety mechanism that becomes possible with PHRs is to expose the record to the patient's review. It is essentially unheard of to find a medical record that does not contain serious errors, many of which are immediately apparent to the patient. Including the patient in the quality improvement process is

an obvious, yet radical innovation that may have significant benefits for organizations that take advantage of it. Ironically, the traditional, oral patient history is the primary source of information in most medical records. However, importing files of patient-created information into EHRs (whether structured data from devices or unstructured data from templates) introduces yet another in-box problem for providers, and another potential source of variance (if not contradictions) that need to be reconciled in the provider's record.

At the time of this writing, Personal Health Records (PHRs) come in three basic flavors, each of which has serious safety concerns (Box 19.9). (The PHRs discussed here do not include raw provider work product that patients may be able to view through electronic portals into provider-controlled EHRs.)

Box 19.9

1. "**Do-It-Yourself PHR**." The patient is presented with an empty template (basically a version of the waiting room clipboard) and is invited to fill it out with what he or she can reconstruct from memory and available documents.
2. "**Insurance Transaction PHR**." The patient's insurance carrier can sometimes deliver a register of transactions it has captured through the provider payment stream.
3. "**EHR Lists and Logs**." Some EHRs can print a summary report comprised of the sentinel lists (e.g., Problems, Procedures, Medications, Immunizations, "Allergies," etc.) contained in the provider record.

All the factors that can make provider-tethered records unreliable similarly apply to patient-controlled records, with added complications.

- Do-It-Yourself PHRs are almost invariably incomplete and can be wildly divergent from physician records—with either more or less reliability. Patients rarely possess complete collections of their records over their lifetimes. They may not accurately recall their medical histories, and may not be able to read, interpret or accurately transcribe record content; they may deliberately withhold or edit material they do not want providers to see.
- Transactional PHRs may amount to little more than "cash register tape," representing items submitted to that carrier for claims processing. These are subject to numerous distortions in the procedure and diagnosis encoding processes; and cannot capture events that are not billed by a provider, or which are billed to other carriers.
- Files exported from EHRs are only as accurate as systems and users make them. Since virtually no EHR is a complete repository of facts on any patient (newborns possibly excepted), excerpts from one EHR would ideally need to be merged with all others to create a "master" record. Formats and standards (e.g., the HL7 Clinical Document Architecture – CDA® [26]) are becoming perfected to allow aggregation of properly compliant files from different systems, but few PHRs that can be maintained by patients are currently designed

to accommodate this need. More problematic is the way EHRs generate summary information that would be exported. Manually maintaining lists of problems, medications and procedures, etc., is a labor intensive activity for practitioners and consequently is often be neglected. Automatically generating such lists is subject to numerous sources of error because of the professional judgment needed to define, label, reconcile and assign items correctly.

While portable, patient-controlled, untethered, professionally created and properly reconciled, authoritative personal health information would have tremendous value to a system with millions of mobile patients interacting with multiple providers, resources and caregivers, this vision is not yet within reach.

In summary, with respect to documentation functions, EHRs:

- Offer the priceless benefit of legibility.
- Have an enormous advantage over paper records with respect to accessibility in multiple locations, by multiple simultaneous users.
- Can be efficiently mined for content by both legitimate and unauthorized parties.
- Provide numerous ways to create more complete and helpful records.
- Provide numerous ways to create false, misleading and harmful records that are indistinguishable from good ones.

Ordering, Reporting and Communication Systems

The documentation process—although it can be enhanced by technology—is not fundamentally different in the paper and electrical worlds. The case is far different for order entry, result reporting and messaging. These are the most powerful ways in which EHRs have altered provider workflow, and are the sources for the most dangerous errors that directly impact patients.

Automating the activities of entering and executing provider orders and receiving and responding to test results have drastically changed the human roles in both in-patient and out-patient environments. And, electronic communication and digital media (e-mail, voicemail, texting, social media, Internet, Wi-Fi, etc.) have wrought the same changes upon healthcare as upon civilization as a whole.

CPOE

Computerized Provider Order Entry (CPOE) is the label for technology that transmits instructions from people who can give them to people who can carry them out. Since orders are likely to:

- Be written repetitively in the same way for many patients
- Be tedious to write under time pressure
- Contain so many components that even experts tend to forget some details
- Cause serious harm if written incorrectly
- Require calculations or adjustments that differ between patients

The CPOE functions of EHRs lend themselves perfectly to shortcuts and automation. According to the laws of Newton (as modified earlier) and Murphy (who is

in charge of all computer programming), any labor saving and safety promoting contrivance can misfire with harmful effects. The work of writing orders is cognitively quite different from writing notes. But, the user interfaces available to providers are very similar, and so CPOE is subject to all of the data input and output risks outlined in the previous section.

Wrong Thing Entered

The primary danger of computer-assisted data entry is entering the wrong thing. In its analysis of 3,099 EHR-related safety events in Pennsylvania, The ECRI Institute attributed the vast majority (1,867) to "wrong input" [27]. This can be achieved through all the functions listed in the prior section, and a few more specifically built for CPOE.

Pharmacy Errors

Reading the literature on EHR errors, it is easy to gather the impression that the vast majority of events are prescribing errors occurring in hospitals. This is mostly an artifact of reporting. The volume of hospital pharmacy transactions is enormous, because of the variety and effectiveness of today's drug armamentarium (and its overuse); pharmacy systems are among the most widely implemented applications in hospitals because of their good cost-benefit ratio; mistakes in drug administration are fairly easy to spot (if one looks) because of the number of individuals involved with them; agencies interested in quality metrics have an easier job finding pharmacy mistakes than many other kinds.

Artifact or not, there is no question that millions of drug errors occur annually across every part of the healthcare system, involving a serious percentage of patients. Although CPOE also has been shown to have benefits of lower error rates related to ambiguous abbreviations, legibility issues, impossible doses and duplications (intercepted by pharmacy logic checks), it can also induce errors. Han et al. found an unexpected increase in mortality among pediatric patients after the installation of a CPOE system in a children's hospital [28].

In a classic article, Koppel, et al. enumerated 22 different categories of medication errors in a mature, teaching hospital CPOE system, with errors occurring almost daily [29]. Among the issues identified were:

1. Information errors
   - Accepting the dose on the screen
   - Duplicating orders
   - Automatic orders linked to procedures
   - Automatic discontinuations
   - Diluent interactions not captured
   - Delayed recognition of contraindications
   - Failure to capture info from all systems
2. Human-machine interface flaws
   - Can't clearly identify the patient
   - Can't view all meds on a single screen
   - Log-in/log-out failures

- Extra steps required to "activate" orders
- Automatic cancellation of pre-surgical orders
- Downtime delays
- Orders near midnight interpreted as "tomorrow"
- Cumbersome interface makes charting difficult

Bar Codes

Because of its far superior accuracy to human keying (by perhaps a factor of millions), bar coding is widely employed by hospitals in pharmacy order entry systems. However, in another study, Koppel, et al. found 31 different causes of misread data (e.g., crinkled, smudged, torn, missing, covered labels; malfunctioning scanners; unreadable, damaged or missing patient wristbands; non-barcoded medications; low batteries; poor wireless connections; emergencies) plus 15 ways users could defeat its benefits with workarounds (e.g., affixing patient barcodes to computer carts, scanners, doorjambs, or nurses' belt-rings; carrying pre-scanned medications on carts) [30].

Auto-completion

A patient with heart failure presented to the Emergency Department, and the hospitalist prescribed a drug by entering the letters "L," and "A," and hitting ENTER. The intended prescription was "Lasix" but the system entered "Labetalol." The patient was dead in 30 min.

Putting the Fault in Default

One valuable service automation can provide is populating fields with default values. This avoids variance and mistakes in data content and format, and restricts choices to a set of selected entries. However, default data entry is the CPOE analog of paste-forward discussed above, and a sure source of wrong-input errors. Defaults can be positive (entering orders) or negative (removing orders). In different facilities narcotic overdoses were caused by a default dose of hydromorphone that was in the clinically appropriate range but too high for many patients; dangerous gaps in treatment were caused by a default that canceled all ICU orders on patients transferred to the medical floor; duplicate orders were written on patients because a rule triggered standing orders that had already been manually entered.

Order Sets

Younger physicians will marvel to learn that doctors once disparaged "cookbook medicine," and prided themselves on not relying upon reference material. Using the crutch of prompts, reminders and standardized order sets was felt to degrade professionalism and even to be dangerous to patients who deserved individualized attention. This sentiment is headed in the direction of leeches. The complexity of diagnosis and treatment today virtually mandates reliance on checklists, guidelines and other forms of prompts and reminders.

However, these tools are not benign. Someone has to build them, and someone cannot envision every possible contingency, which preserves a sliver of validity in

the old protest about cookbooks. There is serious risk to patients in templates being reflexively executed. Like the problem of auto-proofreading, it can be difficult for providers conditioned to invoking a package of tests or treatments to review them critically each time.

Still, the benefit of standard order sets outweighs their risks. Even when only presented to users in the form of general suggestions, they can promote safer care by being useful memory aids. When customized according to rules triggered by individual patient circumstances, they can be even more valuable. But, they need to be thoughtfully designed, their performance must be audited, consensus about their use must be built across different users and groups, they must be updated in the face of new standards of practice, and care must be taken that they function properly after updates, upgrades and modifications to external systems that they depend on for inputs.

Pre-programmed activities are like scalpels: *indispensable*, *but capable of mischief*.

Calculated Data

What computers do best is rapidly calculate numbers. Automatic execution of formulas with data from numeric fields has certainly saved patients from countless errors in diagnosis and therapy. But, even the simplest computer trick can backfire. One case involved converting between different units of measurement. EHRs used in pediatric settings in particular need to accept data entered in feet, inches, centimeters, pounds, kilograms, milliliters, ounces, days, weeks, months, years, and a slew of other units. In one system, programmers created a clever shortcut whereby a pediatric weight field (displaying "kg") would automatically divide whatever was entered by a factor of 2.2 if the number was followed by a space and a tab, but would leave it alone if it were followed by a tab alone. This allowed providers to type either pounds or kilograms, and conveniently convert whatever was entered to the right units. Of course, hundreds of errors were caused by users inadvertently confusing the keyboard sequence. The doctors in the affected practice described their growth charts as looking like seizure recordings.

Usability testing would almost certainly revealed the problem with an idea that must have seemed ingeniously useful in the programmer's imagination.

Programming Error

In any contest between user-error and machine-error, the machines will prove more reliable by a vast margin. Nevertheless, software is designed, built, installed, configured, updated and tested by humans before it reaches end-users, and is subject to flaws at each step. Often, internal flaws in logic, function or data resources will not be apparent to users. Such "black-box" malfunctions can go unnoticed for significant periods, since users may have no immediate ways to recognize that things are going wrong.

A patient with seizures, on phenobarbital, came to the ER in a coma. The resident smartly ordered a phenobarbital blood level, which was reported as "zero." The patient was admitted to ICU and managed on a ventilator overnight. In the morning,

the lab tech called the resident, "To talk about that pentobarbital level." As it turned out, the CPOE system had a list of some thousands of possible drugs that might be measured, and the lab analyzer had been updated with a list of some thousands—plus or minus a few—of drugs it could test. During a software update, the two lists became de-synchronized somewhere before the letter "p," with the result that the resident had correctly ordered phenobarbital, and the system had dutifully tested pentobarbital.

Display Errors

In addition to dangers on the EHR-input side, patients can also be harmed by problems with EHR outputs, including screen displays, reports and notifications.

In a highly publicized case, a software update resulted in a hospital CT scanner delivering eight times the intended dose of radiation to several hundred patients. An FDA investigation revealed that the machines involved were functioning as designed [31]. However, the interaction between the new software—which performed some automatic calculations actually intended to make the process safer—and the user, who needed to evaluate and respond to several inputs on a screen—produced patient injuries. This case illustrates the delicate relationship between designers and users, both of whom must collaborate to generate good or bad outcomes.

Users are faced with many kinds of computer displays, which are subject to countless variables that affect readability, including:

1. Color, focus, brightness, backlighting, contrast, resolution
2. Font, size, style, background, spacing, margins, highlights
3. Physical location, glare, viewing angle
4. Overlays, animations, transparency, graphics

All of these are intended to make it easier to apprehend and interact with information on the screen. All of these can be used brilliantly or horribly by designers and configurators.

Accommodations for users with disabilities (e.g., color-blindness, near- or farsightedness) may not be available or thoughtfully designed; mobile devices with tiny screens are especially challenging; shared devices require multiple users to compromise.

Awful Printouts

Some EHRs seem to have invested all their development funds in designing online interfaces and then run out of money when time came to build their reports. It is common to find that printouts, even ostensibly of on-screen activity, do not faithfully resemble what's displayed. Moreover, many printed reports, particularly those holding themselves to be "copies of the medical record," look nothing like what the EHR user sees in actual use, and can be extremely difficult to interpret by providers who receive them for continuity of care.

Interoperability

In early EHR days, developers had hundreds of combinations of programming languages, operating systems, database platforms, hardware and information coding

standards to choose from in building EHRs they hoped would be clinically and commercially appealing. There was no way of knowing in 1985 which of those building blocks would survive to 1995, let alone today. (Cynics also point out that some vendors may have calculated a market advantage if their software used data formats that could not be transferred to other systems.) Over time, many brilliant designs and concepts proved unmarketable, regardless of clinical worth. Still, today, there remain over 300 active vendors in the EHR space, most of which format patient data in different ways.

Moreover, patients are mobile, doctors are mobile, medical practices come and go, hospitals and groups merge and spin off. EHRs undergo version updates, vendors go out of business, merge and spin off, re-engineer themselves. And, technology evolves. This means the tenure of a given patient within a given EHR environment is transitory. The data has got to become portable.

The demand for—and value of—data exchange across disparate EHRs has engendered (in a Darwinian fashion) both industry standards and regulatory mandates to permit, if not actual interoperability, at least the possibility of exporting a file from one system and importing it without too much damage into another. Every year at the HIMSS Interoperability Showcase (Healthcare Information and Management Systems Society [32]), vendors demonstrate better integration of devices, inputs, outputs and work product across manufacturers, versions, hardware and platforms. Nevertheless, sharing data between EHRs is fraught with risk.

Despite better industry understanding and adherence to technical data standards (of which there are many specialized sets), the process of transmitting even a single record across systems creates a procrustean dilemma.

A. The record can be automatically absorbed into the recipient system. This means each item in the record (e.g., problems, drugs, procedures, immunizations, allergies) will either join an existing list, overwrite an existing item on a list, or be discarded as outdated or duplicative.
B. The record can be directed to some user's "inbox," where it must be deliberately, consciously, accepted or rejected before it joins the existing data.

Both options can create data entry errors, for all the reasons previously outlined. But, the problem become unmanageable when scaled up to thousands or millions of records, which is necessary when a large hospital system switches EHRs, or merges with another.

The transition of an acutely ill patient between points of care is perhaps the most dangerous procedure in medicine. Transferring their data with them is very often bungled. Currently, direct, peer-to-peer verbal sign-offs are the only safe way to insure that critical information is transmitted along with the person, to the embarrassment of EHRs everywhere.

The "Cuckoo's Egg"

A frequent call to risk managers is prompted when a provider receives an orphaned report. This could be a lab, imaging or pathology result with serious and time-sensitive consequences that may slip out of a fax machine or pop up in an inbox (e.g., biopsy positive for cancer), for a patient that the recipient does not recognize. Sometimes this happens because the fax number was misdialed. Or the report may have been intended for a colleague or a provider with a similar name;

or it might be for a patient who has been referred for a visit next week and isn't registered yet.

In any case, the report represents a latent hazard. If it was meant for another recipient, then that provider is presumably unaware of the result. Delay could hurt the patient. The only thing to do is to investigate and take responsibility for getting the right thing done. This takes a bit of effort, but there's no other ethical solution.

The Inbox Problem

Now, imagine this situation multiplied by a thousand. "*Good morning doctor*, *there are 2*,*345 items in your inbox*." Many are results the doctor ordered. Many are duplicates. Many are "for your information" copies. But, the one critical item that doesn't belong and really needs to be addressed is likely to be missed in the workflow. There is currently no automatic way to filter the clinician's incoming task stream. Like e-mail, it needs to be managed, but nobody has figured out how.

Electronic Communication

The discussion of order entry and result reporting was focused on structured data. But, unstructured data represents 80 % of medical information. Among safety issues, miscommunication and failure to communicate stand out as sentinel hazards. Among safety promotion measures, improved communication would be among anyone's top choices. All the tools and devices available to general and consumer markets for electronic communication are available for healthcare purposes—sometimes with "professional" enhancements (e.g., encryption). These offer great value and great risks to physicians and patients (Box 19.10).

Box 19.10

Synchronous (*real-time*) *communication channels*

- Telephone, cell phone, Voice-Over-IP-Phone (VOIP)
- Audio conferencing
- Video conferencing, telepresence

Asynchronous (*store-and-forward*) *communication channels*

- Voicemail
- Fax
- Pager
- E-mail, secure e-mail
- Text messaging, secure messaging
- Portals, file sharing, collaboration environments

Infrastructure

- "Plain old telephone service" (POTS)
- Cell service
- Wired networks
- Wireless networks
- Satellite networks, Global Positioning Systems
- Short area networks (radio, infrared)

However, communication needs to be managed. While security and privacy of electronic communications have (appropriately) received intense attention, other safety issues are just as relevant. All the interface issues outlined for CPOE and result reporting can impact messaging systems. Just about every kind of misdirection, delay, duplication; loss/deletion; failure to notice, respond, forward, reconcile; disposition and delegation errors can easily be envisioned for any set of electronic messages, and has been recorded in the archives of patient safety events.

Patient Connectivity

Finally, the communication capabilities of EHRs are not limited to providers and hospitals. Partly because the multiuser power of EHRs liberates information from being hoarded by physicians; partly because of cultural upgrades that make healthcare knowledge and processes much more transparent to patients, it is today taken for granted that patients are expected to be consumers of and contributors to their own health records.

One effect this has is to add another population of EHR users, who can both create errors and intercept them. The error-trapping potential of including the patient in the loop of documentation, order validation and result management is potentially phenomenal. It will also add complexity to the challenges of designers and implementers, who must plan for the needs and impact of this diverse population. It is important to establish ground rules and norms that are currently not standard among institutions, practitioners and patients for the safe, secure and effective exchange of clinical information across the many nodes in the healthcare network.

Decision Support Systems

The patterns of risk and error above apply to fairly straightforward interactions between humans and computers. Perhaps documentation systems are just fancy word processors. Perhaps order entry systems are just electronic prescription pads and reporting systems are basically printers. None of this is true, but at a simplistic level, each of these applications might be mistaken for a labor-saving device. In contrast, the domain where computers conclusively prove their difference-in-kind from other technology is when they are used to augment human thinking.

Granted, it stretches the concept of "heath record" to mention functions like dose calculation, guideline presentation, therapy planning, alerts, prompts, warnings, reminders, interpretation of clinical findings, access to reference material and diagnostic suggestion systems in a chapter on EHRs. But these categories of HIT are often invoked as the most valuable rewards EHR user can expect, after suffering the pain of converting from paper.

Computer-Assisted Diagnosis

One of the hardest types of safety events to analyze and mitigate is the category labeled "Diagnostic error." Virtually since the day a patient history was first captured electrically, there were dreams of using the associative and correlative power

computers to help with diagnosis. Indeed, the 1990s were boom years for the application of artificial intelligence (and other programming techniques) to this purpose [33]. It is a little hard to know why CADx applications have not been among the most gloriously popular and commercially successful segments of the HIT market. Most of the legacy systems from the early years have fallen out of use, failed commercially or have not been maintained (although a few stalwarts have [34, 35]), but several promising applications have emerged in the last few years that will hopefully rekindle interest.

The safety issue for a diagnostic assistance (or diagnostic suggestion) program is obviously the same for the software as for the human. (There may also be liability issues, although developers rely heavily on the law's "learned intermediary doctrine," which can insulate vendors of products used by experts on behalf of consumers from the liability they have for products intended for use directly by consumers themselves.) In this respect, whether the system points outright to a potential diagnosis, or produces a list of differential possibilities, or calculates a likelihood, or highlights a set of diagnoses associated with a certain set of findings, there will be both Type I and Type II errors (pointing users at the wrong one, or leaving the right one off the list).

Alerts, Alarms and Triggers

Another way technology can be recruited to the cause of safety is to build alarms that alert inattentive or distracted humans when some triggering condition has occurred. EHRs have many locations where alerting functions can be installed—many more if non-EHR devices are included. Doses that need adjustment, therapeutic duplication, orders outside recommended guidelines, contraindications, IV admixtures that are incompatible, lab values or physiological parameters out of range, scheduling, calculating, monitoring, counting; there is no end.

Each of these systems is a mini-program that had to be designed, written, installed, tested, configured and updated, and needed user training. Applying Newton's computer law, any one can misfire in each of these steps. But, most alarm failures are not technology issues, but problems in the way they interact with their human targets. From the standpoint of users, many alarms have only two settings, "Too sensitive" and "Not sensitive enough."

Alarm Fatigue ("Wolf, wolf!")

Alarm fatigue leads to users ignoring and overriding valid warnings, and even disabling systems that generate annoying ones, with obvious consequences. A dilemma that most designers have not seemed to recognize is that users in different situations benefit from different alarm settings. Novices (new employees, interns, consultants who use the system infrequently) may need and tolerate relatively low thresholds for alerting, and fairly verbose messages. High volume experts who develop automaticities through frequent use only want to be interrupted for actual anomalies. Intermediate users need another tuning. The problems that tend to occur with alerts and alarms are when users are confronted with an interruption at a point in the workflow or with a frequency that has no meaning for them. It is in

these cases that users stop responding. Allowing users to customize own alarm levels, while retaining the ability for the system to override user settings just as users can override system settings presents both tricky programming and administrative challenges.

Clinical Calculators

At the time of writing, there have been at least 100,000 "medical" applications developed for mobile devices alone [36]. Some of these products become defunct weekly, many are consumer facing products for fitness and diet management. But, a growing number are explicitly aimed at professional audiences, performing sophisticated functions like helping calculate radiation doses, pediatric drug doses and physiologic parameters like creatinine clearance, etc. The FDA is deeply perplexed about how to review, monitor and regulate the performance of products in this market.

Recall and Reminder Systems

In the world of safety, one of the largest categories of failure is breakdown in the chain of notifying a provider or a patient of the need for follow up. One might think the time honored custom perfected by dentists of sending reminder postcards would have been implemented EHR systems from the beginning. In practice, this turns out to be an immensely complex problem, involving a web of interdependent contingencies and decisions. That said, it is exactly the kind of rule-based conundrum that computers excel at, and do so much better at than humans. In face of the high impact recall failures can have upon patients (and the high prevalence of recall failures among malpractice claims), it is surprising that this category has been given relatively little attention by EHR developers (and their efforts often offhand and occasionally unworkable). The reason is not technical; much harder problems have been attacked successfully in software. The author's experience is that the problem is cultural. There is simply nothing in the traditional autistic, exam-room-centered, face-to-face-biased workflow of physicians that calls for tools to manage recall. This is consistent with the absence of acknowledgment of task recall as a reimbursable item in the pay-for-procedure system that governs physician behavior; thus EHR developers are not used to hearing a demand for such features.

Data Analytics

Behind the scenes of real-time EHR-user interactions, information about patients, providers, institutions, diseases, therapies, costs, outcomes and a thousand other variables is being collected in vast warehouses. Like the (even larger) quantities of consumer data available to marketing analysts, healthcare data increasingly is being sought and used for epidemiology, quality measurement, law enforcement and security, genetics, economics, education and every purpose of pure (and marginal) science and commerce. It is being discussed that in some cases, the need for prospective clinical trials may be able to be avoided because models of treatment effects can be built from streams of existing data. Many of the design challenges of clinical

research may become solved, or at least re-defined, because managing multiple variable statistics is a different undertaking in the context of "big data."

Enormous databases do have some power to mitigate imprecise and muddy data, but less so with actually wrong data. A challenge for miners of healthcare megadata is that several generations of EHRs have passed whose content has been encoded (ICD-9, CPT, etc.) in "lossy" formats that sacrifice accuracy and completeness. Just as poorly designed (or dishonestly conducted) research trials have at times mislead health science with invalid conclusions, care needs to be taken in accepting the products of large data analysis.

Where Is the "Golden Bullet"?

Training

In most high-performance industries (aviation, nuclear power, military), training is embraced as a critical safety control and essential cost. There are places personnel can't go, jobs they can't do, decisions they can't make unless they have demonstrated specific competencies, both large and small.

Oddly, for a culture that makes education the basis of its reputation, healthcare seems ambivalent and even a little resentful to have technical training imposed on it. In this respect, organizations that depend on fees for revenue may have strikingly different attitudes than those with global budgets. HIT demands a high level of technical support, and cooperation by end users in configuring, operating and troubleshooting systems that are becoming more complex every year. The intern's catchphrase, "See one, do one, teach one" is another of those relics of ancient medical culture that needs to be jettisoned from today's environment. While "operator error" is a contributing factor in the vast majority of adverse EHR events reported today, it is unconstructive—and will misdirect mitigation efforts—if every malfunction is addressed by simply mandating more user training.

Physical Hazards

A thorough safety review must include potential physical hazards of electrical devices including shock hazards, radiofrequency interference, toxic components, radiation exposure and miscellaneous rare risks such as detaching from mountings, dropping, skidding and colliding with people or other devices.

Device Hacking

Both wired and wireless devices in hospitals increasingly connect to networks that are exposed to intrusion by hackers. There are reports of experimental and malicious penetration of the controls of both diagnostic and—most concerning—therapeutic instruments, such as insulin pumps, infusion pumps and ventilators.

Take-Home Message

The foregoing has not emphasized—but it is fitting to say out loud—that information technology is a social force of volcanic proportion that will transform the landscape of medical practice as it has re-shaped so many other facets of society, and will continuously revolutionize the ways doctors, nurses, hospitals and patients interact the more pervasive it becomes. EHRs are a central element of HIT, whose value will be multiplied when they are adopted by a critical mass of providers, and master the problems of data exchange across health information networks. Few human inventions have greater impact upon civilization than information technology, whose upheaving effects proceed at a tempo much faster than the march of generations.

However, *if EHRs were drugs*, *the FDA would have concerns like these*:

A. It is not fully clear what disorders they should be prescribed to treat.
B. There is little objective evidence of their effectiveness, despite many claimed benefits.
C. Their side effects are not well characterized and may be under-appreciated.
D. Some uses may be hazardous.

In many ways, EHRs would be considered "investigational" if the healthcare enterprise were not utterly dependent on information for its every operation. New information tools and channels are not subject to the rules that would slow the adoption of other risky innovations.

Fundamentally, the weaknesses of EHRs are not simply flaws in technology that only await smarter programming. The problem is that EHRs manage information—the underlying material of the universe. Human systems where EHRs are embedded are more complex than technology, and their operating principles and decision rules are beyond our ability to replicate in software. This fact guarantees unintended consequences, which are the law of every natural system. Healthcare's dual personality makes ratcheting progress, jerking irregularly forward with brilliant inventions while regarding each novelty with the suspicion of "*First*, *do no harm*."

References

1. Amarasingham R, Plantinga L, Diener-West M, Gaskin DJ, Powe NR. Clinical information technologies and inpatient outcomes: a multiple hospital study. Arch Intern Med. 2009;169(2):108–14.
2. Bright TJWA, Dhurjati R, et al. Effect of clinical decision-support systems: a systematic review. Ann Intern Med. 2012;157(1):29–43.
3. Dorr D, Bonner LM, Cohen AN, et al. Informatics systems to promote improved care for chronic illness: a literature review. J Am Med Inform Assoc. 2007;14(2):156–63.
4. Garg AX, Adhikari NK, McDonald H, et al. Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review. JAMA. 2005;293(10):1223–38.
5. Goodman C. Savings in electronic medical record systems? Do it for the quality. Health Aff (Millwood). 2005;24(5):1124–6.
6. Linder JA, Ma J, Bates DW, Middleton B, Stafford RS. Electronic health record use and the quality of ambulatory care in the United States. Arch Intern Med. 2007;167(13):1400–5.

7. Aspden PCJ, Wolcott J, Erickson SM, editors. Patient safety: achieving a new standard for care. Washington, DC: Institute of Medicine, The National Academies Press; 2004.
8. IOM (Institute of Medicine). Health IT and patient safety: building safer systems for better care. Washington, DC: The National Academies Press; 2012.
9. Public Law 111 – 5 – American Recovery and Reinvestment Act of 2009. (Approved 17 Feb 2009)
10. Mark Mansour, JD, partner, Jones Day (Washington, DC). Presentation at Health Information Management Systems Society (Orlando, FL), 23 Feb 2014.
11. U.S. Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Section 164.308 – Administrative safeguards
12. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), Codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq.
13. National Institute of Standards and Technology. Information security. NIST special publication 800-30, revision 1, Sept 2012. Washington, DC: U.S. Department of Commerce.
14. Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Qual Saf Health Care. 2010;19 Suppl 3:i68–74.
15. ECRI Institute, 5200 Butler Pike, Plymouth Meeting, PA 19462-1298, www.ecri.org
16. Magrabi F, Ong M-S, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19(1): 45–53.
17. U.S. Code of Federal Regulations, Title 42, Chapter 6A, Subchapter VII, Part A, Section 299 – Mission and duties [of the Agency for Healthcare Research and Quality]
18. http://www.pso.ahrq.gov/common.
19. Pace WD, Staton EW, Higgins GS, Main DS, West DR, Harris DM. Database design to ensure anonymous study of medical errors: a report from the ASIPS collaborative. J Am Med Inform Assoc. 2003;10:531–40.
20. Smith PC, Araya-Guerra R, Bublitz C, Parnes B, Dickinson LM, Van Vorst R, Westfall JM, Pace WD. Missing clinical information during primary care visits. JAMA. 2005;293:565–71.
21. Smith v. United States, 119 F. Supp. 2d 561 (D.S.C. 2000). Betty C. SMITH and Rudolph Smith, Plaintiffs, v. United States of America, Defendant. United States District Court, D. South Carolina, Beaufort Division. 5 June 2000.
22. Thornton JD, et al. Prevalence of copied information by attendings and residents in critical care progress notes. Crit Care Med. 2013;41:4.
23. Weir CR, Hurdle JF, Felgar MA, Hoffman JM, Roth B, Nebeker JR. Direct text entry in electronic progress notes: an evaluation of input errors. Methods Inf Med. 2003;42(1):61–7.
24. Department of Veterans Affairs, VHA Handbook 1907.01, Health information management and health records. Washington, DC: Veterans Health Administration. 19 Sep 2012. www.va.gov/vhapublications/ViewPublication.asp?pub_ID=2791
25. National Strategy for Trusted Identities in Cyberspace. www.nist.gov/nstic/index.html
26. Health Level Seven International. The HL7 Version 3 Clinical Document Architecture (CDA®)
27. Presentation by William Marella, MBA (Director, Patient Safety Reporting Programs), and Karen Zimmer, MD, MPH (Medical Director), ECRI Institute Patient Safety Organization, 5200 Butler Pike, Plymouth meeting, PA 19462-1298, www.ecri.org at Health Information Management Systems Society (Orlando, FL), 25 Feb 2014
28. Han YY, Carcillo JA, Venkataraman ST, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics. 2005;116(6):1506–12.
29. Koppel R, Metlay JP, Cohen A, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005;293(10):1197–203.
30. Koppel R, Wetterneck T, Telles JL, Karsh BT. Workarounds to barcode medication administration systems: their occurrences, causes, and threats to patient safety. J Am Med Inform Assoc. 2008;15(4):408–23.
31. U.S. Food and Drug Administration. Safety investigation of CT brain perfusion scans: Update 9 Nov 2010. www.fda.gov/medicaldevices/safety/alertsandnotices/ucm185898.htm

32. Health Information Management Systems Society, (HIMSS), 33 West Monroe Street, Suite 1700, Chicago, IL 60603-5616. www.himss.org
33. Berner ES, Webster GD, Shugerman AA, Jackson JR, Algina J, Baker AL, Ball EV, et al. Performance of four computer-based diagnostic systems. N Engl J Med. 1994;330:1792–6.
34. Massachusetts General Hospital Laboratory of Computer Science. DXplain®. http://lcs.mgh.harvard.edu/projects/dxplain.html
35. Burger C. The use of problem-knowledge couplers in a primary care practice. Perm J. 2010;14:47–50.
36. Edney, Anna. FDA regulators eye medical apps for mobile devices. Bloomberg Businessweek, 26 Sep 2013.