

10-9-2013

The Electronic Health Revolution: How Health Information Technology Is Changing Medicine - And the Obstacles in Its Way

Cameron Stokes

Follow this and additional works at: <http://digitalcommons.wcl.american.edu/hlp>

 Part of the [Health Law Commons](#)

Recommended Citation

Stokes, Cameron. "The Electronic Health Revolution: How Health Information Technology Is Changing Medicine - And the Obstacles in Its Way." Health Law & Policy Brief 7, no. 1 (2013): 21-36.

This Article is brought to you for free and open access by Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in Health Law and Policy Brief by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact fbrown@wcl.american.edu.

THE ELECTRONIC HEALTH REVOLUTION HOW HEALTH INFORMATION TECHNOLOGY IS CHANGING MEDICINE—AND THE OBSTACLES IN ITS WAY

*Cameron Stokes**

I. INTRODUCTION

Hospitals have long been on the cutting edge of technological innovations, both in the operating room and the administrator's office. It is the area in between—where patients are monitored and instructed, and where care is managed—that the medical profession has been a laggard. As a result, medical care within the United States is frighteningly less organized, integrated, and streamlined than is ideal for an industry that, at one time or another, will service nearly every person in the country.

Fortunately, the medical profession is improving through the utilization of health information technology. Many changes stem from the implementation and improvement of electronic health records (EHRs), resulting in improved integration between care providers, such as primary care physicians (PCPs), hospital staff, specialists, and pharmacists. This paper will survey the changing medical landscape resulting from the EHR revolution. The biggest advantages of EHR technology go beyond the ease of electronic recordkeeping and into the integration and interoperability that EHR systems allow. When properly utilized, applications of EHR systems can reduce administrative costs and burdens, improve care quality, reduce mistakes, and provide a boon for public health research.

And yet, there are pitfalls and roadblocks that must be addressed. The dual issues of privacy and information security, resistance to changing

procedures, technologies and high startup costs, and unexpected hiccups in early adoption stand in the way of an easy transition. Each of these issues will be examined, and recommendations will be made for a more robust and successfully integrated health system. EHRs and the greater health information technology changes occurring around us can revolutionize healthcare delivery if the systems can be implemented as envisioned—but whether that will happen remains to be seen.

II. ELEMENTS OF THE ELECTRONIC HEALTH REVOLUTION

In order to understand the overhaul that the electronic health revolution is bringing, it is helpful to understand a few of the most important technological changes that are making an impact on the medical profession. This section will focus on electronic health records (EHRs), health information exchanges (HIEs), and patient safety organizations (PSOs).

A. Electronic Health Records

Electronic health records are most easily described as a one-stop-shop for medical data on a particular patient. An EHR can consist of patient demographics, medical history, clinical notes, symptoms, diagnoses, current medications, vital signs, laboratory data, and radiology reports.¹ In essence, EHRs allow hospitals and physician offices to reduce large paper files into neat, easy-to-access electronic ones.

It is helpful to note the distinction between EHRs and electronic medical records (EMR). EMRs are essentially an electronic version of the paper records held within a medical practice.² EMRs contain patient medical and treatment histories, and are

* Cameron Stokes, J.D. Candidate, Georgetown University Law Center, 2013; B.A., University of North Carolina at Chapel Hill, 2010. The author would like to thank Professor Jennifer Geetter for her support and guidance throughout the drafting and editing process, as well as Katie Keith, Kevin Lucia, and Sabrina Corlette at the Georgetown Health Policy Institute for piquing his interest in health policy.

essentially proprietary. But EMRs are not meant to be interoperable, and thus are not easily transferred between settings. In order to transfer EMR data to another practice, hospital or even department, the data must often be printed out.³ In this way, EMRs are only marginally better than paper records. EHRs, conversely, are *designed to be transferred between care providers and practice settings*.⁴ EHRs thus have the potential to improve care coordination and quality in a way that EMRs cannot. For this reason, this paper will only look at EHRs.

Electronic health records have been around since the 1960s. In the latter half of that decade, various academic hospitals developed proprietary systems for use in their medical centers.⁵ The Department of Veterans' Affairs (VA) began to use its own EHR system in the 1970s, known as VistA.⁶ Though EHR systems have been around for half a century, adoption has been relatively slow. Among hospitals, adoption of at least a basic EHR system was seen in only 13.4% of non-federal acute care hospitals in 2008.⁷ By 2011, however, this number had jumped to 34.8%.⁸ As time progresses and the benefits of EHR systems become more apparent to non-adopters, this number will likely increase at an even greater rate.

Hospitals without EHRs often have separate file systems for each of their departments, such that one hand does not know what the other is doing.⁹ This can occur even when these departments store information in electronic format. To transmit patient data from a doctor to the pharmacy, for example, the information may be faxed over and manually entered into the pharmacist's computer. At best, this lack of coordination results in wasted time and effort, while in the worst case scenario it can result in harm to the patient. EHR systems allow medical professionals quick and easy access to patient records to verify, edit, or insert information. EHRs underpin much of the electronic health revolution as patient care goes online.

EHRs also offer the opportunity for patients to monitor and review their personal health records. This will allow patients to ensure their information is accurate and can also encourage patients to be involved in their healthcare decisions. The Indian Health Service, for example, is in the process of implementing a personal health record through their

EHR system, eventually allowing patients to view information about health conditions, message care providers with questions, and refill prescriptions online.¹⁰

B. Health Information Exchanges

Health Information Exchanges (HIEs) are another tool in the electronic health arsenal. They are essentially an outgrowth of EHRs in that they allow EHR data to be shared across platforms and among stakeholders through interoperability.¹¹ This exchange can improve patient health and safety by reducing errors in transcription and transfer of patient records, while also offering the potential for lower administrative costs. One aspect of the Health Information Technology for Economic and Clinical Health Act (HITECH)¹² was the provision of \$2 billion for the development of HIEs.¹³ A large part of this funding was intended to promote more "meaningful use" of EHR in ways that require HIEs. E-prescribing, for example, requires the exchange of health information between the prescribing doctor and the pharmacy. Health information exchange allows this transfer to occur entirely electronically.

HIEs have already shown themselves to be useful. During Hurricane Sandy in October 2012, many patients in New York-area hospitals had to be relocated. Such a transition would once have required frantic calls to other providers and patient family members in order to piece together a working medical history and current diagnosis. With an integrated HIE, however, administrators were able to call upon a patient's record simply by accessing that information online through the exchange.¹⁴ This was possible because New York has a statewide HIE, known as the Statewide Health Information Network of New York (SHIN-NY), which tracks hospital admittances, allowing providers access to required patient information.¹⁵ HIEs are already an integral part of the electronic health revolution, and have great potential to improve patient safety and reduce administrative costs as their development continues.

C. Patient Safety Organizations

The Patient Safety and Quality Improvement Act (PSQIA)¹⁶ introduced Patient Safety Organizations as a method of improving the quality and safety

of medical care.¹⁷ PSOs accomplish this goal by allowing healthcare providers to share and aggregate data to flag problem areas and reduce risks to patients.¹⁸ To become a PSO, the mission and primary activity of an entity must be the undertaking of activities to improve patient safety and healthcare quality.¹⁹ The Agency for Healthcare Research and Quality (AHRQ) currently recognizes 76 PSOs as meeting the requirements.²⁰ One aspect of the Patient Protection and Affordable Care Act (ACA)²¹ is a push to reduce hospital readmissions. Hospitals with high risk-adjusted readmission rates are encouraged to work with PSOs to improve patient safety.²² Much like HIEs, PSOs function by aggregating large quantities of patient data to form an overall picture of care quality, specifically with the goal of reducing adverse events. In this way, PSOs are yet another aspect of the electronic health revolution that seeks to improve the healthcare system.

III. POTENTIAL BENEFITS OF THE REVOLUTION

These changes in the practice of medicine hold great promise. The ability to integrate records across providers and practice settings means that emergency room (ER) doctors can know a patient's medical history simply by calling up his or her EHR, even if the patient has never been to that hospital before. The computing power behind electronic records means that certain medical knowledge, such as adverse drug interactions and treatment cycles, can be left to the patient's record to monitor, reducing mistakes, and freeing up personnel for other tasks. Even more, EHRs—when the information is anonymized and aggregated across population groups—can potentially revolutionize public health research and reporting. This section analyzes some of the many benefits that the revolution holds for the health care industry and for society.

A. Better Outcomes and Fewer Mistakes

The dream of EHRs begins with the hope that widespread adoption of EHR systems will improve patient outcomes. A study by Kaiser Permanente found that use of EHRs was associated with improved recognition of diabetic patients in need of greater drug treatment as well as better control of disease risk factors among sicker patients.²³

Another study of U.S. nurses found that those who used comprehensive EHR systems reported better care and outcomes and encountered fewer patient safety issues and adverse drug reactions.²⁴ EHR systems can automatically flag potential areas of concern and remind medical professionals—who can be overworked or unfamiliar with a patient—to double check areas they may otherwise overlook.²⁵ A properly implemented and maintained EHR system has the potential to revolutionize care quality in many settings.

With prescription drugs, electronic systems can provide doctors with alerts when they use confusing or inappropriate abbreviations in prescriptions and can check for drug allergy interactions, drug-drug interactions, and duplicate drugs.²⁶ EHRs have also been shown to reduce medication errors through the use of electronic checklists when entering medication histories.²⁷ With complete integration of EHRs through HIEs and interoperable systems, medication errors can be reduced even further. Where a clinician using a basic electronic system has the advantage of an electronic checklist, he or she still must often rely on the patient to provide a complete, accurate medication history. Integrated HIEs allow the clinician to call upon the patient's record from all past encounters with the healthcare system, greatly reducing the chance of forgetting a past medication.²⁸ This possibility demonstrates one of the greatest promises of EHR systems—the ability for systems to “speak” to one another, instantly confirming the safety and necessity of medical care, thereby reducing redundancy, improving outcomes, and minimizing mistakes attributable to human error.

B. Public Health

One of the most promising potentialities of the electronic health revolution is in the area of public health. The health information of one individual may only be useful to that person, but when identifying information is removed and the health data is aggregated with the records of countless other individuals, the data can help society at large. Public health researchers can take aggregated data and spot potential disease outbreaks, find dangerous drug interactions, and improve quality of care in the greater community. The Centers for Disease Control

and Prevention (CDC) sees EHRs as a “game changer” in public health reporting, given the delay and burden of manual reporting of potential disease outbreaks.²⁹ Electronic data transfer allows public health officials to pinpoint problem areas more quickly, while automatic electronic reporting allows providers to share anonymized information that they didn’t know would be relevant to researchers.³⁰ Quick, easy access to aggregated health information stands to benefit public health in significant ways.

C.A Positive Outlook

As more providers implement EHR systems and electronic systems become the norm, resistance to the technology is likely to drop. Both doctors and patients will be more likely to accept the need for EHRs and see the benefits of integrated records systems. As systems are improved and standardized, interoperability is likely to improve, unlocking the greatest benefits of all. EHRs are poised to improve care quality and reduce mistakes as the technology matures, and some of these benefits are already evident among early adopters.³¹ The dream of interoperable health IT requires widespread adoption before all of the care-improving aspects of EHRs can be achieved.³² Once EHR adoption reaches critical mass, they will be poised to revolutionize the American healthcare industry in a number of ways.

IV. CONCERNS MOVING FORWARD

Even with the advantages of the electronic health revolution, there are still a number of drawbacks that must be acknowledged. As with any electronic information system, privacy and security are at the forefront of many people’s minds. Apprehension about who will have access to which records and when—as well as concerns about unauthorized access to protected information—follow whenever personal information is being used in new ways.³³ Change also breeds resistance, and EHRs are no exception. Hospitals and physician practices worry about the cost and burden of implementing these new systems, and some practitioners have shown resistance to making the change.³⁴ There are also some unexpected costs in the early stages of widespread EHR adoption, including an increase in reimbursement requests for expensive tests and

procedures coinciding with the implementation of EHR systems.³⁵

A. Privacy Concerns

Privacy is usually one of the first concerns people have when discussing a system that integrates and shares personal data. EHR systems are no different. One concern is that the move to integrated EHRs may dissuade a certain set of patients from seeing the doctor altogether.³⁶ These patients would be a small minority, but those with a strong distrust of the electronic transition may have a real and significant fear of having their records converted into EHRs.³⁷ For them, doctors in the short run can do little more than provide assurances that patient data privacy and security are taken seriously and explain how EHRs work generally.³⁸

Other patients will see the benefits of electronic systems,³⁹ including the ability to e-prescribe necessary medicines and the reduced number of redundant forms required in office waiting rooms. But these same patients may be on the fence about the larger integrated nature of EHR systems. They may be grateful that they don’t have to take a paper prescription down to the pharmacy to have it filled, but they may be uncomfortable with one specialist having access to the records created during a visit with a different physician. In this way, some patients may be protective of their medical records in a way limits the usefulness of EHR.

Records need not be shared with any and all in the medical profession, but it is entirely plausible that a cardiologist could benefit from a patient’s records created by that patient’s PCP.⁴⁰ In fact, the integration of one system of records among all of a patient’s providers is one of the main tenets of an EHR system via HIEs. Past diagnoses may bear on current examinations and prescriptions much more heavily than a patient can realize, and integrated, interoperable EHR systems are a necessary part of maximizing patient benefit. Much like a loan financier who needs access to an applicant’s bank records and income statements, medical staff need open access to relevant parts of a patient’s medical record in order to effectively diagnose and treat any issues that may exist.

Many of these privacy concerns arise when patients are concerned about potentially authorized access to their medical records. Patients may be uncomfortable with the ease at which their records are accessible by a member of the medical profession, even if the medical or diagnostic benefit to the patient is quite large. These worries are likely to dissipate as EHR systems become not only standard, but obligatory. Hopefully, as more patients see the advantages of integrated EHRs, they will be more open to them.

B. Records Security

It is impossible to create a perfectly secure computer system, and so there will always be a struggle between the poles of security and accessibility.⁴¹ The more restrictive a system is, the more likely it is to be secure from outside threats (though the most advanced cyber threats will always be a step ahead of the most advanced security), but such security comes at the cost of ease of accessibility. Likewise, an open, accessible, and efficient system of interoperable records will likely be less secure than it otherwise could be. The goal of the implementation of EHR systems is to balance the two aspects so that EHRs can be used to facilitate healthcare decision making and reduce administrative burdens while also maintaining patient confidence in the integrity of their protected health information (PHI).

Even in the relatively short history of widespread EHR use, there have been a number of high profile data breaches.⁴² What is most interesting about these breaches is that many occurred not through hacking into secure systems, but through old fashioned loss, theft of physical media, or simple user error. For example, in 2006, the Social Security numbers (SSNs) and birth dates of 26.5 million veterans were compromised when a laptop was stolen from a VA employee.⁴³ Similarly, the theft of a National Institutes of Health (NIH) laptop from a researcher's car in 2008 resulted in the breach of clinical trial information including SSNs of 1,200 participants.⁴⁴ In the private sector, names and diagnoses of almost 20,000 Stanford Hospital emergency room patients were posted online after a job applicant sought help on converting the data into a bar graph.⁴⁵

Encryption of laptops containing sensitive health information, which is *de facto* required,⁴⁶ can help

prevent breaches, such as the theft of workplace computers containing sensitive data. So can disaggregation of information about participants in clinical studies and of patient data used as a sample. However, these procedures are not always followed, and there are still exceptions in the law that make some of these requirements less than mandatory.⁴⁷ Physical theft is not a new problem with EHRs, as it has long existed with paper records, but EHRs allow individual data breaches to involve thousands or millions of records, rather than the few paper records a thief can physically carry.

To be sure, a thief is most likely to value the stolen laptop for its worth as a resalable item or for personal information that has direct monetary value, such as SSNs or payment information.⁴⁸ But there are a number of entities that would find great value in the health information itself, including employers and potential employers, creditors, marketers, and health insurers.⁴⁹ Each of these entities could use the information to make decisions that affect the individual whose information is stolen, as well as the confidence of the public at large.⁵⁰ Even worse, blackmailers and paparazzi have already used celebrity and public officials' PHI for nefarious purposes. Former U.K. Prime Minister Gordon Brown alleged that The Sun newspaper illegally accessed his son's medical records and wrote a story on his cystic fibrosis.⁵¹ While a patient at the UCLA Health System, Farrah Fawcett set up a sting operation to catch one of the hospital's employees who was illegally accessing and disclosing her health information.⁵² In the case of internal leaks of celebrity PHI, especially, encryption and data storage standards will have little effect against employees who have access to the information anyway and wish to use it for unsavory reasons.⁵³

C. Impact of HIPAA

The Health Insurance Portability and Accountability Act of 1996⁵⁴ (HIPAA) was designed with both paper and electronic health records in mind. It contains provisions that require "covered entities"⁵⁵ to make electronic health information secure⁵⁶ and limit access to and disclosure of patient records.⁵⁷ HIPAA functions as a privacy floor in that it does not automatically preempt more-restrictive state

laws. Instead, when determining the privacy standard to apply in a given state, a medical practice must compare HIPAA with the relevant state law and comply with the stricter of the two.⁵⁸ While HIPAA seems like a positive development in medical records privacy and security, it has not entirely lived up to expectations. There is no private right of action to remedy a HIPAA violation, so all potential violations must be prosecuted by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).⁵⁹ Thus, there is no personal remedy for the aggrieved patient or patients whose records were used improperly.⁶⁰

Because electronic records are used more widely and for different purposes than when HIPAA was originally introduced, the HITECH Act was developed as a vehicle for updating HIPAA privacy and security rules. Under HITECH, HIPAA's rules apply directly to business associates—contractors and third parties with access to patient health information—rendering them subject to penalties for violations.⁶¹ Previously, business associates were only liable to the covered entity with whom they were contracted. HITECH also introduced new breach notification rules, whereby breaches of confidentiality involving 500 or more persons require reporting to the news media, and those involving fewer than 500 persons must be reported to HHS.⁶² EHR disclosure rules under HIPAA have been tightened by HITECH as well, so that a patient can request that disclosure of PHI be restricted in certain cases, and that such disclosure be limited to the minimum amount necessary for a given purpose.⁶³ Health care providers must also document disclosures of patient information for three years and make that information available at the patient's request.⁶⁴

Though HITECH is a positive step in HIPAA's development, it patches without solving the enforcement problem. While HITECH allows states' attorneys general to bring civil actions for violations,⁶⁵ it still does not provide a private right of action. Therefore, aggrieved patients can still do little more than report their concerns to a government entity and hope that the government follows up on the complaint.⁶⁶ Patients who either lack faith in the efficacy of this enforcement system or who seek more

control over recourse for violations of their privacy will find the HIPAA-HITECH scheme insufficient, which may in turn harm public confidence in a health information technology structure. Regulators must be vigilant and react swiftly to reports of violations if they are to instill confidence in the privacy and security of patient records.

D. Financially Motivated Resistance

Although EHR systems have the potential for greater efficiencies in the practice of medicine, many medical professionals will likely resist changing their system from the status quo absent some form of incentive. In some cases, resistance stems directly from the cost of implementation.⁶⁷ Some smaller practices are likely to balk at the size of the bill associated with installation, training, and startup of EHR systems.⁶⁸ The cost can be up to \$50,000 per clinician, and many doctors don't see the potential for much additional return on that investment.⁶⁹ The result is a wait-and-see attitude, which drags down integration among providers when some have EHR and some do not. The long-term goals of better care quality and reduced administrative burden that comes with an integrated EHR system cannot be met unless there is widespread use of EHRs.⁷⁰

To incentivize providers, the federal government has implemented financial bonuses to practices that achieve "meaningful use" of EHR.⁷¹ To achieve meaningful use, a practice must comply with a host of requirements laid out over three implementation stages.⁷² For example, eligible medical professionals must achieve twenty of twenty-five meaningful use objectives in the first stage, while hospitals must achieve nineteen of twenty-four total objectives in stage one.⁷³ Stage two, which begins in 2014, attempts to move from data collection to actually improving care. Eligible professionals must meet seventeen core requirements and three of six menu objectives, while hospitals must complete sixteen core requirements and three of six menu objectives.⁷⁴ Recommended health care policy domains include patient safety, care coordination, and efficient use of resources.⁷⁵

Those providers who meet the developing requirements can see financial incentives through Medicare and Medicaid. Medicare providers,

including physicians, podiatrists, dentists, optometrists, and chiropractors,⁷⁶ are eligible for up to \$44,000 in incentives over a period of up to five years for achieving meaningful use.⁷⁷ Under Medicaid, physicians, dentists, certified nurse midwives, nurse practitioners, and physician assistants⁷⁸ may receive up to \$63,750 over six years.⁷⁹ The flip side of this incentive program is that providers who fail to meet the meaningful use criteria by 2015 will face reimbursement *reductions*.⁸⁰ The goal of this carrot-and-stick program is to normalize the use of EHR systems so that the program reaches critical mass and integration and interoperability can be achieved among providers.⁸¹

E. Resistance to Change

Though many hospitals and practices are making the transition to EHR systems—influenced by the combination of financial incentives for achieving meaningful use of EHRs and reimbursement penalties for failure to do so—individual doctors are left with the responsibility to actually use the systems on a daily basis.⁸² As with any significant change, the shift from handwritten notes and sometimes-illegible prescriptions to comments tapped out on a keyboard and checkboxes selected on a tablet PC, has not been universally welcomed by the medical profession. Substantial change comes with the cost of unfamiliarity, and this contrast is starkest for those physicians who have been in practice for many decades.⁸³ However, while the transition may be met with resistance, and though there will be hiccups and wrinkles along the way, integrated, interoperable EHRs hold great promise once their use becomes second nature to the medical profession.

Some physicians feel that the use of EHRs cheapens the doctor-patient interaction.⁸⁴ One doctor sees the use of a laptop to take clinical notes as a barrier between her and the patient.⁸⁵ To her, the use of an electronic system of data management is not necessarily worth the costs of the transitional period.⁸⁶ Many of the concerns of physician distraction during appointments will be minimized once doctors become familiar with EHR systems, and many other worries about clunky menu searching and box checking will be reduced as EHR software is further developed and upgraded with interface concerns in

mind. As with any technological adoption, comfort and speed of use will improve over time, and along with that, the resistance to change will dissipate as use becomes normalized.⁸⁷ The transition to EHR systems was always going to encounter resistance due to human nature. However, for those doctors who enter practice in the age of EHR, as well as for the physicians who take the time to use and better understand EHR systems and their benefits, the medical profession will likely find that the change is not as arduous as once thought.⁸⁸ Indeed, another characteristic of human nature, alongside resistance to change, is adaptability to changing situations.

F. Unexpected Cost Increases

The introduction of EHRs was hailed as a way to significantly reduce medical costs. With the establishment of the Office of the National Coordinator for Health Information Technology (ONC) in 2004, President George W. Bush estimated that EHR systems could reduce healthcare costs by 20% annually.⁸⁹ Likewise, a 2005 RAND analysis predicted more than \$81 billion in annual savings.⁹⁰ Intuitively, EHRs should be able to reduce costs by streamlining care, reducing duplicative tests and procedures, and cutting out administrative costs and waste, including printing costs and physical records maintenance and storage. However, the ease of use of EHR systems can sometimes incentivize more testing and documentation, driving up costs for Medicare and private insurers, as well as those individuals who pay out-of-pocket.

Medicare reimbursements rose by \$1 billion between 2005 and 2010, driven in part by a shift in how hospitals assign billing codes to emergency room patients.⁹¹ In one case in 2009, a New York hospital reported a 43% rise in the number of ER patients requiring the highest level of care, coinciding with the hospital's introducing of EHRs.⁹² A hospital in Tennessee reported an 82% increase in the highest-coded ER patients in 2010, the year that hospital switched to EHRs.⁹³ The hospitals say that the increases are due to improved coding accuracy under the electronic system, and that they were actually underbilling before they switched to EHRs; but federal regulators are concerned that hospitals are “upcoding,” or reporting higher levels of care than

may be necessary, or even performed.⁹⁴ In a letter to several major hospital trade associations, the Obama administration expressed concern that some hospitals are using EHR systems to report a higher intensity of care or severity of patient condition without providing a corresponding improvement in care quality.⁹⁵

Payments have also risen in part due to the ease of “cloning” documentation in EHR systems. Cloning allows doctors to cut and paste exam findings and diagnoses from one patient to another through a key stroke or a button press.⁹⁶ Where doctors once had to scribble notes for each individual patient, electronic systems allow them to use past patient notes as a template, incentivizing cloning as a time-saving measure and potential tool for greater reimbursements. Some payers have begun to push back against cloning, such as Medicare contractor National Government Services, which reported to physicians that it would not pay for claims submitted with cloned documentation.⁹⁷

Another aspect of EHRs that has increased reimbursements stems from the design of the software and the incentives for a provider to use EHRs to maximize profits. Providers can set EHR systems to automatically prompt doctors to click through checklists that indicate a comprehensive patient examination has taken place, even where very few checks have been performed.⁹⁸ Systems can also be programmed to allow doctors to insert pre-created “findings” into a patient’s record using a pre-filled template.⁹⁹ While EHRs are intended to reduce the burden on physicians when completing patient records, they should not be used as a shortcut for actually performing tests. In one telling example, a patient visited a Virginia hospital with a kidney stone, and emerged with a bill that showed examinations that had not been performed.¹⁰⁰

The likely explanation is that the hospital’s EHR system included a template that automatically fills in exam information that has not necessarily been completed.¹⁰¹ While a sophisticated patient poring over his or her own records may notice such a discrepancy, a large insurance provider or Medicare contractor will not be able to check the accuracy of every bill. This will either increase the administrative costs for those payers, as they must hire additional

personnel to audit providers, or will raise the reimbursements granted to providers, in turn raising the costs of Medicare or private insurance to keep up.¹⁰²

While widespread implementation of EHR systems is likely to reduce medical costs in some ways—through better information sharing and integration, for example—the early returns have also shown the potential for increased costs in some other ways. The ease of upcoding, cut-and-paste examinations, and using templates for procedures not actually completed have dampened the cost-saving fervor of EHRs in the early going. Fortunately, these problems have been identified¹⁰³ and solutions are likely to be introduced as standards and regulations catch up to the technology.¹⁰⁴

G. Several Speed Bumps Remain

As EHRs move into the mainstream, however, they will likely become more of a target for bad actors who seek the information they contain for any number of nefarious reasons. PHI of celebrities and public figures could be used in any number of ways that would harm that person’s reputation. Where theft of medical records used to require physical intrusion into the records storage of a medical center, a determined hacker can now theoretically access a patient’s entire file using a laptop with an internet connection. It is a principle of technological development that no matter how strict the security regime is surrounding a product or software, black hats will always outpace the security fixes. EHR security schemes can only be designed to eliminate the most common kinds of intrusions and reduce the more determined ones.

These concerns should not stunt the growth of EHRs, however. Online banking is analogous to the rise of integrated EHR systems—though users are rightly worried about information security, it has not slowed the adoption of online and mobile banking.¹⁰⁵ Convenience and functionality overcome apprehension in the long run. But healthcare providers should not simply ignore security because they cannot eliminate all intrusions. There are certain “best practices” that, if followed, will create a reasonably secure records system.¹⁰⁶ Encryption of records can go a long way towards limiting

unauthorized access to patient information.¹⁰⁷ Annual security compliance assessments can alert providers to potential problem areas.¹⁰⁸ Maintaining electronic records requires administrators to keep up with current best practices in the industry.

V. THE FUTURE OF THE ELECTRONIC HEALTH REVOLUTION

The electronic health revolution is now in full throttle. Adoption rates among doctors are increasing faster each year.¹⁰⁹ Whether for better or worse, EHRs are here to stay. The federal push to achieve meaningful use, including financial incentives and penalties for noncompliance, signals that the U.S. government is fully behind the move to the electronic space.¹¹⁰ There has been a learning curve within practices that have implemented electronic systems, and indeed within the industry at large. And, even if the industry achieves 100% adoption rates in the future, all concerns about EHRs will not be allayed. Electronic records are inevitably at risk of being compromised, and issues of proper coding and reimbursement for services will need to be resolved as the technology matures. This section will reinforce both the advantages and drawbacks of the electronic health revolution before providing a brief discussion of some of the next steps that will help to improve the health IT infrastructure.

The idea of EHRs has been around for decades and systems have been in place for years, though we are still in the formative period of the technology. Slow adoption and high costs, coupled with resistance by the healthcare industry, have partially undermined the growth of EHR systems and the bounty that can come with them. The dam obstructing full implementation may finally have been broken, however, with the recent federal initiative to make the use of EHRs widespread. But although the profession has made significant strides in adoption of EHRs, there is still a large amount of work to be done before many advantages can be fully realized.

A. Multifunctional Systems

As discussed above, implementation rates of basic EHR systems have risen rapidly over the past few years. However, these systems are not necessarily “multifunctional,” which means that they are not

providing the optimal level of information integration. In fact, a recent survey found that only 27% of doctors reported their EHRs as “multifunctional.”¹¹¹ Multifunctional systems go beyond simply acting as an electronic repository for patient information; rather, it provides physicians with decision support, allowing the systems to act as an extra set of eyes.¹¹² The shortage of decision support within American EHRs is one area in which future advancements can be made. Providers that currently have EHR systems cannot be complacent—just as security improvements are a necessary part of maintaining computer systems, functionality improvements should be made over time to ensure that a provider’s EHR system is providing the appropriate level of support.¹¹³

B. Interoperable Systems

Another important aspect of EHRs that must be addressed is one that is at the core of the electronic health revolution: achieving interoperability. Many commentators speak of interoperable systems as the goal of advancements in health IT, but fail to consider how it will be achieved. Currently, there are over 700 separate vendors that make certified EHR products.¹¹⁴ While marketplace competition generally cultivates innovation, the EHR space is inundated with a dizzying array of products with proprietary user interfaces. A practitioner seeking a new EHR vendor for his or her practice will be faced with over 1750 separate products from which to choose.¹¹⁵ Not only are there simply too many options to make a fully informed choice, but several larger companies are attempting to stifle the growth of newcomers, threatening the disruptive innovation that one would hope to see in such a robust market.¹¹⁶

Too many distinct systems can be harmful to interoperability and, without some form of standardization—likely coming from the federal government or a management organization such as HIMSS—true interoperability is likely far down the road. One approach to minimizing this problem is to create a set of flexible standards rather than requiring one specific software infrastructure. In this way, vendors would be free to design their software as they see fit, but with guarantees that their systems would be able to speak with those of another

vendor.¹¹⁷ If we are to achieve the greatest promises of EHRs, we must first ensure that IT systems are able to communicate with one another.

C. Falling Costs and Increased Efficiency

As time goes on, EHR systems are likely to reduce costs in a number of ways. As the technology matures, prices for the system software would likely decrease. More importantly, the costs associated with lost time spent clicking through clunky menus will disappear as interfaces are streamlined.¹¹⁸ At the same time that EHR software is optimized, the use of EHR systems will become second nature for healthcare professionals. This will increase the input and usage speeds of EHRs, and when coupled with the coming influx of health IT data analysts,¹¹⁹ providers are likely to see a substantial increase in efficiency of use and decrease in associated costs over the long run. Over time, providers may look back at the learning curve faced during EHR adoption as trivial in comparison to the efficiency boon gained.

D. Mobile EHRs

Even as EHR systems are coming online in practices, there is already a move to use mobile devices to access and manage records. In fact, 70% of providers say that they are currently using smartphones and tablets to access their EHR software.¹²⁰ Doctors like mobile access to EHRs because it allows for more efficient use of time and easier and quicker access to patient records, especially as doctors quickly move from one exam room to another.¹²¹ With the ability to access patient information on the go, however, comes an increased risk of theft or unauthorized access of that data. Health IT professionals say that encryption and other methods of restricting access to mobile health data will be key moving forward as mobile EHRs become more widely used.¹²² However, these fears may be mitigated somewhat by the large number of practitioners who say their mobile EHR systems do not have the capability to store patient data on the device.¹²³ If mobile EHR systems do not allow for the storage of patient information, data theft will be a much smaller problem for the technology.

While many practices are already utilizing mobile EHR systems for day-to-day care activities,¹²⁴ the

next step for the platform is the development of mobile applications for use by patients.¹²⁵ These patient-oriented applications can allow patients to access test results, schedule and manage appointments, email their doctor, or seek prescription refills all from their mobile device. It is clear that mobile EHRs are only going to increase in prevalence over time given the ubiquity of mobile computing devices, and they have the potential to better integrate patient and doctor to coordinate and manage care.

E. Lingering Problems

No matter how mature the technology becomes, there are certain issues with EHRs that will not easily go away. Patients as a class will likely become more comfortable with their records being in electronic form as time goes on, mitigating the privacy issue. However, concerns about records security will endure long after electronic records become the norm. Just as our societal comfort with the internet as a do-all tool has not meant we are any safer from hackers,¹²⁶ neither will 100% adoption of EHRs in the medical profession mean that our information is any safer than before. Data security will always require vigilance on the part of the providers who maintain EHRs.

Another issue that will endure long after EHRs mature is that of data stability and crashes. Reliability of purely-electronic systems is a sticking point in the developing electronic economy, and storing patient data not only on computer servers but at times offsite in the cloud means that, if something goes wrong in the system, access will be severely limited if not cut off entirely. Provider networks must be prepared to function without electronic access in case of an emergency. The Mayo Clinic, for example, has backup measures in place in the event of an EHR failure, including the ability to call for rapid system repairs and even to revert to paper records if necessary.¹²⁷ Just as it is impossible to protect a system fully from unwanted intrusions, it is impossible to make a system crash proof. Providers must therefore maintain a Plan B in case a system goes down. The “electronic” aspect of the electronic health revolution means that the same problems that affect all technologies will linger.

VI. CONCLUSION

The road traveled by the electronic health revolution has not been entirely smooth. Though there are numerous substantial benefits to fully integrated EHR systems, a number of drawbacks remain. Some, like patient comfort with privacy issues, will likely dissipate somewhat over time. Others, like protection from security risks, will require perpetual vigilance for system operators. Still, despite the growing pains faced by the healthcare industry as it moves to full adoption of EHRs and related health information technologies, the long term benefits seen by the transition are likely to greatly outweigh the negatives. Improved quality of care and reduced medical errors alone will overshadow the existing drawbacks. Time will tell, however, whether the electronic health revolution will progress smoothly over the coming years and whether the dream of an interoperable EHR infrastructure will be realized.

¹ *Electronic Health Record*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, <http://www.himss.org/library/ehr/?navItemNumber=13261> (last visited Mar. 22, 2013).

² Peter Garrett and Joshua Seidman, *EMR vs EHR—What is the Difference?*, HEALTH IT BUZZ (Jan. 4, 2011), <http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/>.

³ *Id.*

⁴ *Id.*

⁵ Jim Atherton, *Development of the Electronic Health Record*, 13 AMERICAN MEDICAL ASSOC. J. OF ETHICS v. 3, 186, at 187 (2011), available at <http://virtualmentor.ama-assn.org/2011/03/pdf/mhst1-1103.pdf>.

⁶ See *id.* (stating that Vista “is consistently well reviewed for reducing medical errors and improving health-record component integration”).

⁷ Dustin Charles, Michael Furukawa, & Meghan Hufstader, ELECTRONIC HEALTH RECORD SYSTEMS AND INTENT TO ATTEST TO MEANINGFUL USE AMONG NON-FEDERAL ACUTE CARE HOSPITALS IN THE UNITED STATES: 2008-2011, OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, ONC DATA BRIEF No. 1, 4 (2012), available at http://www.healthit.gov/media/pdf/ONC_Data_Brief_AHA_2011.pdf.

⁸ See *id.* (finding that the large jump is mostly attributable to the federal government’s push to adoption of EHRs by using Medicare and Medicaid payment incentives).

⁹ See John Hazewinkel, *Digital Health Care Reform Under the HITECH Act*, 90 Mich. B.J. 33, 34 (2011) (explaining how the health care industry lags behind other industries in its use of information technology for its core business, i.e., clinical care, while it is used extensively for other functions, such as processing claims for payment).

¹⁰ Mary Mosquera, *Indian Health Service Creates PHR System*, GOVERNMENTHEALTHIT (Oct. 29, 2012), <http://www.govhealthit.com/news/indian-health-service-creates-phr-system>.

[govhealthit.com/news/indian-health-service-creates-phr-system](http://www.govhealthit.com/news/indian-health-service-creates-phr-system).

¹¹ *Health Information Exchange*, HEALTHIT.GOV, <http://www.healthit.gov/providers-professionals/health-information-exchange> (last visited Mar. 7, 2013).

¹² The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as Title XIII of the American Recovery and Reinvestment Act (ARRA) of 2009, Pub. L. 111-5, 123 Stat. 226 (2009).

¹³ Health Information Exchanges Part 1: The Basics 55, HEALTHCARE INFORMATION MANAGEMENT SYSTEMS SOCIETY, available at http://www.himss.org/content/files/HIMSS_HIE_Presentation_HIE_TheBasics.pdf.

¹⁴ See Dan Bowman, *HIE Critical to Care Continuity in Natural Disasters*, FIERCEHEALTHIT (Nov. 2, 2012), <http://www.fiercehealthit.com/story/health-information-exchange-critical-care-continuity-natural-disasters/2012-11-02>.

¹⁵ *Id.*

¹⁶ 42 U.S.C. § 201 et. seq., Pub. L. 109-41, 119 Stat. 424 (2005).

¹⁷ *Welcome to AHRQ’s Patient Safety Organization Web Site*, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, <http://www.pso.ahrq.gov/> (last visited Oct. 25, 2012).

¹⁸ *What is a Patient Safety Organization (PSO)?*, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, <http://www.pso.ahrq.gov/psos/overview.htm> (last visited Mar. 7, 2013).

¹⁹ See 42 C.F.R. § 3.102(b) (including having “appropriately qualified workforce members” and not qualifying as a “health insurance issuer”).

²⁰ *Alphabetical Directory of Listed Patient Safety Organizations*, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, <http://www.pso.ahrq.gov/listing/alphabetist.htm> (last visited Mar. 7, 2013).

²¹ Pub. L. 111-148, 124 Stat. 119 (2010).

²² *Resources for Reducing Unnecessary Hospital Readmissions*, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, <http://www.pso.ahrq.gov/readmin/readminres.htm#tools> (last visited Mar. 7, 2013).

²³ Mary Reed, et al., *Outpatient Electronic Health Records and the Clinical Care and Outcomes of Patients With Diabetes Mellitus*, ANNALS OF INTERNAL MEDICINE (Oct. 2, 2012), available at <http://www.ncbi.nlm.nih.gov/pubmed/23027319>.

²⁴ Ann Kutney-Lee & Deena Kelly, *The Effect of Hospital Electronic Health Record Adoption on Nurse-Assessed Quality of Care and Patient Safety*, 41 J. OF NURSING ADMIN. 11, 466, available at <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3236066/>.

²⁵ See Ed Susman, *EMR Cuts Rx Errors for HIV Hospital Patients*, MEDPAGE TODAY, Oct. 20, 2012, http://www.medpagetoday.com/MeetingCoverage/IDWeek/35442?utm_content=&utm_medium=email&utm_campaign=DailyHeadlines&utm_source=WC&xid=NL_DHE_2012-10-22&eun=g419441d0r&userid=419441&email=mdhirsch@comcast.net&mu_id=5518887 (noting that a lack of familiarity with complex antiretroviral regimens was the main cause of medical error before implementing electronic systems).

²⁶ Andrew Klein, *Newer Electronic Health Record Systems Reduce Rx Errors, but Doctors Find the Switch Difficult*, WEILL CORNELL MEDICAL COLLEGE (May 26, 2011),

available at http://weill.cornell.edu/news/releases/wcmc/wcmc_2011/05_25_11.shtml.

²⁷ See Ken Terry, *Electronic Checklists Help Prevent Medical Errors*, INFORMATION WEEK (Oct. 19, 2012), available at <http://www.informationweek.com/healthcare/patient/electronic-checklists-help-prevent-medic/240009348> (noting that handwritten medication histories have more errors than electronically recorded entries).

²⁸ *Id.*

²⁹ Neil Versel, *CDC Sees EHRs as Public Health 'Game Changer'*, INFORMATION WEEK (Apr. 6, 2011), available at <http://www.informationweek.com/healthcare/interoperability/cdc-sees-ehrs-as-public-health-game-chan/229401061>.

³⁰ See *id.*

³¹ See, e.g., *supra* notes 23-27.

³² Systems that are able to “speak” with one another are the ultimate goal of EHRs, but before systems can communicate, they have to be implemented in the first place. If a patient’s specialist seeks the records from a PCP, but that PCP doesn’t have electronic records at all, electronic distribution is impossible. There’s no way to get interoperability without first implementing the infrastructure.

³³ A Harris Interactive poll recently found that 63% of Americans fear that a hacker will steal their personal data used in EHRs, a decrease of only 1% from 2010. The same study found that 85% of Americans have “some kind” of EHR anxiety, including fear of information loss, damage, or corruption. See Robert Lowes, *Fear of Data Theft Blunts Public Acceptance of EHRs*, MEDSCAPE (Aug. 24, 2012), <http://www.medscape.com/viewarticle/769778>.

³⁴ One doctor theorized that the shift to EHRs is being resisted because it takes away some of the humanity—and, likely, some autonomy—associated with a purely face-to-face interaction. See Richard Reese, *Why Doctors Don't Like Electronic Health Records*, THE HEALTH CARE BLOG (Oct. 7, 2011), <http://thehealthcareblog.com/blog/2011/10/07/why-doctors-dont-like-electronic-health-records/#more-32729> (“You cannot look a computer in the eye. You cannot read its body language. You cannot talk to an algorithm. You cannot sympathize or empathize with it. . . . We choose not to be reduced to data-entry clerks sorting through undigested computer bytes.”).

³⁵ See Fred Schulte, *Growth of electronic medical records eases path to inflated bills*, CENTER FOR PUBLIC INTEGRITY (Sept. 19, 2012), <http://www.publicintegrity.org/2012/09/19/10812/growth-electronic-medical-records-eases-path-inflated-bills> (“Interviews with hospital administrators, doctors and health information technology professionals confirmed that digital billing gear often prompts higher coding, though many in the medical field argue that they are simply recouping money that they previously failed to collect.”).

³⁶ See Emily Badger, *Can Privacy, Electronic Medical Records Coexist?*, PACIFIC STANDARD (June 15, 2011), <http://www.psmag.com/health/can-health-privacy-electronic-medical-records-coexist-32350/> (suggesting that privacy concerns could be the biggest hindrance to widespread implementation of electronic health records).

³⁷ *Patients Fear EHRs Increase Chances for Medical Data to be Stolen*, ATLANTICON (Sept. 5, 2012), <http://www.atlanticon.net/blog/2012/09/05/patients-fear-ehrs-increase-chances-for-medical-data-to-be-stolen/>.

³⁸ Anne Zeiger, *Patients might leave your practice if they fear EHR data isn't secure*, EHR OUTLOOK, http://www.ehroulook.com/trends/Patients-might-leave-your-practice-if-they-fear-EHR-data-isnt-secure_182.html (last visited Nov. 2, 2012).

³⁹ In fact, a 2007 WSJ/Harris Interactive Poll found that even at that early stage in EHR development, most respondents agreed that improved information sharing via electronic systems would improve care and 63% agreed that sharing of such records could decrease medical errors. However, about one-quarter of adults were unsure about the benefits of EHRs. See Beckey Bright, *Benefits of Electronic Health Records Seen as Outweighing Privacy Risks*, WALL ST. J., Nov. 29, 2007, <http://online.wsj.com/article/SB119565244262500549.html>.

⁴⁰ Patient transfers are another area in which record sharing is necessary to improve safety and coordination. Think of a patient who was recently treated for congestive heart failure and has been discharged to a nursing home. Medical care does not stop at the door—rather, the nursing home staff will need the patient’s records in order to make the discharge transition as safe as possible. See Paul Cerrato, *National Health Information Exchange: Why the Delay?*, INFORMATION WEEK (Nov. 5, 2012), <http://www.informationweek.com/healthcare/interoperability/national-health-information-exchange-why/240044378>.

⁴¹ A “perfectly secure” computer would require that no user could access the data held within it. Likewise, a perfectly accessible computer would have no way of preventing access by anyone. The balancing maneuver requires determining an acceptable location on the continuum between the two for a given purpose. See Michelle McNickle, *4 Best Practices: Combat Health Data Breaches*, INFORMATION WEEK (Nov. 1, 2012), <http://www.informationweek.com/healthcare/security-privacy/4-best-practices-combat-health-data-brea/240012739> (“[D]ata is liquid; it needs to move around so much that it’s impossible to completely eliminate breaches.”) (statement of Doug Pollack, chief strategy officer at ID Experts).

⁴² Less well-known is that nearly 20 million patient records have been compromised within the past two years alone. See *id.*

⁴³ Susan R. Gering, *Electronic Health Records: How to Avoid Digital Disaster*, 16 MICH. ST. U. J. MED. & L. 297, 309 (2012).

⁴⁴ Rick Weiss & Ellen Nakashima, *Stolen NIH Laptop Held Social Security Numbers*, WASH. POST, Apr. 10, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/09/AR2008040903680.html>.

⁴⁵ Darius Tahir, *Can Electronic Medical Records Improve Our Health Without Jeopardizing Our Privacy?*, THE NEW REPUBLIC, Nov. 25, 2011, <http://www.tnr.com/blog/jonathan-cohn/97801/electronic-medical-records-privacy-stanford>.

⁴⁶ See Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,741-42,742 (Aug. 24, 2009) (to be codified at 45 C.F.R. 160) (“[I]f a covered entity chooses to encrypt protected health information to comply

with the Security Rule, does so pursuant to this guidance, and subsequently discovers a breach of that encrypted information, the covered entity will not be required to provide breach notification. . . . [I]f a covered entity has decided to use a method other than encryption. . . . that is not specified in this guidance to safeguard protected health information. . . . following a breach of this information, the covered entity would have to provide breach notification to affected individuals.”).

⁴⁷ See *id.* (“[B]ecause these are addressable implementation specifications, a covered entity may be in compliance with the Security Rule even if it reasonably decides not to encrypt electronic protected health information and instead uses a comparable method to safeguard the information.”).

⁴⁸ See VERIZON, DBIR INDUSTRY SNAPSHOT: HEALTHCARE 1 (2012), available at http://www.verizonbusiness.com/resources/reports/rp_dbir-industry-snapshot-healthcare_en_xg.pdf (“The vast majority of attackers seek information from which they can directly or indirectly profit. This includes personal and payment information. . . .”).

⁴⁹ See Gering, *supra* note 43, at 310–11.

⁵⁰ See Badger, *supra* note 36 (“The associated dangers aren’t just about privacy on principle. An insurance company that learns of a particular illness might decline to cover you. An employer who realizes that your costly medical condition is weighing down the group health plan might find other cause to fire you.”).

⁵¹ Jennifer Dennard, *Personal Health Information and the Rupert Murdoch Effect*, HEALTHCARE IT NEWS, July 13, 2011, <http://www.healthcareitnews.com/blog/personal-health-information-and-rupert-murdoch-effect>.

⁵² *Id.* (listing Britney Spears and Maria Shriver as among the list of celebrity patients that have been targets of unauthorized leaks of protected health information).

⁵³ See VERIZON, *supra* note 48, at 2 (“Insider jobs [are] much less frequent, but they can’t be ignored. When employees do go rogue, their ready access to and knowledge of information assets means they can do quite a bit of damage without expending a lot of effort.”).

⁵⁴ Pub. L. 104-191, 110 Stat. 1936 (1996).

⁵⁵ See 45 C.F.R. § 160.103 (A “covered entity” is either (1) a health plan, (2) a health care clearinghouse, or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the regulations).

⁵⁶ See 45 C.F.R. §§ 164.306-18.

⁵⁷ See 45 C.F.R. §§ 164.502-10.

⁵⁸ *Does the HIPAA Privacy Rule Preempt State Laws?*, HHS.gov, available at <http://www.hhs.gov/hipaafaq/state/399.html> (last visited Nov. 3, 2012) (noting that the Privacy Rule does not preempt state laws where a state law “relates to the privacy of individually identifiable health information and provides greater privacy protections or privacy rights with respect to such information.”).

⁵⁹ See *Acara v. Banks*, 470 F.3d 569, 571 (5th Cir. 2006) (“HIPAA does not contain any express language conferring privacy rights upon a specific class of individuals. Instead, it focuses on regulating persons that have access to individually identifiable medical information and who conduct certain electronic health care transactions. . . .

HIPAA limits enforcement of the statute to the Secretary of Health and Human Services.”).

⁶⁰ See *Case Examples and Resolution Agreements*, HHS.gov, available at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html> (last visited Nov. 3, 2012) (highlighting a number of settlements and resolution agreements with HIPAA violators).

⁶¹ *What Changes in HIPAA Compliance Requirements Were Made by the HITECH Act?*, HRSA.gov, available at <http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/compliancereqs.html>.

⁶² Hazewinkel, *supra* note 9, at 35.

⁶³ *What changes in HIPAA compliance requirements were made by the HITECH Act?*, *supra* note 61.

⁶⁴ *Id.*

⁶⁵ Hazewinkel, *supra* note 9, at 35.

⁶⁶ See, e.g., *Health Information Privacy Complaint*, DEPT. OF HEALTH AND HUMAN SVCS., OFFICE FOR CIVIL RIGHTS, available at <http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf> (An aggrieved individual must fill out the HHS form and file it with the appropriate OCR regional office within 180 days from when the individual learned of the grievance); see also *How to File a Complaint*, U.S. DEP’T OF HEALTH & HUMAN SERVS., <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html> (last visited Mar. 26, 2013).

⁶⁷ Perhaps somewhat ironically, 69% of physicians participating in a survey conducted by the Bipartisan Policy Center said that electronic information exchange will improve efficiencies in their practices. Thus, many doctors recognize the longer-term advantages of electronic systems, but the startup costs are still a barrier for some. See BIPARTISAN POLICY CENTER HEALTH INFORMATION TECHNOLOGY INITIATIVE, CLINICIAN PERSPECTIVES ON ELECTRONIC HEALTH INFORMATION SHARING FOR TRANSITIONS OF CARE 12 (2012), available at [http://bipartisanpolicy.org/sites/default/files/Clinician%20Survey_format%20\(2\).pdf](http://bipartisanpolicy.org/sites/default/files/Clinician%20Survey_format%20(2).pdf); see also *id.* at 13 (indicating that the same survey also revealed that 69% of respondents saw the cost of setting up and maintaining interfaces and exchanges as a major barrier to clinical information sharing).

⁶⁸ Gering, *supra* note 43, at 311–12.

⁶⁹ Lena H. Sun, *Despite Incentives, Doctors Are Wary About Switching to Electronic Health Records*, WASH. POST, Mar. 14, 2011, http://articles.washingtonpost.com/2011-03-14/national/35207018_1_electronic-records-doctors-computerized-records.

⁷⁰ The Bipartisan Policy Center survey found that 80% of clinicians surveyed felt that HIE will improve care quality, and 80% also said HIE would improve coordination. See Bipartisan Policy Center, *supra* note 67, at 12.

⁷¹ See *Electronic Health Record (EHR) Incentive Program FAQs*, CENTERS FOR MEDICARE AND MEDICAID SERVICES, available at <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/FAQsRemediatedandRevised.pdf> (last visited Nov. 2, 2012).

⁷² Stage 1 involves “data capture and sharing”; Stage 2 encompasses “advanced clinical processes”; and Stage 3 seeks “improved outcomes”. *Meaningful Use Definition & Objectives, EHR Incentives & Certification*, HEALTHIT.gov, available at [Spring 2013](http://www.healthit.gov/providers-</p></div><div data-bbox=)

professionals/meaningful-use-definition-objectives (last visited Oct. 15, 2012).

⁷³ See *Meaningful Use*, CENTERS FOR MEDICARE AND MEDICAID SERVICES, available at http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html.

⁷⁴ Patrick Ouellette, *Stage 2 Meaningful Use Checklist*, EHR INTELLIGENCE, Sept. 20, 2012, available at <http://ehrintelligence.com/2012/09/20/stage-2-meaningful-use-checklist/>.

⁷⁵ *Id.*

⁷⁶ American Recovery and Reinvestment Act of 2009 § 4101(a), 42 U.S.C. § 1395w-4(o)(5)(C) (2010).

⁷⁷ *Medicare Electronic Health Record Incentive Program for Eligible Professionals*, CENTERS FOR MEDICARE AND MEDICAID SERVICES (Nov. 2010), available at <http://www.documentcloud.org/documents/71331-tip-sheet-medicare-ehr-incentive-payments-for.html>.

⁷⁸ American Recovery and Reinvestment Act of 2009 § 4201(a)(2), 42 U.S.C. 1396b(t)(3)(B) (2010).

⁷⁹ *Medicaid Electronic Health Record Incentive Payments for Eligible Professionals*, CENTERS FOR MEDICARE AND MEDICAID SERVICES (Nov. 2010), available at <http://www.documentcloud.org/documents/71332-tip-sheet-medicare-electronic-health-records.html>.

⁸⁰ Hazewinkel, *supra* note 9, at 34.

⁸¹ See Bipartisan Policy Center, *supra* note 67, at 12 (noting that clinicians have cited financial incentives as one main reason for their adoption of EHR systems--in the Bipartisan Policy Center survey, 72% of respondents said that adoption of HIE technology would have a positive impact on their ability to participate in incentive programs).

⁸² In the months following EHR adoption in a practice, doctors tend to see fewer patients and work longer hours. Many vendors suggest scheduling only 50% of patient capacity for the few weeks following EHR implementation to account for the learning curve. See Michael McBride, *Time check: Physicians see fewer patients as they implement EHRs*, MEDICAL ECONOMICS, June 10, 2012, <http://www.modernmedicine.com/modernmedicine/article/articleDetail.jsp?id=776741>.

⁸³ See Olga Khazan, *For some doctors, electronic records aren't a miracle cure*, WASH. POST, Nov. 5, 2012, available at http://www.washingtonpost.com/national/health-science/for-some-doctors-electronic-records-arent-a-miracle-cure/2012/11/05/f12c3400-f1fb-11e1-a612-3cfc842a6d89_story.html ("Older physicians are less likely to use digital records, in part because . . . they've accumulated mounds of charts and aren't sure they'll be practicing long enough to make transitioning to a new system worthwhile.").

⁸⁴ The Center for Studying Health System Change found that, although doctors typically agree that EHRs will aid overall doctor-patient interaction (through the use of e-mails and the ability to pull up important patient information on the spot), many are concerned that interpersonal communication will suffer as a result of EHRs, particularly due to distractions in the software and because EHRs mean doctors, ironically, need to ask fewer questions of a patient during a visit. See Ann S. O'Malley, Genna R. Cohen & Joy M. Grossman, *Issue Brief: Electronic Medical Records and Communication with Patients and Other Clinicians:*

Are We Talking Less?, CENTER FOR STUDYING HEALTH SYSTEM CHANGE 2 (Apr. 2010), available at <http://www.hschange.com/CONTENT/1125/1125.pdf>.

⁸⁵ Anne Marie Valinoti, *Physician, Steel Thyself for Electronic Records*, WALL ST. J., Oct. 22, 2012, <http://online.wsj.com/article/SB10000872396390443675404578058480752741280.html>.

⁸⁶ *Id.*

⁸⁷ Changes as small as a website's user interface refresh or as large as the switch to an entirely different operating system will often invoke the same type of rejection at first, though any well-planned transition will ultimately be accepted as its merits are understood and users spend more time interacting with the new system.

⁸⁸ See Fred Schulte, *Switch to electronic records getting mixed reviews at hospitals and clinics*, CENTER FOR PUBLIC INTEGRITY (Nov. 24, 2009), <http://www.publicintegrity.org/2009/11/24/7011/switch-electronic-records-getting-mixed-reviews-hospitals-and-clinics> ("[M]ost doctors who have taken the plunge would never go back to pen and paper and [. . .] that those who are reluctant will come around.").

⁸⁹ Jaan Sidorov, *It Ain't Necessarily So: The Electronic Health Record And The Unlikely Prospect Of Reducing Health Care Costs*, 25 HEALTH AFFAIRS 1079, 1079 (2006) (citing *Office of the National Coordinator for Health Information Technology*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (May 23, 2005), <http://www.hhs.gov/healthit/valueHIT.html>).

⁹⁰ *Id.* at 1080.

⁹¹ Reed Abelson, et al., *Medicare Bills Rise as Records Turn Electronic*, N.Y. TIMES, Sept. 22, 2012, at A1.

⁹² *Id.*

⁹³ *Id.*

⁹⁴ See Reed Abelson & Julie Creswell, *U.S. Warning to Hospitals on Medicare Bill Abuses*, N.Y. TIMES, Sept. 25, 2012, at B1.

⁹⁵ *Id.*

⁹⁶ See Abelson, et al., *supra* note 91, at A1.

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² HHS has already announced it will step up audits of Medicare patients' hospital bills where EHRs are involved, looking out for instances of upcoding. See Schulte, *supra* note 35.

¹⁰³ Critics of the Medicare program's approach to EHRs say that not only did CMS fail to anticipate the rise in reimbursement rates, but that "meaningful use" incentive payments have also been improperly overseen, and that the program lacks appropriate safeguards. See Reed Abelson, *Medicare is Faulted on Shift to Electronic Records*, N.Y. TIMES, Nov. 29, 2012, http://www.nytimes.com/2012/11/29/business/medicare-is-faulted-in-electronic-medical-records-conversion.html?adxnnl=1&adxnnlx=1355253387-Kwwu6bNby4NDJqAIYr6Gng&_r=0.

¹⁰⁴ In the wake of the reimbursement rate controversy, the American Hospital Association wrote a letter to Secretary Sebelius and Attorney General Holder seeking the creation of guidelines on hospital coding. See Letter

from Rich Umbdenstock, AHA President and CEO, to Kathleen Sebelius, HHS Secretary, and Eric Holder, U.S. Attorney General (Nov. 12, 2012), available at <http://www.ihealthbeat.org/articles/2012/11/15/aha-to-work-with-officials-to-curb-use-of-ehrs-for-upcoding.aspx>.

¹⁰⁵ *Global Mobile Banking Customer Base to Reach 1.1 Billion by 2015, According to New Report by Global Industry Analysts, Inc.*, GLOBAL INDUSTRY ANALYSTS (Feb. 16, 2010), <http://www.prweb.com/releases/2010/02/prweb3553494.htm>.

¹⁰⁶ Though there are no government-standard best practices in the Health IT realm, there are a number of private organizations that have identified key aspects of a secure EHR system. See, e.g., Kathleen Roney, *5 Best Practices for Improving Data Security*, BECKER'S HOSPITAL REVIEW (May 9, 2012), <http://www.beckershospitalreview.com/healthcare-information-technology/5-best-practices-for-improving-data-security.html> (listing risk assessments, tailored data protection, employee training, upgraded data loss protection tools, and thinking outside the box as five key practices to reinforce records security).

¹⁰⁷ See McNickle, *supra* note 41.

¹⁰⁸ See *id.*

¹⁰⁹ Most recently, a Commonwealth Fund study found that 69% of PCPs in the U.S. reported using EHRs in 2012. See Cathy Schoen, et al., *A Survey Of Primary Care Doctors In Ten Countries Shows Progress In Use Of Health Information Technology, Less In Other Areas*, 10 HEALTH AFFAIRS 1377 (2012).

¹¹⁰ Indeed, in response to a letter from House Republicans in October 2012, Secretary Sebelius said that "suspending the incentive program, arguing that it 'would be profoundly unfair to the hospitals and eligible professionals that have invested billions of dollars and devoted countless hours of work to purchase and install systems and educate staff,'" signaling that the Department is fully behind the move. See Abelson, *supra* note 91.

¹¹¹ Ken Terry, *EHR Adoption: U.S. Remains a Slowpoke*, INFORMATION WEEK, Nov. 15, 2012, <http://www.informationweek.com/healthcare/electronic-medical-records/ehr-adoption-us-remains-the-slow-poke/240142152>.

¹¹² "To measure EHR capabilities, the researchers asked physicians about electronic functions in four categories: The generation of patient information, such as lists of patients' medications; the generation of patient registry and panel information, such as a list of patients due for preventive care; order entry management, such as electronic prescribing; and decision support, such as alerts about potential adverse drug interactions. To be counted as a user of a multifunctional EHR, a practice had to report that its system had at least two functions in each of these four domains." *Id.*

¹¹³ See Paul Cerrato, *5 Healthcare IT Resolutions for 2013*, INFORMATION WEEK, Dec. 10, 2012, <http://www.informationweek.com/healthcare/cpoe/5-healthcare-it-resolutions-for-2013/240144068>.

¹¹⁴ Kenneth D. Mandl & Isaac S. Kohane, *Escaping the EHR Trap: The Future of Health IT*, 366 NEW ENGLAND J. OF MEDICINE 2240, 2241 (2012), available at <http://www.nejm.org/doi/full/10.1056/NEJMp1203102>.

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ See *id.* at 2242 ("[T]he ONC-initiated Direct Project promotes a secure communications system for health care based on SMTP (Simple Mail Transfer Protocol), the decades-old store-and-forward email standard. The Direct Project exemplifies the way in which highly effective general technologies can be adapted to health care in an open, standard, integratable fashion.").

¹¹⁸ See Milt Freudenheim, *The Ups and Downs of Electronic Medical Records*, N.Y. TIMES, Oct. 8, 2012, <http://www.nytimes.com/2012/10/09/health/the-ups-and-downs-of-electronic-medical-records-the-digital-doctor.html>.

¹¹⁹ See Cerrato, *supra* note 113 ("[W]ith the push to do more big data analytics and get started in population health management, top-flight analysts are no longer a 'nice-to-have' but a must-have.").

¹²⁰ Anthony Vecchione, *9 Mobile EHRs Fight for Doctors' Attention*, INFORMATION WEEK, Dec. 12, 2012, <http://www.informationweek.com/healthcare/electronic-medical-records/9-mobile-ehrs-fight-for-doctors-attention/240144143>.

¹²¹ *Mobile EHRs-An Overview*, EXCITE HEALTH PARTNERS (Nov. 30, 2012), <http://www.excitehealthpartners.com/news/mobile-ehrs-an-overview/>.

¹²² *Id.*

¹²³ *HIMSS Analytics Survey Demonstrates Widespread Use of Mobile Devices to Support Patient Care Activities*, HIMSS ANALYTICS (Dec. 3, 2012), <http://www.himssanalytics.org/about/NewsDetail.aspx?nid=81558> ("83 percent of IT professionals noted the devices used by their clinicians do not retain patient-specific information.").

¹²⁴ These activities, as noted in the HIMSS Analytics survey, include bedside data collection (45% of respondents); use of bar code reader on mobile devices (38%); monitoring data from medical devices (34%); and capturing visual representation of patient data (27%). *Id.*

¹²⁵ The HIMSS Analytics survey found that, while mobile EHR use is widespread for clinical activities, only 13% of respondents said their practice had created an app for patient use. *Id.*

¹²⁶ If anything, the ubiquitous nature of the internet means that we are more susceptible to identity theft, as normalcy breeds complacency and a greater number of theft-enticing services are accessed online now than ever before.

¹²⁷ See Freudenheim, *supra* note 118.

