

Keys to Electronic Records Implementation Compliance

Presenters: Matthew Weber, Partner, Holland & Hart LLP
William H. Fischer, Of Counsel, Holland & Hart LLP

I. Getting what you want from vendors.

- (The types of deliverables and warranties needed in vendor contracts.)

A. Introduction – There are various types of agreements that may be found relating to the implementation of electronic health records (EHR), including but not limited to software license agreement, maintenance agreement, professional service agreement, outsourcing agreement, hosting or co-location agreement, and so on.

As technology changes, so do the products and services provided by vendors. As laws change, so do business requirements and compliance challenges. Perhaps more now than ever in the past, it is extremely important for health care professionals to understand how contract provisions can impact the implementation of EHR, compliance with legal requirements, and financial responsibility for information system security breach.

This section will discuss how recent changes to technology and law require health care professionals, attorneys, and vendors to take a second look at traditional contract provisions. Specifically, this section will discuss contract provisions that cover the following topics: limited liability disclaimer, confidentiality, compliance and standards, reporting requirements, and subcontracting and third parties.

B. Limited Liability Disclaimer

1. Traditional Approach – There are many losses and damages that vendors are not willing to (or capable of) taking on. For example, a vendor that picks up and stores back-up tapes of computer data for \$200 per month may not want to (or may not be able to) pay for the losses resulting from the loss of a tape containing the personal information of 100,000 customers.

Traditionally, the limited liability disclaimer will include an exclusion of special, indirect, incidental, punitive, and consequential damages. Other liabilities the vendors seek to limit involved those arising from actions of third parties or from the customer's employees. Often, vendors seek to limit their liability to the value of the contract or to expected profits. And finally, vendors will often try to require that any claims against the vendor be brought within a short period of time, effectively shortening the statute of limitations.

2. Changes in Technology or Law – As organizations move from paper-based records to electronic records, they become more dependent upon technology. Essentially, there are more eggs in fewer baskets. This means the consequences of failure, errors, mistakes, or unavailability of information systems are much greater than they were in the past. Also, the costs of recovery, repair,

and replacement of information systems or data can be high when considering all of the vendors and individuals involved in such an effort.

In addition, legal sources of authority are placing greater responsibility on the organization. While organizations can outsource certain services or IT functions, they cannot outsource or escape responsibility for the ultimate safety of patients or compliance with the law. Also, losses or damages are often the result of a third party's or an organization's own employees. In cases where the privacy or confidentiality of an individual's personal information was compromised, that individual often places the blame on the organization, causing the organization to be a "double victim:" once for the initial breach, then again for the subsequent lawsuit. So in addition to technical losses and damages, organizations can expect to pay for costly internal investigations and legal services in anticipation of litigation.

3. Considerations – To mitigate such losses, health care organizations should consider revising the standard limited liability disclaimer by (i) carving out certain claims and certain damages from the vendor's limit of liability, (ii) examining other provisions to ensure compatibility with such carve-outs, and (iii) consider requiring insurance where such claims could result in losses or damages that exceed the amount the vendors is willing to or capable of taking on.

Carve-outs – Typical carve-outs may include patent indemnification, personal bodily injury and personal property damage, vendor's intentional breach of confidentiality obligations, gross negligence, recklessness, and intentional misconduct. To address changes in technology and law, the health care organization may consider carving out certain claims, such as breach of confidentiality of personally identifiable information caused by the acts or omissions of the vendor, the vendor's employees, or subcontractors. Other claims to consider carving out include those limiting or restricting breach of contract or warranty claims. Any acts or omissions the health care organization wishes to prevent should trigger a breach of contract claim, in addition to a tort claim. This requires careful review of the contract as a whole to ensure that breach of contract includes violations of those provisions.

Also, the health care organization may consider carving out certain damages from the limited liability disclaimer to permit the organization to recover for costs relating to information system downtime, response and investigation, system recovery, and regulatory (e.g., CMS, FTC) or private (e.g., PCI) fines and penalties. Such damages can be difficult to prove as direct or may be expressly included in the typical limited liability disclaimer's laundry list of excluded damages. One method to accomplish this task is to include a subsection entitled "Acknowledged Direct Damages," where the parties agreed that a certain list of damages shall be deemed "direct" and not indirect, incidental, special, etc.

Other Contract Provision Compatibility – Any changes in the limited liability disclaimer need to be considered in the context of the entire contract, and therefore, the health care organization should examine the indemnification and remedies provisions to ensure they are compatible. For example, any claim that may be carved out of the limited liability disclaimer should be indemnified elsewhere in the agreement. Also, carving out certain damages or losses in the limited liability disclaimer should be analyzed for compatibility with provisions specifying remedies or liquidated damages.

Insurance – When vendors are not willing or capable of taking on certain potential losses, the health care organization may consider requiring insurance to cover specific claims. More insurance companies are offering services that cover losses and damages that traditional general commercial liability or error and omissions policies typically exclude. Policies must be tailored to address the specific needs of the health care organization, and therefore, the health care organization must carefully review any policy a vendor claims already provides coverage.¹

C. Confidentiality

1. Traditional Approach – Standard confidentiality provisions restrict the disclosure and use of certain information. Typical confidentiality provisions provide exceptions for situations where information is available to the public or for information that is provided from third parties. Vendors seek to expand such exceptions as much as possible in order to limit their exposure to liability.

2. Changes in Technology or Law – The applicability of some laws relating to the protection of information depends on the source or use of the data, rather than the actual contents of the data. For example, demographic information that is freely available to the public in the white pages of a telephone directory may be deemed protected health information (PHI) under HIPAA if the same information comes from a hospital. On the other hand, a vendor that causes the unauthorized disclosure of such information may seek protection under the exception to the confidentiality provision for information that is available to the public.

Due to the vast amounts of data and the desire to turn all that data into usable information, organizations often hire vendors to provide data processing or other services to consolidate or manage data from various sources. Under such arrangements, a vendor could claim that any unauthorized breach or disclosure of such information does not violate a confidentiality provision if there is an exception for information lawfully received from third parties.

¹ In addition, health care organizations should require notice for any lapse in coverage and require the vendor to name the health care organization as a beneficiary to the policy.

3. Considerations – To ensure the confidentiality provision provides adequate protection, the health care organization should (i) restrict all uses and disclosures, permitting few by exception, (ii) limit or remove typical exceptions, and (iii) require vendors to enforce obligations on subcontractors and third parties.

Restrict All, Permit Few by Exception – Health care organizations should carefully draft the general confidentiality provision to ensure that it prohibits the use or disclosure of confidential information for *any* purpose other than to carry out the contracted services.² While this may seem to be intuitive advice, be wary of language that requires the discloser health care organization to specify prohibited uses or that provides the vendor with discretion in selecting which uses or disclosures are permitted. Bottom line: Restrict all, permit few by exception.

Limit Exceptions – The health care organization needs to address the exceptions discussed above. While other remedies may be available under contract or tort law, an organization should seek to protect all possible future claims, including claims for a vendor’s violation of a confidentiality provision. Therefore, health care organizations should seek to minimize the impact of exceptions to the confidentiality provision by either removing certain exceptions altogether or carving-out certain information (such as personally identifiable information or personal health information) from such exceptions.

Downstream Obligations – In addition to enforcing confidentiality and restricting use of information by vendors, health care organizations need to require vendors to pass along such obligations to the vendor’s subcontractor, outsourcers, and other third parties. This can be done by requiring the vendor to ensure all third parties sign a separate confidentiality agreement or by requiring the vendor to ensure third parties at least agree to undertake the same or similar obligations. In all cases, the health care organization should include a provision whereby the vendor agrees to be liable for all acts and omissions of its subcontractor, outsourcers, and other third parties.

D. Compliance

1. Traditional Approach – Traditionally, standard provisions generally require the vendor to warrant that its employees and software comply with relevant statutory and regulatory requirements. Vendors will argue they should only be on the hook to comply with laws and statutes that exist at the time the agreement was executed and they should only be required to comply with laws in the context of their role (i.e., as a “business associate”).

2

2. Changes in Technology or Law – Laws impacting the implementation of HIT are constantly changing.³ It is reasonable to expect more changes in regulatory interpretations and rulemaking regarding fraud and abuse as health care organizations find new ways to promote EHRs. In addition, state laws regarding information security and privacy continue to evolve as state lawmakers seek to protect consumers against identity theft.⁴ In just the past few years, almost every state has enacted its own data breach notification statute.⁵ States are also bolstering laws that govern the use and protection of consumer social security numbers,⁶ financial information,⁷ and biometric information.⁸ Some new state laws have begun to require the implementation of certain technical controls, such as encryption.⁹

And while existing laws, such as HIPAA, require health care organizations to include certain restrictions in vendor contracts, those laws do not permit the health care organization to escape responsibility for the actions of the vendor and the obligations of a vendor may be limited to those prescribed within the contract.

³ *E.g.*, Health Information Technology Legislative Tracking Database, National Conference of State Legislatures, available at http://www.ncsl.org/programs/health/forum/Hitch/HIT_database.cfm; Health Information Technology 2007 and 2008 State Legislation, National Conference of State Legislatures, available at <http://www.ncsl.org/programs/health/forum/Hitch/enacted0708.htm>.

⁴ *E.g.*, Identity Theft Statutes and Criminal Penalties, National Conference of State Legislatures, available at <http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm>; see also Consumer Report Security Freeze State Laws, National Conference of State Legislatures, available at <http://www.ncsl.org/programs/banking/securityfreezelaws.htm>.

⁵ *E.g.*, Breach of Information, National Conference of State Legislatures, available at <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>.

⁶ *E.g.*, Enacted Social Security Numbers Legislation, National Conference of State Legislatures, available at <http://www.ncsl.org/programs/lis/privacy/financeprivacy.htm>, see also Social Security Number Protection Legislation for States, ConsumersUnion.org, available at http://www.consumersunion.org/pub/core_financial_services/004801.html.

⁷ *E.g.*, FinancialPrivacyNow.org, Consumers Union, available at <http://www.consumersunion.org/campaigns/financialprivacynow/learn.html>; see also state laws regarding credit card numbers on receipts and skimming devices laws at <http://www.ncsl.org/programs/lis/privacy/financeprivacy.htm>.

⁸ *E.g.*, Illinois Biometric Information Privacy Act, Public Act 95-0994, 740 ILCS 14/1 (2008) available at <http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=095-0994>.

⁹ *E.g.*, Nevada Revised Statute Section 597.970, available at <http://www.leg.state.nv.us/NRS/NRS-597.html#NRS597Sec970>; Massachusetts Standards for the Protection of Personal Information of Residents of Commonwealth, available at http://www.mass.gov/?pageID=ocamodulechunk&L=1&L0=Home&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17&csid=Eoc.

Thus, a vendor who enters into a standard business associate agreement requiring the vendor to generally comply with all applicable laws, will argue it is only on the hook to comply with the contract and not any other requirements, or that it is only on the hook to comply with laws as they relate specifically to business associates (not covered entities).

3. Considerations – To address these challenges, health care organizations must ensure they provide flexibility in the contract to modify the contract in relation to changes in law that effect *either* party. In addition, health care organizations should require the vendor to comply with all laws “applicable to the performance of obligations hereunder,” including all laws that the vendor would be required to comply with as if it were the health care organization. The vendor must be obligated to apply the same level of effort required of the health care organization or else the health care organization will have to make up the difference itself.

E. Compatibility / Interoperability

1. Traditional Approach – Traditionally, compatibility clauses may be limited to a warranty that the software is operational on the hardware or that the software will not impair the operation of other software installed on the same hardware.

2. Changes in Technology or Law – Technology is becoming much more complex than ever before. Various specialists are required to translate business requirements, technical specifications, and contract terms. Such complexity and diversity of perspectives among stakeholders often leads to ambiguity, confusion, and misunderstanding about the expected project. Unfortunately, these challenges cannot be ignored because advancements in technology are also pushing for all systems to interact.

In addition to changes in technology, some regulations require HIT systems to be compatible and interoperable. For example, in order for organizations to take advantage of the EHR exception to the physician self-referral act and the EHR safe harbor to the anti-kickback statute, the software must be interoperable.¹⁰ In both situations, interoperability is presumed if a certifying body recognized by HHS has certified the software within the prior year.¹¹

In addition to requiring interoperability, a new trend may be emerging that requires organizations to comply with specific information security standards. For example, Nevada and Massachusetts have enacted laws requiring

¹⁰ 42 C.F.R. § 357(w)(2) (physician self-referral act); 42 C.F.R. §1001.952(y)(2) (anti-kickback statute)

¹¹ *Id.*; *see also* HIT Certification, HHS Health Information Technology,

organizations to encrypt certain data.¹² It is possible that other states who have already enacted data breach notification statutes will follow Nevada's and Massachusetts' lead in an effort to show activity in the fight against identity theft.

3. Considerations – As stated above, interoperability of EHR software is presumed if it is certified by a certifying body recognized by the HHS. Until HHS determines through notice and comment rulemaking how it will recognize certifying bodies, the Office of National Coordinator for Health Information Technology (ONC), Health and Human Services, issued interim guidance.¹³

At the time of this publication, only the Certification Commission for Healthcare Information Technology (CCHIT) was recognized by HHS as a certification body,¹⁴ and therefore, only that certification for ambulatory EHR will provide a presumption of interoperability under the anti-kickback statute and physician self-referral act.

There are many “standards”¹⁵ and “certifications”¹⁶ vendors may attempt to highlight in their sales efforts. It is important to know exactly what the certification is, who is the certifying body, and to understand the operational and legal impact of such certification. No standards or certification can provide absolute protection from liability, and so be cautious of vendors who attempt to sell you blue sky.

After conducting such an analysis, the health care organization may wish to include provisions in the contract requiring compliance with specific standards or achievement and retention of a specific certification. Such provisions should require any software, hardware or service not only be compatible/interoperable with other systems within the health care organization (traditional provision), but

¹² E.g., Nevada Revised Statute Section 597.970, available at <http://www.leg.state.nv.us/NRS/NRS-597.html#NRS597Sec970>; Massachusetts Standards for the Protection of Personal Information of Residents of Commonwealth, available at http://www.mass.gov/?pageID=ocamodulechunk&L=1&L0=Home&sid=Eoca&b=terminalcont&f=idtheft_201cmr17&csid=Eoc.

¹³ See Interim Guidance Regarding the Recognition of Certification Bodies, ONC, available at <http://www.hhs.gov/healthit/documents/RCBGuidance.pdf>.

¹⁴ See Press Release: HHS Official Recognizes Certification Body to Evaluate Electronic Health Records, available at <http://www.hhs.gov/news/press/2006pres/20061026a.html>.

¹⁵ E.g., ISO 9001, ISO 27000, NIST 800 Series, etc.

¹⁶ E.g., NIST C&A, ISO 27001, SAS 70, etc.

that it is also compatible/interoperable with industry standards,¹⁷ specific laws,¹⁸ or certain third parties.¹⁹

Other provisions that relate to compatibility/interoperability may address software obsolescence (requiring the vendor to warrant to the organization that it will continue to enhance the software), auditing (permitting the organization to verify compliance with certain standards or compatibility/interoperability requirements)

¹⁷ *E.g.*, CCHIT.

¹⁸ *E.g.*, State law requiring encryption of data transmission.

¹⁹ *E.g.*, Those the organization exchanges information with on an ongoing basis.

II. Designing to HIPAA Compliance²⁰

- How HIPAA's security rules affect system design.

A. Introduction - Although enforcement of HIPAA has been somewhat lacking since its adoption, recent activity seems to indicate that the honeymoon is over. For example, consider the following:

1. 2007 – CMS has begun conducting “surprise” compliance audits.

CMS has authority to conduct compliance reviews of HIPAA “covered entities.”²¹ While almost all enforcement of HIPAA is complaint-driven, health care organizations that were the subject of a complaint may find themselves subject to a compliance review by the government. The first compliance review was conducted in 2007, in which CMS audited Atlanta's Piedmont Hospital.²²

2. July 2008 – HHS entered into its first Resolution Agreement with Providence Health & Services. The Resolution Agreement required Providence to pay \$100,000 and implement corrective measures to address weaknesses and compliance discrepancies regarding its protection of electronic patient information.²³

3. October 2008 – HHS OIG criticizes CMS's oversight and enforcement of HIPAA's Security Rule. In its memo dated October 27, 2008, the HHS OIG stated that CMS has “taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule,” and further recommended CMS

²⁰ See generally Office for Civil Rights, Compliance and Enforcement, *available at* <http://www.hhs.gov/ocr/privacy/enforcement/>; Centers for Medicare & Medicaid Services, Enforcement, *available at* <http://www.cms.hhs.gov/Enforcement/>.

²¹ 45 C.F.R. § 160.308 (Compliance Reviews); *see also* HIPAA Administrative Simplification: Enforcement; Final Rule, 71 Fed. Reg. 8,396 (“Compliance reviews are conducted at the discretion of the Secretary.”); HIPAA Compliance Review Information and Examples, Centers for Medicare & Medicaid Services, *available at* http://www.cms.hhs.gov/Enforcement/09_HIPAAComplianceReviewInformationandExamples.asp.

²² See HIPAA audit at hospital riles health care IT: Industry on edge after feds examine data security procedures at Atlanta facility, ComputerWorld.com, June 15, 2007 *available at* <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024921>; The HIPAA Audit Will Come: Be Prepared, ITBusinessEdge.com, June 19, 2007, *available at* <http://www.itbusinessedge.com/item/?ci=29906>.

²³ See Press Release: HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information, July 17, 2008, *available at* <http://www.hhs.gov/news/press/2008pres/07/20080717a.html>; *see also* Resolution Agreement and Corrective Action Plan *at* <http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf>; *see also* Assurance of Voluntary Compliance entered into between Providence and the Oregon Department of Justice *at* http://doj.state.or.us/releases/pdf/finfraud_providence_avc.pdf.

“establish policies and procedures for conducting HIPAA Security Rule compliance reviews of covered entities.”²⁴

4. December 2008 – ONC publishes new framework for privacy and information security.²⁵ This framework was designed to provide a single, consistent approach to address privacy and security. OCR has also provided a “toolkit” that is designed to supplement other HHS resources, such as the HIPAA Security Information Series.²⁶ While these documents are not binding, they may further define what HHS deems important and may be used to establish a standard of care.

B. Design Considerations – In designing an information system that facilitates the creation, receipt, maintenance or transmission of EHR, most health care organizations must consider the requirements of the HIPAA Security Rule.²⁷ The HIPAA Security Rule is a set of generally accepted security standards designed to protect the confidentiality,²⁸ integrity,²⁹ and availability³⁰ of electronic protected health information.³¹ While there are plenty of resources available for health care organizations

²⁴ Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight (A-04-07~05064), October 27, 2008, available at <http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf>.

²⁵ See Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information, December 15, 2008, available at http://www.hhs.gov/healthit/documents/NationwidePS_Framework.pdf.

²⁶ Privacy and Security Toolkit to implement The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Privacy and Security Framework), OCR, available at <http://www.hhs.gov/ocr/hipaa/hit/>; see also HIPAA Security Information Series, CMS, available at http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp.

²⁷ "Security Standards for the Protection of Electronic Protected Health Information", found at 45 C.F.R. Part 160 and Part 164, Subparts A and C; see also Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003), available at <http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>.

²⁸ Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes. 45 C.F.R. §164.304.

²⁹ Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner. 45 C.F.R. §164.304.

³⁰ Availability means the property that data or information is accessible and useable upon demand by an authorized person. 45 C.F.R. §164.304.

³¹ Electronic protected health information means individually identifiable health information that is transmitted by electronic media or maintained in electronic media and is not related to education records or employment records. Individually identifiable health information is

to learn more about specific administrative, technical and physical security controls,³² the following is a short list of specific standards or safeguards that are very important in the design of EHR, especially in light of recent changes in technology and law: (1) auditing and logging capabilities; (2) end-user security; (3) encryption; and (4) controls ensuring the integrity of the EHR.

1. Audit & Logging Capabilities – HIPAA requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.³³ Unlike many other security standards required by HIPAA, the regulations do not provide additional guidance in the form of implementation specifications for audit controls. Nevertheless, changes in technology and law make this standard more important than ever before.

For example, one of the goals of advancing the implementation of EHR systems is to promote the sharing of EHRs among various entities, including health care providers, payors, and patients. More and more people are going to have access to the EHR, and many may have the capability to modify the EHR. As a result, the health care organization needs to determine which data is accessed, who accessed that data, and what changes (if any) were made to the data. Audit and logging capabilities permit an organization to identify, and possibly reverse, unauthorized or unintended changes to EHRs resulting from error or misconduct.

In addition, data breach notification laws may require health care entities to notify patients if the confidentiality of the EHR stored or transmitted via its system has been compromised by either an internal or external party. Also, HIPAA requires covered entities to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents that become known, and document security incidents and their outcomes.³⁴

information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. §160.103.

³² *E.g.*, HIPAA Security Information Series, CMS, *available at* http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp; NIST Special Publication 800-66, Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, *available at* <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.

³³ 45 C.F.R. § 164.312(b).

³⁴ Mitigation of harmful effects in response to a security incident is required under HIPAA. 45 C.F.R. § 164.308(a)(6); *see also* 45 C.F.R. § 164.530(f) (Privacy Rule's duty to mitigate).

Audit and logging capabilities permit the organization to identify the data that was accessed, and therefore, mitigate harmful effects of such unauthorized access. They can also help the organization focus the investigation and response on the affected data. Otherwise, any determination that a breach occurred may require the organization to provide costly and embarrassing notification to all patients, when in reality only a small portion of the entire record set may have been compromised.

2. Encryption – Under HIPAA, encryption is an “addressable” implementation specification relating to the access control standard³⁵ and the transmission security standard.³⁶ Covered entities must assess whether an “addressable” implementation specification is reasonable and appropriate in its environment. If determined to be reasonable and appropriate, then it must be implemented; otherwise, the covered entity must document why it is not reasonable and appropriate.

Changes in technology and law are making encryption a more reasonable and appropriate measure. Not only does encryption increase the protection of such data, encryption serves as a de facto “safe harbor” under all state data breach notification laws. Most state data breach notification laws require the entity that uses or owns personally identifiable information (PII) to notify all data subjects when *unencrypted* PII is compromised (accessed, stolen, etc.). In addition, some states are now requiring encryption of PII.³⁷

Therefore, health care organizations should consider including encryption of stored data and data in transit in the design of EHR systems.

3. End-User / Employee Security – Under HIPAA, covered entities are required to implement policies and procedures to ensure that only members of its workforce who are authorized to access ePHI have access to such data.³⁸ In addition, the HIPAA Privacy Rule requires covered entities to implement

³⁵ 45 C.F.R. §§ 164.312(a)(1) and (a)(2)(iv) (requires covered entities to implement measures that only allow authorized persons or software programs to access the information system).

³⁶ 45 C.F.R. §§ 164.312(e)(1) and (e)(2)(ii) (requires covered entities to implement measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network).

³⁷ *E.g.*, Nevada Revised Statute Section 597.970, available at <http://www.leg.state.nv.us/NRS/NRS-597.html#NRS597Sec970>; Massachusetts Standards for the Protection of Personal Information of Residents of Commonwealth, available at http://www.mass.gov/?pageID=ocamodulechunk&L=1&L0=Home&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17&csid=Eoc.

³⁸ 45 C.F.R. §164.308(a)(3).

safeguards that limit the access to and disclosure of protected health information to (i.e., patient data) that which is necessary.³⁹

Recent publicity surrounding unauthorized access to health records by health care employees has brought employee security to the forefront.⁴⁰ In fact, California recently expanded laws that protect medical privacy in response to such “employee snooping.”⁴¹ In addition to requiring similar safeguards that are provided in HIPAA, the new California laws provide for private cause of action against health care organizations that negligently release confidential information or records.

While HIPAA’s workforce security standard is classified as an “administrative” safeguard,⁴² certain “technical” safeguards⁴³ should be used to implement workforce security. For example, the access control standard can be implemented to help ensure employees are only able to access EHRs they need to have access to in order to complete their authorized duties.⁴⁴ And the audit control standard (discussed in the previous section), can help health care organizations identify misconduct through monitoring and analysis of audit logs.⁴⁵ Finally, the person or entity authentication standard can help mitigate internal employee misconduct by verifying that a person who seeks access to EHR is who they claim to be.⁴⁶

³⁹ 45 C.F.R. Part 160 and Part 164, Subparts A and E (Privacy Rule); *see also* 45 C.F.R. § 164.514(d).

⁴⁰ *E.g.*, After Hospital’s Celebrity Snooping, a Push for Tougher Penalties, Wall Street Journal, Health Blog, *available at* <http://blogs.wsj.com/health/2008/08/27/after-hospitals-celebrity-snooping-a-push-for-tougher-penalties/>; What’s behind the rash of employee cybersnooping?, ComputerWorld, *available at* <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110280>.

⁴¹ *E.g.*, California Assembly Bill No. 211, *available at* http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0201-0250/ab_211_bill_20080930_chaptered.pdf; California Senate Bill No., 541 *available at* http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0501-0550/sb_541_bill_20080930_chaptered.pdf.

⁴² Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information. 45 C.F.R. 164.304.

⁴³ Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 C.F.R. 164.304.

⁴⁴ 45 C.F.R. § 164.312(a).

⁴⁵ 45 C.F.R. § 164.312(b).

⁴⁶ 45 C.F.R. § 164.312(d) (Person or entity authentication standard).

Therefore, health care organizations should closely analyze all features of an EHR system that can be used to help deter and detect employee misconduct.

4. Integrity of the Record - As stated above, one of the goals of advancing the implementation of EHR systems is to promote the sharing of EHRs among various entities, including health care providers, payors, and patients. This means that information within an EHR may come from various sources not within the control of the health care organization.

This requires the health care organization to identify trusted sources of data and to only permit those sources to be used within the organization. To help reduce the risk that decisions are made based on bad data, the design of any EHR system should provide capabilities to verify the identity of the source of the information⁴⁷ and ensure the data has not been altered.⁴⁸

In summary, in designing or formulating requirements for an EHR system, a health care organization should pay close attention to (1) auditing and logging capabilities; (2) end-user security, (3) encryption, and (4) controls that protect the integrity of the EHR.

It should be noted, too, that in addition to certifying a software's interoperability, CCHIT's certification includes a verification that certain functions and features are included in the software that achieves certification.⁴⁹ Many of these features and functions "map back" to regulatory requirements, including those provided within the HIPAA Security Rule. Therefore, a health care company should always ask a vendor whether their EHR system has achieved CCHIT certification. Even if a particular piece of software is not certified by CCHIT, or if the EHR systems is custom-built, a health care organization may consider analyzing some of the criteria CCHIT makes available to the public in helping formulate design requirements.⁵⁰

⁴⁷ 45 C.F.R. §164.312(d) (Person or entity authentication standard).

⁴⁸ 45 C.F.R. § 164.312(c) (Integrity standard).

⁴⁹ See generally An Introduction to Health IT Certification, CCHIT, available at <http://ehrdecisions.com/wp-content/files/CCHITIntroToHealthIT20090113.pdf>; see also Physician's Guide to Certification for 08 EHRs, CCHIT, available at <http://cchit.org/files/CCHITPhysiciansGuide08.pdf>.

⁵⁰ Relevant criteria is available on the CCHIT website at <http://www.cchit.org/>.

III. Making electronic record systems available to physicians and other providers without violating anti-kickback, Stark, and tax exemption regulations.

- How to enlist provider participation in electronic records implementation without violating regulatory restrictions.

A. Introduction – The **physician self-referral law** (“Stark”) (1) prohibits a physician from making referrals for certain designated health services (DHS) payable by Medicare to an entity with which he or she (or an immediate family member) has a financial relationship (ownership interest, investment interest or compensation arrangement), unless an exception applies; and (2) prohibits the entity from submitting claims to Medicare or billing the beneficiary or third party payor for those referred services, unless an exception applies. The statute establishes a number of exceptions and grants the Secretary the authority to create additional regulatory exceptions for financial relationships that do not pose a risk of program or patient abuse. The **federal anti-kickback statute** provides criminal penalties for individuals or entities that knowingly and willfully offer, pay, solicit, or receive remuneration in order to induce or reward the referral of business reimbursable under any of the Federal health care programs. The types of remuneration prohibited specifically include, without limitation, kickbacks, bribes, and rebates, whether made directly or indirectly, overtly or covertly, in cash or in kind. Prohibited conduct includes not only the payment of remuneration intended to induce or reward referrals of patients, but also the payment of remuneration intended to induce or reward the purchasing, leasing, or ordering of, or arranging for or recommending the purchasing, leasing, or ordering of, any good, facility, service, or item reimbursable by any Federal health care program.

B. Exceptions & Safe Harbors – In order to promote the adoption of electronic health records technology consistent with the goal of achieving fully interoperable electronic health records and prescribing transactions, the Centers for Medicare & Medicaid Services (CMS) of the Department of Health and Human Services (HHS) promulgated two new exceptions to the Stark law. *See* Medicare Program; Physicians’ Referrals to Health Care Entities With Which They Have Financial Relationships; Exceptions for Certain Electronic Prescribing and Electronic Health Records Arrangements; Final Rule, 71 Fed.Reg. 45140 (Aug. 8, 2006); *see also* Stark II (Phase III), 72 Fed.Reg. 51012 (Sept. 5, 2007), Stark II (Phase II), 69 Fed.Reg. 16054 (March 26, 2004). At the same time, the HHS Office of Inspector General (OIG) issued two new safe harbors from the anti-kickback statute that correspond with the new Stark exceptions. *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, Final Rule 71 Fed. Reg. 45110 (Aug. 8, 2006).

C. Stark II Exceptions – The two exceptions to the Stark self-referral prohibition that are most relevant to EHR are the (a) the exception for Electronic Prescribing Items and Services, 42 C.F.R. § 411.357(v) (“e-Prescribing Exception”), and (b) the exception for Electronic Health Records Items and Services, 42 C.F.R. § 411.357(w) (“EHR Exception”). Each of these exceptions permit physicians to receive “nonmonetary”

compensation in the form of certain technology and services that are necessary for the implementation of the electronic prescribing or EHR systems.

1. e-Prescribing Exception permits donation of technology and training that is necessary and used solely to transmit electronic prescription information.

Permitted donations include: (a) hardware; (b) software; and (c) information technology and training services. CMS has interpreted the statutory language to include broadband or wireless internet connectivity, training, information technology support services, and other items and services used in connection with the transmission or receipt of electronic prescription information. In addition, CMS has stated that licenses, rights of use, intellectual property, upgrades, and educational and support services (e.g., help desk and maintenance services) may be permitted donations if all other required conditions are met. Finally, operating software may also qualify for protection if such software is necessary for the hardware to function. 71 Fed. Reg. 45,144

Some technology and services CMS says are excluded include: (a) billing, scheduling, administrative, and other general office software (i.e., no bundled software... must rely on EHR Exception); (b) provision of office staff; and (c) provision of technology used for personal, nonmedical purposes. 71 Fed. Reg. 45,144-45.

2. EHR Exception permits donation of services and “interoperable software” that contains e-prescribing capabilities and is “necessary” and “used predominantly” to create, maintain, transmit, or receive EHR.

Permitted donations include: (a) software packages that include other functionality directly related to the care and treatment of individual patients (e.g., patient administration, scheduling functions, billing, and clinical support); (b) interface and translation software; (c) rights, licenses, and intellectual property related to electronic health records software; (d) connectivity services, including broadband and wireless internet services; (e) clinical support and information services related to patient care (but not separate research or marketing support services); (f) maintenance services; (g) secure messaging (e.g., permitting physicians to communicate with patients through electronic messaging); (h) training and support services (i.e., access to help desk services); (i) EHR system operating within ASP (application service provider) model; and (j) patient portal software. 71 Fed. Reg. 45,151-52.

Expressly excluded EHR technology and services include: (a) hardware (and operating software that makes the hardware function); (b) storage devices; (c) software with core functionality other than electronic health records (e.g., human resources or payroll software); (e) items or services used by a physician primarily to conduct personal business or business unrelated to the physician’s practice; (f) unnecessary software and services (i.e., those recipient already has); (g)

reimbursement for previously incurred expenses; and (h) provision of office staff. 71 Fed. Reg. 45,151-54.

3. Other Potentially Relevant Stark Exceptions – Other potentially relevant exceptions may include the following: (a) Community-Wide HIS, 42 C.F.R. § 411.357(u); (b) Non-Monetary Compensation, 42 C.F.R. § 411.357(k); (c) Fair Market Value Compensation, 42 C.F.R. § 411.357(l); and (d) Medical Staff Incidental Benefits, 42 C.F.R. § 411.357(m).

D. Anti-Kickback Safe Harbors – The safe harbors to the anti-kickback statute relating to EHR include the following: (a) the electronic prescribing safe harbor, 42 C.F.R. § 1001.952(x) (“e-Prescribing Safe Harbor”), and (b) the electronic health records exception, 42 C.F.R. § 1001.952(y) (“EHR Safe Harbor”). Each of these safe harbors set forth conditions under which the provision of technology and services by hospitals, group practices, and prescription drug plan (PDP) sponsors and Medicare Advantage (MA) organizations to certain prescribing health care professionals, pharmacies, and pharmacists would be protected.

The **e-Prescribing Safe Harbor** and the **EHR Safe Harbor** are similar, but not entirely identical to the Stark exceptions discussed above. *See* 71 Fed Reg. 45119. Two significant differences exist: (1) compliance with the anti-kickback statute safe harbor is not the only way to avoid liability under the anti-kickback statute (for instance, there is also a defense available based on lack of intent), but compliance with the Stark exceptions discussed above is required; and (2) the anti-kickback statute applies to all health care providers, whereas Stark generally applies to Physicians only (“Physician” as defined in Stark).

E. Tax Exemption - The Director of Exempt Organizations of the Internal Revenue Service (IRS) issued a short memorandum on May 11, 2007, followed-up by a Q&A, in which the IRS stated that the IRS will not treat the benefits a hospital provides to its medical staff physicians in implementing EHR systems as impermissible private benefit or inurement in violation of section 501(c)(3) of the Internal Revenue Code if the following “safe harbor” elements are met: (1) the arrangements between the medical staff physicians and the hospital required the parties to comply with Stark and anti-kickback statute rules (described above); (2) the hospital is able to access medical records created by physicians pursuant to the subsidized EHR arrangement (to the extent permitted by law); (3) the subsidized EHR software and services are available to all medical staff physicians; and (4) the hospital provides the same level of subsidy to all its medical staff physicians or varies the level of subsidy by applying criteria related to meeting the healthcare needs of the community.⁵¹ Failure to meet the “safe harbor”

⁵¹ IRS memorandum, “Hospitals Providing Financial Assistance to Staff Physicians Involving Electronic Health Records” at <http://www.irs.gov/pub/irs-tege/ehrdirective.pdf> and Q&A at http://ftp.irs.gov/pub/irs-tege/ehr_qa_062007.pdf; *see also* IRS ruling allows hospitals to provide healthcare IT to physicians at <http://www.healthcareitnews.com/story.cms?id=7132>; and IRS

elements previously listed does not constitute a violation; rather, in those situations, the IRS will consider the facts and circumstances of the specific arrangement.

IV. Other Potential Issues

A. What is the Medical Record? – One challenge to consider when selecting or designing an EHR system is how to define what now constitutes the hospital’s or other provider’s medical record. CMS regulations define “electronic health record” as “ a repository of consumer health status information in computer processable form used for clinical diagnosis and treatment for a broad array of clinical conditions.”⁵² This definition may provide insight into what substantive content an EHR may include, but it does not define where a particular provider’s medical record begins and ends. For example, data from an EHR may come from a variety of entities, including health care providers, payors, and the patients. Such data may also be in a variety of physical locations, such as third party internet websites, handheld computers or other mobile devices, desktops or laptops, or on removable media (e.g., disks).⁵³

The rise in personal health records (PHRs) may make it even more difficult to define the “medical record” because PHRs may not be integrated into the health care organization’s EHR system, PHRs are controlled by the patient and not the health care organization, and PHRs may reside in a variety of locations.⁵⁴

B. Record Retention & Record Management – Another challenge in implementing an EHR system is determining whether the health care organization can destroy paper copies of records that have been integrated into the EHR system.⁵⁵ Some state laws may expressly require the retention of the paper record or they may imply a requirement to retain the paper record by requiring the health care entity to provide the “original” to the patient or other health care professional or entity.⁵⁶ On the other hand,

⁵² 42 C.F.R. § 411.351.

⁵³ See generally “Electronic Discovery and Electronic Health Records: The Impact of e-Discovery Involving EHR Upon Healthcare Entities,” Health Lawyers News, May 2007, Gerald, “Jud” DeLoss and Edward F. Shay, *available at* <http://www.gpmlaw.com/uploadedFiles/Resources/Publications/Health-Lawyers-News-Gerald-Jud-DeLoss-May-2007.pdf>.

⁵⁴ See “Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption,” The Practice of Informatics, JAMIA, *available at* <http://www.jamia.org/cgi/reprint/13/2/121.pdf>; see also “The Rise of Personal Health Record: Panacea or Pitfall for Health Information,” Health Lawyers News, Robert L. Coffield and Gerald “Jud” DeLoss, October 2008, *available at* http://www.gpmlaw.com/uploadedFiles/Resources/Articles/Personal-Health-Record_HLN-DeLoss10-2008%20.pdf.

⁵⁵ See “We Now Have Electronic Health Records – When Can We Destroy the Paper?” Compliance Today, January 2009.

⁵⁶ E.g., Colorado Revised Statute Sections 25-1-801 and 802 require a health care facility or provider to “make the original of any such film available to the patient or another health care

some states have adopted the Uniform Electronic Transactions Act (UETA) or the Uniform Photographic Copies of Business and Public Records as Evidence Act, which may allow the electronic copies of records to have the same legal effect as the original.

For example, Colorado has adopted versions of both UETA and the Uniform Photographic Copies of Business and Public Records as Evidence Act. Under Colorado's UETA, if a law requires a record to be in writing, an electronic record satisfies that law.⁵⁷ Also under Colorado's UETA, an electronic record satisfies a law requiring a person to retain a record for evidentiary, audit, or other like purposes, so long as the record accurately reflects the information from the original record and remains accessible for later reference, unless the law requiring retention of such information specifically prohibits the use of an electronic record for the specified purpose.⁵⁸ And under the Colorado Uniform Photographic Copies of Business and Public Records as Evidence Act, the reproduction or copy of a record will have the same legal effect in terms of admissibility as evidence, even if the original record was destroyed in the regular course of business.⁵⁹

On the other hand, Colorado statutes also provides the following:

In the event that a licensed health care professional determines that a copy of any X-ray, mammogram, CT SCAN, MRI, or other film is not sufficient for diagnostic or other treatment purposes, the health facility or entity shall make the original of any such film available to the patient or another health care professional or facility as specifically directed by the patient pursuant to a written authorization request for films and upon the payment of the reasonable costs for such film. If a health facility releases an original film pursuant to this subparagraph (II), it shall not be responsible for any loss, damage, or other consequences as a result of such release.

C.R.S. § 25-1-801(1)(b)(II); *see also* C.R.S. § 25-1-802(1)(b)(II).

So in this example, while it appears Colorado accepts the reproduction of a record in electronic format and permits the destruction of the original, a health care organization should proceed with caution and ensure any reproduction or copy accurately reflects the information contained on the original.

4408152_6.DOC

professional or facility as specifically directed by the patient pursuant to a written authorization-request for films and upon the payment of the reasonable costs for such film.”

⁵⁷ C.R.S. § 24-71.3.107(3).

⁵⁸ C.R.S. §§ 24-71.3-112(1), (6).

⁵⁹ C.R.S. § 13-26-102.

ePrescribing & EHR: Fraud and Abuse Regulations Comparison

Comparison of Regulations

(adapted from the Federal Register, 71 Fed. Reg. 45,141 (Stark), 71 Fed. Reg. 45,111)

	Stark ePrescribing Exception	Stark EHR Exception	AKS ePrescribing Safe Harbor	AKS EHR Safe Harbor
Citation	42 C.F.R. § 411.357(v)	42 C.F.R. § 411.357(w)	42 C.F.R. § 1001.952(x)	42 C.F.R. § 1001.952(y)
Authority	Section 101 of the MMA	Section 1877(b)(4) of the Social Security Act	Section 101 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003.	Section 1128B(b)(3)(E) of the Social Security Act.
Additional Guidance	71 FR 45140 (Aug. 8, 2006)	71 FR 45140 (Aug. 8, 2006)	71 FR 45110 (Aug. 8, 2006)	71 FR 45110 (Aug. 8, 2006)
Required	Mandatory (violation)	Mandatory (violation)	Safe Harbor (case-by-case)	Safe Harbor (case-by-case)
Covered Technology	<p>Items and services that are necessary and used solely to transmit and receive electronic prescription information.</p> <p>Includes hardware, software, internet connectivity, and training and support services.</p>	<p>Software necessary and used predominantly to create, maintain, transmit, or receive electronic health records. Software packages <u>may</u> include functions related to patient administration, for example, scheduling functions, billing, and clinical support.</p> <p>Software <u>must</u> include electronic prescribing capability.</p> <p>Information technology and training services, which would include, for example, internet connectivity and help desk support services.</p> <p>This exception excludes hardware, storage devices, software with core functionality other than EHR, and items or services used for personal or other businesses</p>	<p>Items and services that are necessary and used solely to transmit and receive electronic prescription information.</p> <p>Includes hardware, software, internet connectivity, and training and support services.</p>	<p>Software necessary and used predominantly to create, maintain, transmit, or receive electronic health records. Software <i>must</i> include an electronic prescribing component.</p> <p>Software packages may also include functions related to patient administration, for example, scheduling, billing, and clinical support.</p> <p>Software must include electronic prescribing capability.</p> <p>Information technology and training services, which could include, for example, internet connectivity and help desk support services.</p> <p>Does not include hardware.</p>
Standards with Which Donated Technology Must Comply	Applicable standards for electronic prescribing under Part D (currently, the first set of these standards is codified at 42 C.F.R. § 423.160).	Electronic prescribing capability must comply with the applicable standards for electronic prescribing under Part D (currently, the first set of these standards is codified at	Final standards for electronic prescribing as adopted by the Secretary.	Electronic health records software that is interoperable. Certified software may be deemed interoperable under certain circumstances.

ePrescribing & EHR: Fraud and Abuse Regulations Comparison

	Stark ePrescribing Exception	Stark EHR Exception	AKS ePrescribing Safe Harbor	AKS EHR Safe Harbor
		42 C.F.R. § 423.160). Electronic health records software must be interoperable. Software may be deemed interoperable under certain circumstances.		Electronic prescribing capability must comply with final standards for electronic prescribing adopted by the Secretary.
Donors and Recipients	As required by statute, protected donors and recipients are hospitals to members of their medical staffs; group practices to physician members; prescription drug plan (PDP) sponsors and Medicare Advantage (MA) organizations to prescribing physicians.	Entities that furnish designated health services (DHS) to any physician.	As required by statute, protected donors and recipients are hospitals to members of their medical staffs, group practices to physician members, prescription drug plan (PDP) sponsors and Medicare Advantage (MA) organizations to network pharmacists and pharmacies, and to prescribing health care professionals.	Protected donors are (i) individuals and entities that provide covered services and submit claims or requests for payment, either directly or through reassignment, to any Federal health care program and (ii) health plans. Protected recipients are individuals and entities engaged in the delivery of health care.
Selection of Recipients	Donors may not take into account directly or indirectly the volume or value of referrals from the recipient or other business generated between the parties.	Donors may use selection criteria that are not directly related to the volume or value of referrals from the recipient or other business generated between the parties.	Donors may not select recipients using any method that takes into account the volume or value of referrals from the recipient or other business generated between the parties.	Donors may not select recipients using any method that takes into account <i>directly</i> the volume or value of referrals from the recipient or other business generated between the parties.
Value of Protected Technology	No limit on the value of donations of electronic prescribing technology. No cost sharing requirement.	Physician recipients must pay 15 percent of the donor's cost for the donated technology and training services. The donor may not finance the physician recipient's payment or loan funds to the physician recipient for use by the physician recipient to pay for the items and services.	No limit on the value of donations of electronic prescribing technology. No cost sharing requirement.	Recipients must pay 15% of the donor's cost for the donated technology. The donor (or any affiliate) must not finance the recipient's payment or loan funds to the recipient for use by the recipient to pay for the technology.
Expiration	None	Exception sunsets on Dec. 31, 2013.	None	Exception sunsets on Dec. 31, 2013.