INTRODUCTION

“The passage of the Patient Protection and Affordable Care Act of 2010 marks a new era in American health care. Yet in many ways, this era began more than a year earlier, with the passage of the American Recovery and Reinvestment Act (ARRA) of 2009 and its Health Information Technology for Economic and Clinical Health (HITECH) provisions. Although HITECH may be viewed narrowly as legislation to stimulate the adoption of health information technology . . . , it is better understood as an essential foundation for our broader efforts to restructure health care delivery.”

How should we reform our healthcare system? The public debates are endless and mostly focus on the expansion of coverage. Yet as conceived by HITECH, the collection and exchange of patient data through health information technology (HIT) offers enormous opportunities to improve the quality of care and reduce costs. HITECH laid the groundwork for a new patient data ecosystem through the adoption of electronic health records (EHRs) and the creation of a national health information exchange (HIE). (HIT also introduces a new set of acronyms.) This article explores the EHR/HIT ecosystem; the privacy and security risks and protections for electronic patient data under the Health Information Portability and Accountability Act (HIPAA), as amended by HITECH; and some of the legal issues for EHRs and HIEs related to contracting, privacy and security, fraud, and malpractice. There is also a final word about the use of software and applications on mobile devices (mHealth) within this new ecosystem.

As lawyers, HIT issues affect many of our clients: physicians and other healthcare providers; healthcare payors (including employers with respect to their employee benefit

1 Lisa W. Clark is a partner in the Health Law Practice Group of Duane Morris LLP in its Philadelphia, PA office. Erin M. Duffy, Esq., Melissa Sobel Snyder, Esq. and Ashley Maguire, Third Year Law Student, Drexel University School of Law, substantially contributed to this article.

2 42 U.S.C. §§300j-1 et seq.; §§17901 et seq.

3 Melinda Beeuwkes Buntin, Sachin H. Jain and David Blumenthal, Health Information Technology: Laying The Infrastructure For National Health Reform, Health Affairs, 29, no. 6 (2010): 1214-1219.

4 45 C.F.R. Parts 160, 162, & 164.

5 HIT offers enormous benefits with respect to other aspects of the healthcare system such as claims and billing; research; personalized medicine; and the distribution of supplies.
plans); technology companies; businesses that collect and share health data for billing, advertising and other purposes; and of course individuals. Depending on the HIT issue that crosses your desk, consider whether you need to understand the technology; many lawyers are not well versed in this area. Also note that the law on HIT is not well developed, and that the ecosystem changes minute-by-minute. So consider HIT a brave, exciting new frontier—and ask for expert help where needed.

**PRIVACY AND SECURITY OF PATIENT DATA IN THE HIT ECOSYSTEM/HIPAA**

The HIT ecosystem is built on patient data. Each visit to the physician or the hospital creates reams of personal data, much of which is being collected, stored and transmitted electronically. Whether or not we can expect privacy anymore, there are important laws in place to try to protect our health information and give us rights to keep confidential mental health, substance abuse and other highly sensitive data. The best-known law in this area is HIPAA. HIPAA was refined for the digital age by HITECH in two key areas: by expanding the definition of Business Associates and by adding new breach response provisions. Last year, the U.S. Department of Health and Human Services’ (“HHS”) Office of Civil Rights issued the final omnibus rule under HITECH amending the HIPAA regulations.6

A very brief primer on HIPAA: HIPAA safeguards protected health information (PHI) through its privacy requirements and security standards. The law applies to most health care providers, payors (including most employer group health plans known as group health plans (GHPs)) and clearinghouses like billing companies (collectively, Covered Entities) and their Business Associates, those direct subcontractors, vendors and agents that handle PHI. The HIPAA privacy provisions provide rights to healthcare consumers such as the right to receive a Notice of Privacy Practices explaining a Covered Entity’s privacy practices. HIPAA also defines the circumstances under which Covered Entities and Business Associates may share PHI without patient authorization, for instance for treatment purposes or as required by law, and imposes administrative requirements like training and sanctions on these entities. Your employer client whose benefits program qualifies as a GHP must fulfill all of these requirements.

HIPAA also imposes security standards on the use and disclosure of electronic PHI (ePHI), which is central to HIT. These standards require Covered Entities and Business Associates to perform risk analyses, address any risk gaps, implement an emergency data management plan, and conduct audits, among others.7 It is a myth that HIPAA “requires” encryption, but HHS does require entities to consider whether it is feasible. HHS takes security compliance very seriously. HHS’s OIG 2014 Workplan announced that one of its target areas is the security of portable devices “such as laptops, jump drives, backup tapes, and equipment considered for disposal.”8 Last year, HHS’s Office of the Inspector General (OIG) fined a health plan for failing to erase PHI on photocopiers.9 HHS’s website includes an audit protocol that HHS uses in investigating violations.10 The audit protocol is an excellent tool for demonstrating compliance. If HHS were to knock at the door to investigate a security issue, the first question would be: “Did you implement and do you follow the audit protocol?” This is a question that counsel should ask clients that are subject to HIPAA.

Counsel that negotiate Business Associate Agreements should also know that the definition of a Business Associate has significantly expanded to apply to the universe of entities that handle PHI on behalf of a Covered Entity.11 First, the definition of a Business Associate is any entity that creates, receives, maintains or transmits PHI on behalf of a Covered Entity or a

---

7 45 C.F.R. Parts 160 and 164, Subpart C.
9 See http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html.
11 See 45 C.F.R. §§164.308(b); 164.502(e); 164.504(e).
Business Associate. This means that a subcontractor of a Business Associate that handles PHI, and that subcontractor’s sub-contractor that handles PHI, etc., etc., now qualify as Business Associates.

Second, the new definition specifically applies to HIT vendors and consultants, such as an EHR consultant; a data storage entity; a software vendor; a mobile health vendor; or a data transmission organization. Finally, the definition of a Business Associate also includes a personal health record (“PHR”) vendor of a Covered Entity, like the patient portal available on a hospital’s website.

The net effect of the expanded definition of a Business Associate is to explode the number of Business Associates, many of which may be unaware of their new status. For instance, a data storage provider may offer services to store ePHI on behalf of a health care billing company. Or, a web designer may provide services to a consultant assisting a nursing home in implementing an EHR. Typically, the Business Associate Agreement arrives in the mail with instructions to sign. It is critical that the erstwhile Business Associate closely review the document, including with reference to the underlying services agreement before execution. Note that indemnification is not required under HIPAA. A misstep by a sub-Business Associate may create unsuspecting costs and liabilities for the Covered Entity or upstream Business Associate, particularly with respect to a data breach.

Data breaches are front and center to HIPAA enforcement and to EHRs. HITECH introduced new requirements to report data breaches to individuals and the government, and for large breaches, to the media. But note that there is a safe harbor for breach reporting when data has been secured. HHS defines “unsecured PHI” as data that have not been rendered unusable, unreadable or indecipherable through a use of a technology or methodology specified by HHS, which currently include specifications developed by the National Institute of Standards and Technology (NIST). HHS also permits a risk analysis to determine whether the breach caused harm. An EHR may be pinged by a hacker, but as long as data is not disclosed, or the data meets the secure PHI standard, there is no breach. Still, if it looks and smells like a breach, it probably is one, and HIPAA’s breach response protocol must be followed. In almost all cases they must be reported to the States where the individuals live under State law. Breach reporting can be very expensive; taking into account some recent mega-breaches, the cost of the average breach is $5.4 million.

There are many takeaways from the new breach requirements for Covered Entities and Business Associates engaged in HIT. First, they should make best efforts to secure PHI according to the NIST and any other industry-level standards. Second, they should ensure that their interests are protected in Business Associate Agreements, including between Business Associates and their subcontractors. Third, they should be aware of HHS’s OIG specific interest in ePHI security for enforcement purposes. Fourth, for all of the reasons above, cybersecurity insurance is strongly recommended.

THE REWARDS AND RISKS IN THE EHR/HIE ECOSYSTEM

In addition to amending HIPAA, HITECH created the architecture for a national health information highway built on electronic patients records, the EHRs. It also directed HHS and other federal agencies to take a leadership role in developing standards. It created the Office of the National Coordinator (“ONC”) to develop the HIE infrastructure and services and to distribute monies, including $2 billion under HITECH, to fund development. The ONC’s website contains a large amount of information on ONC activities related to HIEs, as well as to EHRs, mobile health, and other HIT technologies and solutions.

The EHR is maintained by a healthcare provider and includes all of the key administrative and clinical data relevant to the individual’s care. It goes beyond an electronic health record

---

12 45 C.F.R. §§164.400 et seq.
16 See e.g., 42 U.S.C. §§300jj–11-300jj–17.
to include information from other sources. Treatment data may be transmitted to the EHR from various sources: primary physician and staff notes; picture archives; laboratory reports; pharmacy orders; reports from other providers, such as specialists; and data from medical devices. Billing and administrative data may be included as well. Under HITECH’s framework, an EHR is implemented at the ground level by the hospital, physician, or other organization, such as an ACO (the ground-level organization is the “enterprise”). Via the Internet, the EHR may communicate with other EHRs and data systems to share information between multiple parties: provider-provider; provider-patient; provider-payor; provider-pharmacy; provider-nursing home, provider-government, etc. These other parties can then share information among themselves, creating the connected HIE at the enterprise, community, regional, state and federal level. When the full architecture is in place, if you live in Pennsylvania and need medical care while vacationing in California, your records will be available to your California provider at the press of a button.

There are multiple advantages of EHRs and the HIE systems: EHRs provide ready access to PHI, thereby reducing duplication of tests and delays in treatment; they help reduce medical errors by improving the accuracy and clarity of medical records; they streamline the workflow; and they reduce the high costs of paper records. Similarly, the HIEs reduce costs by facilitating access to health information as well as creating large pools of data that can be used to conduct population-based studies. It is hard to dispute the advantages of the EHR or the HIE—except when they fail, such as in the case of a data breach or misuse of information causing an adverse health outcome. There is also the cost; EHRs and HIEs are supposed to save money, but as a practical matter there are no dedicated income streams or clear model for sustainability for EHRs and HIEs.

**EHRs**

The impetus to adopt EHRs and to create the HIE was HITECH, which provided $36 billion for EHR implementation. Under the act, HHS’s Centers for Medicare and Medicaid Services (CMS) provides for Medicare incentive payments for eligible Medicare Advantage Organizations (MAOs), acute care inpatient hospitals, critical access hospitals and eligible professionals that are “meaningful users” of “certified EHR technology.” Various time frames apply in order for hospitals and non-hospital based physicians to attest to meeting the MU standards in order to receive incentive payments. Incentive payments were first made to entities and professionals meeting MU standards in FY 2011. Eligible entities that are not meaningful users of certified EHR technology beginning in federal fiscal year 2015, however, will be subject to Medicare payment adjustments. There are also meaningful use monies available under the Medicaid program and from some States. And even though the incentive monies are available only for MAOs, hospitals and physicians, other providers, such as nursing homes and home health agencies, are implementing EHRs, often based on the principles for EHRs established by CMS.

The current EHR marketplace is big and multi-faceted, with many established and emerging players. There are several recognized, full-service EHR vendors that cater, for instance, to hospitals or physician groups. They provide an EHR service with multiple capabilities. A newer model of EHR has the advantage of providing the entire revenue cycle process in addition to the electronic clinical information. The marketplace is also filled with discrete EHR add-on products, like data storage providers and laboratory processing solutions. An entity can pick and choose off the menu to create the right EHR system.

To support the careful and deliberate implementation of EHRs, the meaningful use (MU) program provides for three stages of adoption. Each stage has a different emphasis: Stage 1—data capture and creation of EHRs; Stage 2—advance clinical procedures and exchange of information; and Stage 3—improved outcomes. Examples of Stage 1 MU objectives include: using computerized provider order entry and providing patients the ability to view online, download and transmit their health information within four (4) days of the information being available to the ordering professional. Stage 2 MU criteria build on Stage 1 MU requirements and impose more rigorous requirements such as for laboratory results.

---

18 See 42 C.F.R. §495.2 (Incentive Payments); 45 C.F.R. §170.102 (EHR Certification).
19 Eligible professionals have until the start of calendar year 2015.
20 42 C.F.R. §495.6(f).
21 42 C.F.R. §495.6(f)-(l).
2 also requires that EHRs be able to electronically transmit patient care summaries to ordering professionals; to engage with patients such as through email; and to perform HIPAA-level security audits. Stage 3 criteria will build on Stage 2 and are due to be announced this year. Thus, by stages, the healthcare provider’s EHR develops to allow access by stakeholders such as patients and the integration with other data systems—and the enterprise—and community-level HIE is born.

Providers have to demonstrate “meaningful use” through an electronic attestation to CMS that they have met each of the meaningful use measures.22 The information submitted must be generated from the provider’s certified EHR—and attestations are subject to potential audits. Indeed HHS has begun to visit hospitals to conduct these audits, and many will be required to payback EHR monies.

**EHR Legal Issues**

You represent a software company that offers a security fix for a software program including EHRs. Or, you represent an individual who believes that her laboratory results were disclosed. Depending on the situation, here are some EHR-related legal issues to consider:

**Privacy and Security**

HITECH put EHRs squarely under the HIPAA privacy and security umbrella. Not only does the new definition of the Business Associate include the EHR vendor (and its subcontractors), additionally the MU Stage 2 objectives require that the EHR satisfy HIPAA security requirements. Depending on the complexity of a particular EHR system, there may be multiple Business Associates and potential data breach risk points; this is why many parties to a particular EHR system demand contractual indemnification. In addition to HIPAA, there is a particularly thorny problem concerning highly-sensitive PHI in the EHR. Nearly all states, including Pennsylvania, place stiff restrictions on how mental health information is used and disclosed.23 Other highly sensitive PHI includes information on substance abuse, HIV/AIDS and other infectious diseases, reproductive rights, genetic information, and PHI concerning minors. The EHR may be able to segregate notes about a substance abuse admission, but should the fact that the patient takes anti-depressants be included in the EHR to prevent adverse interactions? What if the patient complains that information on his/her antidepressants should not be included in the EHR? The government is struggling with these issues as well. HHS’s OCR recently released guidance on frequently asked questions regarding when it is appropriate to disclose the PHI of a patient being treated for a mental health condition.24 The FDA has expressed a concern for cybersecurity risks in medical devices and hospital networks.25

**Contracts**

Outsourcing information technology systems facilitates implementation but presents numerous risks that are endemic to many software contracts. Some of these issues include: establishing system prerequisites and protocols for modifications and updates (are updates included in the fees?); enforcing service levels, including downtime (when the system goes down, who bears the cost?); without cause termination and transitions (what level of assistance is needed to transition to a new vendor?); third party license issues (would software licenses be violated through integration with another vendor?); indemnification and limitations of liability. Liability issues loom large if the vendor does not make deadlines so that the organization may qualify for EHR monies. In 2012, Girard Medical Center, located in rural Kansas, sued the Cerner Corporation for failing to implement an EHR system timely and walking away from the project.26 EHR contracts can require extensive negotiations, so build in the necessary time.

**Fraud**

In December 2013, the HHS’s OIG issued a report, “Not All Recommended Fraud Safeguards Have Been Implemented In Hospital EHR Technology.”27 The report emphasized the fraudulent...
billing exposure caused by EHR misuse, such as cutting-and-pasting patient notes that do not reflect the services rendered, or using auto-population features that support increased payment levels. OIG has announced that it will rigorously investigate fraudulent billing and EHRs. In addition, the OIG has recently begun using its enforcement authority to audit the incentive payment program and reportedly is demanding paybacks where criteria have not been met. Also there are safe harbor protections and exemptions to the Anti-Kickback Statute and the Stark law, respectively, that protect hospitals that provide physicians with EHRs and those physicians from allegations of improper referral behavior. In December 2013, the OIG and CMS extended these protections through 2021. There are similar provisions for e-prescribing.

**Malpractice**

When the healthcare professional relies on an EHR to diagnose a condition or provide treatment, he/she is assuming that the system is providing accurate information—but what if it isn’t? What if the users aren’t correctly using the EHR to input accurate PHI? What if training was inadequate? Technology presents risks, but so do humans. In October 2013, the Veterans Administration’s Office of the Inspector General confirmed two deaths were caused by staff failing to use the EHR system properly. In another telling example, in June 2013, Picis Inc.’s Caresuite ED PulseCheck, an EHR vendor software application used in the emergency department, reported to the Food and Drug Administration (FDA) that it had recalled its product in fifteen states because of an error that caused the EHR to fail to add data to patients’ charts and to print medication records. Although no adverse health outcomes were announced, it is easy to see how they could have occurred.

**HIEs**

HITECH also put in place the building blocks, particularly EHRs, to stimulate the development of HIEs at the enterprise, community, regional, statewide and federal levels. HITECH provided $2 billion for HIEs, and many states and localities are offering monies as well. These initiatives are ambitious, like trying to build a national transportation highway system all at one time.

The enterprise-level HIE may be a hospital, a health system, a large physician group or an ACO that seeks to enhance the exchange of patient data within its ‘four walls.’ There is no one model for an HIE, and HIEs are developing based on different needs, governance models, directives, time frames, interface issues, and systems’ upgrades and replacements. Developing the enterprise-level HIE is often complicated by the fact that various hospital-based clinics, specialty groups like orthopedics and radiologists very often use their own EHRs. The community-level HIE expands from the enterprise hub out to community providers such as physicians, clinics, pharmacies, nursing homes, and home health agencies. Many Pennsylvania hospitals are in the process of developing enterprise-level HIEs to obtain MU incentive monies that are only available if certain information exchange features, like the ability to exchange patient summaries between providers, are satisfied.

Regional and state HIEs are organized based on geographic area and may be publicly or privately established. An example of a regional HIE is HealthShare Exchange ofSoutheastern Pennsylvania (“HealthShare”), a collaboration among major healthcare stakeholders, including hospitals and payors, across the five-county Philadelphia region to enable the electronic exchange of PHI. HealthShare is working on a tight timeline to e-connect hospitals, city clinics, practitioners and payors in the next few years. Ultimately, ACOs will be connected through the regional exchange as well. At the community level, there is the challenging overlapping hubs, such as two health systems, each with an HIE, that seek to integrate with the same

---

28 42 C.F.R. §495.8(c).
29 42 C.F.R. §§411.357(w); 42 C.F.R. 1001.952(y).
30 42 C.F.R. §§411.357(w)(13); 42 C.F.R. 1001.952(y)(13).
31 42 C.F.R. §§411.357(v); 42 C.F.R. 1001.952(x).
community physicians. HealthShare and other Pennsylvania regional exchanges are also aiming to connect with the Commonwealth’s HIE. In July, 2012, Pennsylvania passed the PA eHealth Information Technology Act (the “eHealth Act”) to implement its statewide HIE efforts. The eHealth Act establishes the Pennsylvania eHealth Partnership Authority (the “Authority”) to develop, establish and maintain the Commonwealth’s HIE. The Authority is working on the critical consent issue to ensure that patients have rights to control what PHI goes into, and is segregated from the HIE. The Authority has also developed the Pennsylvania Patient & Provider Network (“P³N”) to support the secure exchange of PHI between HIEs and providers.

Finally, at the national level, the ONC is authorized to develop the national HIE and has funded the Nationwide Health Information Network (“NwHIN”), a set of standards, services, and policies governing the secure electronic exchange of health information. Already NwHIN has connected many federal agencies and certain private organizations that need to exchange patient information securely. Examples of participating organization include CMS, the Centers for Disease Control, the Department of Defense, the Department of Veterans Affairs, and the Social Security Administration. These participating organizations enter into a Data Use and Reciprocal Support Agreement (“DURSA”), a multiparty agreement outlining the roles and responsibilities of the parties.

HIE Legal Issues

HIEs raise many of the same issues that EHRs raise, but on a larger platform. Even if you are not a dedicated health care attorney, you may need access to PHI in the HIE for litigation, or be asked to review an agreement on behalf of a provider.

Privacy and Security

Maintaining the privacy and security of PHI is perhaps the most obvious legal issue facing HIEs. Who is the Covered Entity and who is the Business Associate may be complicated in the HIE depending on its structure, but since the PHI derives from EHRs, ultimately all of the participants must agree to protect PHI to HIPAA standards. Implementing appropriate security protections to protect the use, storage and transmission of data, is key. This is easier said than done: what if a participating professional does not secure his/her EHR to the NIST standards? How is that enforced? How will the HIE track which provider staff may access the HIE? Random audits are one solution—but if a violation is found, then what? Terminating an HIE participant’s user rights may not an option if the user is critical to the HIE, such as a local pharmacy. Contracts need to anticipate these and other issues.

Patient Consent

Most consumers are still on the learning curve with respect to how HIEs work. Pennsylvania is what is called an “opt-out” state, meaning the HIE must provide a mechanism for the patient to opt-out of the HIE so that his/her PHI, or portions thereof, is not stored or transmitted through the state HIE. Although the opt-out mechanism is required, it is difficult to operationalize. Consequently, it is considered good practice to educate patients about HIEs so that they fully understand the benefits and the risks, and ideally do not opt-out (and to minimize patient complaints). Patients will also have to consent, or not, to the inclusion of any sensitive PHI into the HIE. It is possible to obtain consent at registration or when the consumer first accesses the HIE, for instance through a pop-up “Terms and Conditions of Use” link on the patient portal webpage. If patient consent is not correctly obtained, state and federal government agencies that have an interest in consumer protection, including HHS and the Federal Trade Commission (FTC), may be knocking at the door.

Contracts

Many HIEs use consultants and vendors and have the same contracting issues as for EHR vendors described above. Additionally, for HIEs that extend out into the community and be-

---

35 35 P.S. §§510.101 et. seq.
39 35 P.S. §§510.701(c).
Beyond, participating organizations in the HIE sign participation agreements. As end users, they agree to use the system as it is intended to be used, and not to take advantage of the ready access to the vast quantities of PHI submitted by other participants into the HIE. The HIE creates a valuable store of ‘big data’ for interested parties. For instance, a device supplier may be permitted to access HIE data on its patients for quality of care purposes, but it should be prohibited from pulling down data on patients who recently were treated in the emergency department for orthopaedic events in order to market to those patients. Participation agreements must address other issues like capturing patient consent; training staff; representations to input accurate information; breach reporting; proper use of the HIE web and device portals; and compliance with the HIE’s policies and procedures.

**Fraud and Malpractice**

Prosecution of a fraudulent billing or medical malpractice case within the HIE presents untested issues. Through its web of connected health care providers and others, HIEs maintain information trails and potentially open up discovery opportunities in investigations and lawsuits. The possibilities for who is liable in a malpractice case expand with the use of HIEs—if a decision is made based on inaccurate data, does liability rest with the HIE, the physician who treated the patient, or the physician who input the inaccurate data? HIEs also present challenges due to patient identification. A social security number is the only universal identifier, but some organizations do not always provide access to it. An HIE accessed by multiple individuals and entities thus sets up the risk of false negatives (not finding information on a patient that exists in the HIE) and false positives (finding information belonging to another patient) or simple fraudulent or unlawful behavior (cutting and pasting notes from a prior patient encounter to boost payment).

It is not clear what types of duties would be applied to an HIE in a fraud investigation or a negligence case—does the HIE itself have a duty to ensure the integrity of data, a duty to provide technical support, a duty to adequately train participants? Who is liable if data is somehow manipulated during transmission? Some of these issues should be addressed through good contracting but overall illustrate that the EHR/HIE ecosystem is a new frontier.

**A FINAL WORD ON MOBILE MEDICAL SOFTWARE AND APPS**

In 2009, HITECH put in place the pieces for the creation of a new HIT ecosystem for the delivery of healthcare. But HITECH did not anticipate the recent explosion in mHealth solutions, which expand the ecosystem's reach in significant ways. mHealth is healthcare delivered through mobile communication technology, such as applications (apps) on a mobile device. Examples of mHealth apps include those that measure an individual’s glucose levels; diagnose health conditions like acne; or assist a diabetic in coordinating care between his/her physician, pharmacy, payor and support coaches. The mHealth market is expected to reach approximately $26 billion by 2017. 40 By altering how we manage and treat our own healthcare, mHealth is a critical piece of healthcare reform.

Reflecting how quickly mHealth is impacting the landscape, in 2012, Congress passed The Food and Drug Administration Safety and Innovation Act (FDASIA) 41 in which it authorized the development of a regulatory framework for mHealth. 42 The ONC, the FDA and others agencies are engaged in that effort. Many of the legal principles laid out in this article apply to mHealth, as well unique ones, like FDA regulation. mHealth reinforces the freshness and complexity of the emerging HIT ecosystem. When a client knocks at your door with an idea for an mHealth app or requests help in negotiating an HIE or HIE vendor contract, consider this an exciting challenge to deepen and expand your practice.

---