Electronic Health Records

IT's a HIT

by Jenny Carroll and Daniel O. Carroll

In today's healthcare industry, the use of electronic health records (EHRs) by healthcare providers (from small physician practices to large healthcare systems) is a necessary means of conducting core healthcare operations and delivering and coordinating patient care. For at least a decade, the federal government has targeted the proliferation of the use of EHRs as a primary means of effecting healthcare reform. At the end of George W. Bush's first term as president, he announced the goal of establishing and implementing a nationwide health information technology (HIT) infrastructure that can be accessed and used by providers and patients alike.[1]

EHRs have been identified as a way to cut unnecessary costs, avoid dangerous medical mistakes, eliminate waste and, above all, improve the delivery and quality of care.[2] The federal government continues to support and promote the implementation and use of EHRs by providing incentives for their meaningful use and applying disincentives for failing to do so. The true value of EHRs, and the goal of improved healthcare, can only be realized with nationwide acceptance and use of EHRs by healthcare providers and their patients.

EHR Adoption and Implementation

From a business perspective, the benefits of EHRs to healthcare providers can be seen in purely economic terms with the government incentives provided to meaningful users, the reduced administrative costs involved with maintaining paper charts and transcription services, and the increased opera-

tional efficiencies. From a healthcare perspective, the benefits of EHRs can be seen in terms of improving the quality of care for patients. The use of EHRs has been identified as a way to reduce medication errors and resulting adverse drug events.[3]

In order to achieve the federal government's vision of a fully integrated nationwide HIT, there have been significant technological, financial and regulatory hurdles to clear. Initially, EHRs were expensive investments that lacked the uniformity and interoperability necessary to realize their full potential. In addition to the challenges of promoting the acquisition and adoption of EHR systems by healthcare providers, the federal government and the marketplace had to address significant challenges in the implementation and use of EHR systems.[4]

Significantly, acquisition and implementation of EHRs could not adequately be promoted under the regulatory structure that existed prior to 2004. President Bush issued an executive order in April 2004 creating an executive office "to provide leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care."[5] In other words, the charge of this central office was to determine how to smoothly and securely share health records among appropriate parties once in electronic format. By virtue of this executive order, the Office of National Coordinator for Health Information Technology (ONC) was established under the oversight of the United States Department of Health and Human Services (HHS). Since its inception, the ONC's role has been expanded to support HIT implementation by subsequent legislation.[6] The ONC is responsible for establishing standards for certified EHR, including privacy, security and interoperability.[7]

After more than a decade, the ONC has acknowledged the significant progress made with HIT in the United States, but has also recognized there remain barriers to secure, efficient and effective sharing and use of electronic health information nationwide.[8] These barriers include: 1) failure to sufficiently structure and standardize electronic health information, causing workflow difficulties; 2) inadequate financial motives and inconsistent legal and operational policies, which inhibit the sharing of electronic health information; and 3) despite existing networks offering interoperability across a select set of participants, there remains no reliable way to establish the necessary trust for the sharing of electronic health information across disparate networks nationwide.

While the ONC concedes it is not realistic to think all electronic health information needs in the United States can be met with a single approach to sharing such information, it strongly believes a common set of policies and technical standards must be adopted to facilitate nationwide interoperability and provide end users of EHRs with flexibility.[9]

Clearing Regulatory Hurdles

In order to foster widespread acquisition and adoption of EHRs, several regulatory restrictions required adjustment. Specifically, the federal Stark law and the anti-kickback statute had to be modified to permit and facilitate the adoption of EHR systems by healthcare providers. In addition, the federal regulations needed to set the functional and operational standards for the type of EHRs that should be promoted, and therefore qualify for these regulatory protections. Accordingly, it was determined early on that certification of EHRs by the federal government was a critical component of implementing a nationwide HIT.

In 2006, the Office of Inspector General (OIG) and the Centers for Medicare and Medicaid Services (CMS) promulgated regulations designed to advance the goal of improving "health care quality and efficiency through widespread adoption of interoperable electronic health records systems."[10] These regulations established a new exception to the Stark law and a new safe harbor under the anti-kickback statute. Pursuant to the new rules, a hospital is able to provide its staff physicians with financial assistance for the acquisition of certified EHR systems. The regulations detail how these arrangements are to be structured and documented. It is worth noting that the regulatory provisions allowing these arrangements are available for a limited period of time, and are set to expire in 2021.[11]

Even though the federal regulatory barriers were addressed from a fraud and abuse perspective, federal tax law posed an additional concern for tax-exempt hospitals. Tax-exempt hospitals feared that providing financial assistance to their staff physicians to acquire EHRs would constitute an impermissible private benefit to these physicians. In 2007, the Internal Revenue Service issued a memorandum assuring tax-exempt hospitals that providing EHR acquisition assistance to physicians would not constitute an impermissible private benefit, as long as the regulatory requirements for the Stark law exception and the anti-kickback statute safe harbor were satisfied together with some additional requirements.[12]

Incentives and Penalties

After initial regulatory barriers were addressed, the next step in promoting the adoption of EHRs came as part of broader legislation designed to address a downturn in the national economy. In Feb. 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Rein-

vestment Act of 2009.[13] In part, the HITECH Act was designed to promote the adoption and meaningful use of health information technology. Through the HITECH Act, the government enacted a regulatory scheme that would provide financial incentives for adoption of EHRs by eligible healthcare providers, while at the same time impose penalties on those who refused or failed to adopt and implement EHR systems.

The HITECH Act sets the parameters for the EHR incentive program (*i.e.*, eligibility requirements for payments, incentive calculation and payment amounts, payment timelines and penalties), but relies on CMS to promulgate regulatory requirements to determine how and when providers achieve 'meaningful use' of certified EHRs. Incentive payments for adoption and meaningful use of certified EHRs are available to certain eligible professionals, eligible hospitals and critical access hospitals.[14]

Pursuant to the HITECH Act, a user of an EHR system must be able to demonstrate: 1) the use of a certified EHR system in a meaningful manner; 2) the certified EHR system is connected in a manner that provides for the electronic exchange of health information to improve the quality of care; and 3) the use of the certified EHR system to submit clinical quality measures and other measures, as may be required.[15] In order to participate in the government-sponsored EHR incentive programs, and to receive incentive payments while avoiding payment adjustments or penalties, providers must be eligible and must successfully demonstrate meaningful use of EHRs for each year of participation in the EHR incentive program.[16]

In order to maintain flexibility with ever-changing and rapidly developing EHR technology, CMS has adopted an approach that will stagger or phase in the requirements for EHR adoption and meaningful use over time in successive stages. The graduated approach of stages is intended to allow rulemaking based on user experience with the available technology, and each stage will progressively and incrementally expand the requirements for achieving meaningful use of EHRs.[17]

The stages of meaningful use are designed as follows: 1) Stage 1 meaningful use criteria is focused on data capture and sharing; specifically, electronically capturing health information in a standard format; using the information to track key clinical conditions; communicating captured information for care coordination processes; initiating the reporting of clinical quality measures and public health information; and using information to engage patients and their families in their care; 2) Stage 2 meaningful use criteria is focused on advance clinical processes; specifically, more rigorous health information exchange; increased requirements for e-prescribing and incorporating lab results; electronic transmission of patient care summaries across multiple settings; and more patient-controlled data; and 3) Stage 3 meaningful use criteria is focused on improved outcomes; specifically, improving quality, safety and efficiency, leading to improved health outcomes; decision support for national high-priority conditions; patient access to self-management tools; access to comprehensive patient data through a patient-centered health information exchange (HIE); and improving population health. CMS indicated that it may adopt additional stages to introduce further meaningful use criteria at a later date.[18]

While eligible professionals and eligible hospitals that are able to successfully attest to compliance with meaningful use criteria will receive incentive payments, those who are unable to do so in the required time period will be subject to penalties or payment adjustments. The payment adjustments are effected through the Medicare physician fee schedule (PFS) for covered professional services furnished during the year.[19] Payment adjustments are graduated as follows: 1) a one percent reduction in Medicare PFS payments in 2015; 2) a two percent reduction in Medicare PFS payments in 2016; and 3) a three percent reduction in Medicare PFS payments in 2017 and subsequent years.[20] In addition, meaningful use must be demonstrated every year by the eligible professional in order to avoid payment adjustments in subsequent years.[21] Notably, CMS may increase penalties beginning in 2018.[22]

Audits and Appeals

All providers receiving incentive payments may be subject to an audit by CMS to verify the applicable provider's attestation.[23] During the audit, CMS will look for the source documentation used by the provider when making the attestation. This documentation should be retained by the attesting provider for at least six years post-attestation.[24] The OIG's 2015 and 2016 work plans indicate a commitment to conducting more audits related to the use of EHRs by healthcare providers. Specifically, the OIG is focusing on security matters for EHRs, as well as reviewing EHR incentive payments to ascertain if they were properly made.[25] As a matter of best practices, eligible professionals and hospitals should conduct their own self-audits to ensure attestations are properly made and to be prepared for any possible government audits. Self-audits may provide the audited eligible professional or hospital with a basis for appealing any adverse audit determinations made by the government.[26]

Non-Regulatory Barriers to Implementation

Addressing regulatory and legal issues is only part of the challenge to a successful EHR implementation. Equally impor-

tant, and sometimes more daunting, are the business issues that may impede success. There have been several studies concerning these real world (*i.e.*, non-legal) challenges for healthcare providers adopting and implementing EHR systems. These studies seem to reveal three major categories of obstacles to successful adoption of EHR systems by healthcare providers: 1) cost; 2) technical issues; and 3) workforce training and education. When faced with these obstacles, the challenge to implement an EHR system successfully is further compounded by negative attitudes and resistance to change from the individuals tasked with executing the project.[27]

First and foremost, healthcare providers are faced with a significant investment to purchase and install an EHR system. These significant financial costs are felt immediately and directly by the healthcare provider paying for the EHR system, while the benefits may not be realized for quite some time. In addition, some of the more important benefits of EHR implementation are actually realized by others who do not pay for the EHR system, such as patients and payors.

Since an EHR system represents a significant financial investment for a healthcare provider, it is crucial to select the right system. Choosing the right EHR system means addressing technical concerns, such as system interoperability (*i.e.*, healthcare data maintained in 'silos'), non-standardized EHR applications, concerns about privacy and security, risks of technical errors in software causing billing errors, data capture anomalies, programming errors, invalid decision support information, risks of EHR systems quickly becoming obsolete and the risk of EHR vendors going out of business and being unable to support the investment.

Finally, successful implementation of an EHR system requires the healthcare provider's staff to make a significant investment of time to be educated and trained to properly and meaningfully use the EHR system. Initially (and until the workforce is trained and the system is integrated into the practice), workflow will be interrupted and staff will need to devote significant time and effort in mastering the EHR system. In the end, the goal is to appropriately use the system to reduce medical errors, improve the quality of care, practice medicine more efficiently and share information among a patient's healthcare providers.[28]

Even if a healthcare provider chooses the right EHR system and all technical concerns are addressed (or otherwise minimized), system implementation will not succeed without proper training and education of the users on its capabilities. Poorly trained users, or a staff with a reluctant or negative attitude about EHR implementation, can threaten a successful launch and the healthcare provider's substantial investment of time and money. Continuous training, education and support for the use of an EHR system are integral components in achieving meaningful use of the system.

Poor training and lack of education on the proper use of an EHR system can expose users and their patients to unintended risks. For example, standardized or template language included in an EHR system should not be ignored and should not be maintained if its presence in a medical chart would create a false or misleading medical record. Patient care may be adversely affected or allegations of fraud may arise if a physician, who has not been adequately trained in the use of an EHR system, unintentionally leaves default or template language in an EHR record.[29]

After the initial EHR adoption, these 'real world' barriers and provider concerns may resurface if the healthcare provider needs to switch EHR systems. The need to change EHR systems may be precipitated by any number of circumstances, including dissatisfaction with the functionality of a current EHR system, dissatisfaction with vendor support for the EHR system, physician practice or hospital mergers and acquisitions, and physician alignment with a hospital.

When changing EHR systems, healthcare providers must consider not only what needs to be done to transition to the new EHR system, but also how to properly and effectively sunset the old EHR system. A mechanism for a data transfer upon termination or expiration of a contract is an important item to be included in an EHR service agreement. Once again, concerns related to incurring additional costs, managing operational change and re-training or re-educating the provider's workforce must be factored into an investment of another new EHR system. In addition, providers must understand how a transition will affect their status as meaningful users of EHRs and how they can ensure access to patient information is not interrupted during a transition. While a primary focus for healthcare providers is selecting the appropriate EHR system, equally important in a successful switch of EHR systems is understanding how the change will impact patient care and practice flow. Promoting and securing a positive attitude among staff about the transition and re-training will go a long way in successfully instituting a replacement EHR system.[30]

CMS has recognized that some healthcare providers participating in an EHR incentive program may need to switch EHR systems during the program year. If an eligible professional or a hospital is in the process of attesting to meaningful use when it makes a switch to a new EHR system, the healthcare provider or hospital must still attest to the applicable stage of meaningful use for the entire program year. However, "the data collected for the selected menu objectives and quality measures should be combined from both of the EHR systems for attestation. The count

of unique patients does not need to be reconciled when combining from the two EHR systems."[31] Further, "[i]f the menu objectives and/or clinical quality measures used are also being changed when switching vendors, the menu objectives and/or quality measures collected from the EHR system that was used for the majority of the program year should be reported."[32]

EHR Privacy and Security

From a privacy perspective, sharing individually identifiable health information (protected health information or PHI) remains an ever-present concern.[33] The Health Insurance Portability and Accountability Act of 1996,[34] and related privacy rules[35] and security rules,[36] as amended by HITECH (collectively referred to below as HIPAA) provide the framework under which providers must protect the privacy and provide security for identifiable patient information. When a healthcare provider of services,[37] such as a physician or hospital, transmits health information in an electronic form, the provider is considered to be a 'covered entity' under HIPAA.[38]

Covered entities have specific obligations relative to safeguarding and sharing patient PHI that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium, other than where an exception applies.[39] At its core, HIPAA permits covered entities to use and disclose PHI in order to carry out treatment, payment or healthcare operations.[40] Unless an authorization is specifically required with respect to specific uses and disclosures, a healthcare provider may (but is not required to) obtain consent of the individual to use or disclose PHI for these purposes.[41]

Due in large part to the incentives provided for engaging in meaningful use of EHRs, medical practices and healthcare systems have significantly migrated from the paper medical chart and committed to the electronic format for record storage and billing. But this initial step represents only the tip of the iceberg. Financial incentives, in-office efficiency, modernization and improvement of care may have been an early driver to go electronic, but the bigger picture requires these individual EHR systems transmit data between and among other EHR systems. Technical difficulties aside, when varying platforms may or may not achieve compatibility, sharing PHI opens the door to a multitude of beneficial applications, restrained within the framework of privacy laws. Regulatory boundaries to unbridled sharing of data set the limits that create hurdles for healthcare providers to collaborate and coordinate care under a successful and compliant model.

Healthcare reform has stirred innova-

tion and decreased applicability of linear physician-to-physician relationships. Rather than one physician's office calling another to request medical records, or faxing a consent to do so, providers can now pull or push data from an online portal containing information compiled by multiple specialists and providers. Data exchanges are operable, whereby patient data exists in the cloud, for a host of recipients to obtain. Patient care models and other new modalities, such as accountable care organizations (ACOs), require sharing data among providers and vendors, in order to manage and improve outcomes. Electronic data is also quantifiable in a way that paper records were not, for use in reporting requirements, quality measures, research, Medicare shared savings programs and aggregate data from multiple sources and locations.

With all of this information uploading and sharing, it is easy for the lines to become blurred with respect to the security of data, and who is responsible for it. As the sharing of patient data proliferates electronically, the responsibilities of healthcare providers remain unclear in terms of reviewing and acting upon it. Reviewing large amounts of health information, such as test results, that get automatically uploaded into a chart, raises new questions about expectations and follow-ups.

The multitude of governing laws and regulations also present challenges. In addition to HIPAA, the National Institute of Standards and Technology (NIST) has created a cybersecurity framework that encompasses infrastructures, including healthcare.[42] Add in state laws, accrediting bodies, membership organizations, and other applicable rules and adherence to the multitude of laws, regulations and guidance becomes challenging, and may even act as a hindrance to care.[43] Developing compliant agreements and securing contracts from each user or end user obtaining information from an electronic record, including HIEs, presents unique challenges, or even barriers.

Trust is an integral part of care. Physicians and hospitals are charged with maintaining and honoring that expectation of privacy in a patient's health record. Covered entities must ensure the confidentiality, integrity and availability of PHI it creates, receives, maintains or transmits; protect against reasonably anticipated threats to the security or integrity of the PHI; protect against reasonably anticipated unpermitted uses or disclosures of PHI; and ensure compliance by its workforce.[44] The covered entity has flexibility in deciding what security measures are appropriate, taking into account factors of size, complexity and capabilities, technical infrastructure, costs, and probability and criticality of risks to PHI.[45] These protective measures include administrative safeguards, physical safeguards and technical safeguards.[46]

While digitizing records reduces administrative and staffing expenses, data hacks and security breaches can rise to insurmountable levels. Staffing education and a sound arsenal of security policies can go a long way to ensure PHI is handled correctly and securely to the extent possible. Firewalls, passcodes and sophisticated encryption are undoubtedly within the realm of necessary safeguards to fend off potential cyber attacks. Auditing system users is also an essential step in ensuring only those individuals with a need to access patient data do so.

An important first step in setting forth the rights and obligations of the parties disclosing and receiving PHI is to enter into a business associate agreement (BAA). A business associate is a party that creates, receives, maintains or transmits PHI for and on behalf of a covered entity, where the provision of the services involves disclosure of PHI.[47] Extending the obligations of a covered entity, a BAA sets forth the obligation of the business associate to likewise implement administrative, physical and technical safeguards to appropriately protect the PHI the business associate creates, receives, maintains or transmits on the covered entity's behalf.[48]

Another obligation of the business associate under a BAA is the reporting of any security incident of which it becomes aware.[49]

In the context of EHRs, the causes of breaches may take many forms, such as inadequate encryption, a lost or stolen laptop, or even impermissible disclosures without a patient's consent. This may affect one or many patients, and the magnitude of the breach will affect the reporting requirements.[50] Breaches are treated as discovered as of the first day the breach is known.[51] The covered entity must determine, to the extent possible, every individual whose PHI has been accessed, acquired, used or disclosed as a result of the breach.[52] Upon the occurrence of an electronic breach, the fact-finding process may be a difficult path to follow.

Under HIPAA, an unauthorized disclosure of PHI is presumed to be a breach unless the covered entity can demonstrate there is a low probability the PHI has been compromised by engaging in a risk assessment.[53] In order to perform a risk assessment that involves EHR, technical or forensic experts may need to be consulted to follow the electronic flow of information or determine the accessibility of electronic data and mitigate damages, when possible. The days of locking charts in a cabinet have been replaced by computer data loss scenarios that may be costly and/or difficult to detect. Each individual whose PHI has been accessed must be notified, without unreasonable delay, and not more than 60 days from discovery of the breach, in compliance with HIPAA[54] and the New Jersey Identity Theft Prevention Act.[55]

Providers that participate in HIE organizations (HIOs) benefit from the combination of advanced technology and efficient secure connections with other participating providers. Member healthcare organizations and providers may quickly gain access to patient histories and medications that leads to enhanced patient satisfaction, improved care and error reduction. It also lends itself to the development of patient portals and electronic communication systems, aimed at encouraging patients to participate in their own care. The larger the network of providers, the more comprehensive and reliable the information will be.

With patient consent, PHI may be shared by and between various healthcare providers, ACOs and other care models that would otherwise be unrelated. Patients retain the choice of whether to participate in an HIO, and can opt out at any time. At this time, HIOs are becoming more prevalent on the state level. However, a broader national system may be possible with increased interoperability or a universal EHR system. While the broader scope of health information sharing may result in a bigger potential upside, any such potential must be measured against the grander potential impact of a data breach and the enhanced difficulty in deciphering the root cause, or the responsible party.

Conclusion

Health information technology application has a future that will extend well beyond the regulatory objective of 'meaningful use.' Improving patient care and reducing medical errors are two goals that may be achieved through increased interoperability between EHR systems and exchanges. Whether change is driven purely by government incentives or a demand in the marketplace for better service and outcomes, the direction of the industry is one toward fully electronic medical record use, retention and exchange. Privacy and security measures will be required in order to maintain the integrity of the provider-patient relationship and adherence to applicable laws. As interoperability among systems is a top priority, this endeavor requires parties to work together to develop comprehensive policies detailing who may access such PHI, how and for what purpose.[56] While avoiding data breaches should be a top priority, having a plan in place to respond to these incidents and to mitigate damages in the event of a breach remains a crucial obligation.

Although significant strides have been made toward realizing the goal of a secure and readily accessible nationwide HIT infrastructure, there is still a significant distance to close. As the remaining challenges are met, healthcare providers and patients alike will enjoy the benefits

of secure, efficient and effective sharing of health information with improved quality of healthcare delivery and results at lower costs.

Jenny Carroll *is corporate counsel for Atlantic Health System, Inc., where she provides corporate and regulatory guidance to the hospital system and numerous satellite facilities.* ***Daniel O. Carroll*** *is a partner with Schenck, Price, Smith & King, LLP, based in the Florham Park office. He is a member of the healthcare law and corporate practice groups and focuses his practice on healthcare corporate, transactional and regulatory matters for institutional healthcare providers.*

ENDNOTES

1. In his Jan. 20, 2004, State of the Union speech, President Bush stated that "[b]y computerizing health records, we can avoid dangerous medical mistakes, reduce costs and improve care." President Discusses Health Care in State of the Union, georgewbush-whitehouse.archives.gov/news/releases/2004/01/print/20040120-11.html (Jan. 20, 2004) Later in 2004, President Bush also proclaimed his goal of every American having a personal electronic medical record within 10 years. *See* Nicolas P. Terry, Under the Knife: Health Law, Health Care Reform, and Beyond: Information Technology's Failure to Disrupt Health Care, 13 *Nev. L.J.* 722 (Spring 2013) (internal citation omitted).
2. *See Id.* at 728-29 (internal citations omitted); *see also*, Exec. Order No. 13335, 69 Fed. Reg. 24059-60 (April 30, 2004); *see generally*, Robert D. Belfort *et al.*, Health Information Technology: Emerging Landscape, Legal Issues and Opportunities, (BNA's Health L. & Bus. Series, No. 1150) 1150.01.A, 1150.00101, (*citing* Committee on Quality of Health Care in America, Crossing the Quality Chasm: A New Health System for the 21st Century, IOM (March 2001)).
3. *See* 42 U.S.C. § 300jj-11; *see generally*, Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.); *see also*, Sima Ajami and Razieh Arab-Chadegani, Barriers to Implement Electronic Health Records (EHRs) Mater Sociomed. 2013;25(3):213–215 (2013), ncbi.nlm.nih.gov/pmc/articles/PMC3804410/.
4. *See generally*, Nicolas P. Terry, Under the Knife: Health Law, Health Care Reform, and Beyond: information Technology's Failure to Disrupt Health Care, 13 *Nev. L.J.* 722 (Spring 2013).
5. Exec. Order No. 13335, 69 Fed. Reg. 24059-60 (April 30, 2004).
6. *See* Zeng, Xiaoming *et al.*, Redefining the Roles of Health Information Management Professionals in Health Information Technology, Perspectives in Health Information Management (Sept. 16, 2009), ncbi.nlm.nih.gov/pmc/articles/PMC2781729/?report=classic.
7. *See* 42 U.S.C. § 300jj-11; *see also,* Ranjit Janardhanan, Uncle Sam Knows What's In Your Cabinet: The Security and Privacy Protection of Health Records Under the HITECH Act, 30 *J. Marshall J. Info. Tech. & Privacy L.* 667, (Summer 2014); *see generally*, Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009)(codified as amended in scattered sections of 42 U.S.C.).
8. *See* Office of the National Coordinator for Health Information Technology (ONC), Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, (Draft Version 1.0), healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf (suggesting a roadmap focusing on actions to enable a majority of individuals and health care providers nationwide across the continuum of care to send, receive, find and use a common set of electronic clinical information by the end of 2017).
9. *Id.*
10. *See* Medicare and State Health Care Programs: Fraud and Abuse; Safe Harbors for Certain Electronic Prescribing and Electronic Health Records Arrangements Under the Anti-Kickback Statute, 71 Fed. Reg. 45,110 (Aug. 8, 2006)(codified at 42 C.F.R. §1001.952(y)(detailing conditions of safe harbor)); Medicare Program; Physicians Referrals to Health Care Entities With Which They Have Financial Relationships; Exceptions for Certain Electronic Prescribing and Electronic Health Records Arrangements, 71 Fed. Reg. 45,140 (Aug. 8, 2006)(codified at 42 C.F.R. §411.357(w)(detailing conditions for the exception to apply)).
11. Initially set to expire on Dec. 31, 2013, the regulatory sunset date for the Stark law exception and the anti-kickback safe harbor was extended to Dec. 31, 2021. *See* 42 C.F.R. §411.357(w)(13) and 42 C.F.R. §1001.952(y)(13).
12. I.R.S. Mem., Hospitals Providing Financial Assistance to Staff Physicians Involving Electronic Health Records (May 11, 2007), irs.gov/pub/irs-tege/ehrdirective.pdf, (requiring a written agreement with the physicians for such assistance, hospital access to all of the records created using the EHR, and availability of the EHR technology to all staff physicians and the same level of financial assistance must be made available to all medical staff physicians).
13. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009)(codified as amended in scattered sections of 42 U.S.C.).
14. *Id.*; CMS oversees the Medicare EHR Incentive Program and state Medicaid agencies oversee the Medicaid EHR Incentive Program. Eligibility for incentives will differ depending on the applicable program. Most eligible hospitals will participate in both the Medicare and Medicaid EHR Incentive Programs. CMS, EHR Incentive Programs, An Introduction to the Medicare EHR Incentive Program for Eligible Professionals, cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/beginners_guide.pdf.
15. 42 U.S.C. §1395w-4(o)(2)(A)(i)-(iii).
16. CMS, EHR Incentive Programs, An Introduction to the Medicare EHR Incentive Program for Eligible Professionals, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/beginners_guide.pdf.
17. Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 75 Fed. Reg. 44,314, 44,321 (July 28, 2010) (noting that the phased approach is intended to build up to "a more robust definition of meaningful use as technology and capabilities evolve"); accord, Medicare and

Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed. Reg. 53,968, 53,973 (Sept. 4, 2012)(codified at 42 C.F.R. Parts 412, 413, 422 and 495); *see also*, ONC, Guide to Privacy and Security of Electronic Health Information, Ver. 2.0, Ch. 5, (April 2015) healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-5.pdf.

18. *See* ONC, EHR Incentives & Certification: How to Attain Meaningful Use, http://www.healthit.gov/providers-professionals/how-attain-meaningful-use; Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 75 Fed. Reg. at 44,323; Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed. Reg. at 53,968.
19. 42 C.F.R. §495.102(d).
20. *Id.* Eligible professionals may apply for an exemption from the penalties if achieving meaningful use would constitute a significant hardship. Such applications are considered on a case-by-case basis.
21. 42 C.F.R. §495.4.
22. 42 U.S.C. §1395w-4(a)(7); 42 C.F.R. §495.102(d)(3).
23. 42 C.F.R. §495.316.
24. CMS, EHR Incentive Programs Supporting Documentation For Audits, (last updated Feb. 2013), available at cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_SupportingDocumentation_Audits.pdf.
25. OIG, U.S. Dept. of Health & Human Services, Work Plan Fiscal Year 2015, oig.hhs.gov/reports-and-publications/archives/workplan/2015/FY15-Work-Plan.pdf at 74-75; OIG, U.S. Dept. of Health & Human Services, Work Plan Fiscal Year 2016, oig.hhs.gov/reports-and-publications/archives/workplan/2016/oig-work-plan-2016.pdf at 75-76.
26. Audit determinations can be appealed. Permissible appeals fall into three categories: 1) eligibility appeals; 2) meaningful use appeals; and 3) incentive payment appeals. Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed. Reg. 53,986, 54,112 (Sept. 4, 2012).
27. *See* Sima Ajami and Razieh Arab-Chadegani, Barriers to implement Electronic Health Records (EHRs), (2013), ncbi.nlm.nih.gov/pmc/articles/PMC3804410/.
28. *Id.*; *see also*, Agency for Healthcare Research and Quality, U.S. Dept. of Health & Human Services, Barriers to HIT Implementation, healthit.ahrq.gov/health-it-tools-and-resources/health-it-costs-and-benefits-database/barriers-hit-implementation.
29. *See* Robert D. Belfort *et al.*, Health Information Technology: Emerging Landscape, Legal Issues and Opportunities, (BNA's Health L. & Bus. Series, No. 1150) 1150.02.D.1.a, 1150.0221-0222.
30. *See* Sima Ajami and Razieh Arab-Chadegani, Barriers to implement Electronic Health Records (EHRs) (2013), ncbi.nlm.nih.gov/pmc/articles/PMC3804410/.
31. *See* CMS, FAQ available at questions.cms.gov/faq.php?faqId=8227 (created 4/22/2013).
32. *Id.*
33. 45 C.F.R. §160.103.
34. Pub. L. No. 104-191.
35. 45 C.F.R. 164 Subpart E.
36. 45 C.F.R. 164 Subpart C.
37. 42 U.S.C. §1395x(s) and (u).
38. 45 C.F.R. §160.103.
39. *Id.*
40. 45 C.F.R. §164.506.
41. 45 C.F.R. §164.508.
42. *See* Matthew Scholl *et al.*, Security Architecture Design Process for Health Information Exchanges (HIEs), National Institute of Standards and Technology, U.S. Dept. of Commerce, NISTIR 7497 (Sept. 2010), (providing a systematic approach to designing a technical security architecture for the exchange of health information leveraging common government and commercial practices and demonstrating how these practices can be applied to the development of HIEs).
43. *See* ONC Roadmap, *supra* note 8.
44. 45 C.F.R. §164.306.
45. *Id.*
46. 45 C.F.R. §§164.308, .310, and .312.
47. 45 C.F.R. §160.103.
48. 45 C.F.R. 164.314.
49. *Id.*
50. 45 C.F.R. §§164.406 and .408.
51. 45 C.F.R. §164.410.
52. *Id.*
53. 45 C.F.R. §164.402.
54. 45 C.F.R. §164.404.
55. N.J.S.A. §56:11-44, *et seq.*
56. Julie Creswell, Doctors Find Barriers to Sharing Digital Medical Records, *N.Y. Times*, Sept. 30, 2014, available at nytimes.com/2014/10/01/business/digital-medical-records-become-common-but-sharing-remains-challenging.html?comments&_r=0 (also in print on Oct. 1, 2014 at B1).

This article was originally published in the April 2016 issue of New Jersey Lawyer, a publication of the New Jersey State Bar Association, and is reprinted here with permission.