RM

NATIONAL ASSOCIATION OF Community Health Centers

RISK MANAGEMENT SERIES

Medical Records: Managing Risk in the Conversion from Paper to Electronic Format

Jacqueline C. Leifer, Esq.
Marisa B. Guevara, Esq.
Adam J. Falk, Esq.
Feldesman Tucker Leifer Fidell LLP
Washington, DC

For more information contact:

Betsy Vieth
National Association of Community Health Centers, Inc.
7200 Wisconsin Avenue, Suite 210
Bethesda, MD 20814
Telephone (301) 347-0400
Email: BVieth@nachc.com

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is published with the understanding that the publisher is not engaged in rendering legal, financial or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The Health Resources and Services Administration, Bureau of Primary Health Care (HRSA/BPHC) supported this publication under Cooperative Agreement Number U30CS08661-02-00. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of HRSA/BPHC.

Health information technology (Health IT) presents significant legal issues as "old laws" collide with "new technology." But many of these legal issues can be successfully addressed by adapting the underlying legal principles to the new technology. For example, laws governing the confidentiality of medical information mean the same thing regardless of whether the health center's medical records are stored in file cabinets or on computers. In either case, the "doors" to the medical record cabinet should be locked when not in use.

If it has not already, your health center will soon face the question of whether to implement an electronic records system. The enactment of the American Recovery and Reinvestment Act (ARRA) offers significant incentives for health centers and other providers to implement an electronic health records (EHR) system, such as loan programs and grants to support various aspects of the transition to electronic records.[1]

The process of converting paper records to an electronic format can be broken down into four steps – creating, storing, sharing, and destroying the electronic record.

1 ARRA, Pub. L. 111-005 was signed into law by President Obama on February 17, 2009. Title XIII of ARRA contains the health information technology provisions and is titled Health Information Technology for Economic and Clinical Health (HITECH Act).

For each step, a number of legal issues arise that need to be adequately addressed by health centers as they convert from paper to electronic medical records. To assist health centers that are in the process of implementing electronic records, this Information Bulletin:

- Explores each of the four steps in converting from paper records to an electronic system;
- Identifies the legal issues that may arise during the conversion of a paper-based medical record system to an electronic format;
- Reviews the applicable legal requirements;
- Recommends ways to address compliance with legal requirements.

CREATING THE ELECTRONIC RECORD

Can a Health Center Accept Donated Equipment to Use in Creating an Electronic Records System?

Federal fraud and abuse law is intended to prevent fraudulent or abusive arrangements between or among providers that could result in higher costs to the federal government or compromise the quality of care provided to beneficiaries of Medicare, Medicaid and/or other federal health care programs. The Office of Inspector General (OIG) and the Centers for Medicare and Medicaid Services (CMS) within the Department of Health and Human Services (HHS) have been charged with implementing and enforcing two of these laws – the federal Anti-Kickback statute and the Stark law. In the context of electronic medical records, both agencies have issued regulations that allow health centers and other providers to accept donated equipment for electronic records and electronic prescribing that would otherwise be prohibited under fraud and abuse, in particular, the Anti-Kickback and Stark laws and regulations.

Accepting Donated Equipment under the Stark Law

Typically, the Stark law (*i.e.*, the physician self-referral prohibition) prohibits a physician from referring a Medicare or Medicaid patient to another physician or provider that furnishes certain health services in which the referring physician has a financial interest or relationship if the services will be paid for by Medicare or Medicaid. There are, however, certain statutory and regulatory exceptions to the Stark law and if an arrangement meets all of the requirements of a specific exception, the arrangement will not be prohibited under the Stark law.

CMS has issued an exception that covers physician compensation, including non-monetary remuneration (*e.g.*, the donation of equipment) that is "necessary and used solely to receive and transmit electronic prescription information" for "certain arrangements involving the provision of non-monetary remuneration in the form of electronic health records software or information technology and training services necessary and used predominantly to create, maintain, transmit, or receive electronic health records."[2] This exception, for example, would allow a local hospital to donate electronic records equipment to a health center to permit the sharing of medical records between the hospital and health center.

Accepting Donated Equipment under the Anti-Kickback Law

Ordinarily, the federal Anti-Kickback statute prohibits health care providers from knowingly offering, soliciting or receiving remuneration in exchange for referrals of patients, items or services paid for, in whole or in part, by Medicare, Medicaid and/or other federal healthcare program. (42 U.S.C. § 1320a-7b(b)). This means that a provider, in this case a health center, cannot enter into referral arrangements where the health center offers or receives money, property or other benefits in exchange for making or receiving referrals. Similar to the Stark law, there are statutory and regulatory "safe harbors" – if an arrangement

2 71 *Fed. Reg.* 45140 (August 8, 2006).

meets all of the requirements of a specific safe harbor, it will be exempt from scrutiny under the Anti-Kickback statute. Unlike the Stark law exceptions, however, arrangements that do not meet safe harbor requirements will be reviewed on a case-by-case basis to determine whether they violate the Anti-Kickback statute.

The OIG has established a safe harbor that is more limited than the Stark exception, covering only donations of software and training services related to electronic health records or health information technology.[3] However, other non-monetary remuneration, such as hardware, may be protected under the general health center safe harbor that protects donations to grant-funded Federally Qualified Health Centers (FQHCs), so long as the arrangement meets the nine requirements listed therein.[4] Indeed, the broader protections under this safe harbor could permit a broad range of donations of items, services, and remuneration to health centers.

Is a Health Center Liable for Errors or Misstatements Contained in a Patient's Electronic Record?

Theoretically, a health center could be liable for an error in a patient's electronic record that caused harm to a patient if the health center did not meet the standard of care for medical record keeping. For example, a court might determine that the health center should have implemented certain processes to ensure that the medical records are kept up-to-date or that known health risks, if relevant, were displayed prominently on the medical record. However, such a determination appears unlikely given the lack of a recognized standard for medical recordkeeping.

Nevertheless, it is important to recognize that such potential liability (however unlikely) exists regardless of whether the medical record is in paper or electronic format. Unless the error was created during the conversion process to electronic format, both paper and electronic medical records are susceptible to misstatements, inaccuracies, or incompleteness. In either event, federally-funded health centers are covered by the Federal Tort Claims Act (FTCA) for medical malpractice actions arising out of these or similar errors involving medical records.

A federally-funded health center may apply to HHS to have its employees, officers, and directors deemed to be federal employees and therefore protected under the FTCA, which is "the legal mechanism for compensating people who have suffered personal injury by the negligent or wrongful action of employees of the US government."[5] In general, deemed health centers are covered by FTCA for medical malpractice actions for personal injury that arise from acts or omissions conducted within the health center's scope of project and committed by health center employees (and certain contractors) who were acting within their scope of employment.[6]

Accordingly, health centers should be protected under FTCA for malpractice actions arising out of electronic record errors so long as the underlying service was furnished within the health center's scope of project and the employee was acting within his/her scope of employment. For example, FTCA would cover liability caused by an adverse drug reaction that resulted from an incomplete electronic record but would not cover liability caused by an employee

3 42 C.F.R. § 1001.952(y). *See also* 71 Fed. Reg. 45136 (August 8, 2006).

4 The health center safe harbor is codified at 42 C.F.R. § 1001.952(w). *See also* 72 Fed. Reg. 56644 (October 4, 2007). The health center safe harbor covers only health centers receiving funds under Section 330. Additional information on the health center safe harbor is available in Issue Brief #91 of the Medicare/Medicaid Technical Assistance Series – *The Final Health Center Safe Harbor Rule: What Is It & What Does It Mean For You?*, which is available on-line at http://www.nachc.com/client/documents/publications-resources/IB_91_08.pdf.

5 The Federal Health Center Program: Federal Tort Claims Act, *available at* http://bphc.hrsa.gov/FTCA/ (accessed June 4, 2009).

6 Additional information regarding FTCA coverage is available in numerous Issue Briefs and Information Bulletins, on-line at http://iweb.nachc.com/Purchase/SearchCatalog.aspx.

who illegally stole patient health or financial information because that employee would be acting outside his or her scope of employment. In addition, FTCA does not extend coverage to a health center's vendors, so FTCA would not protect a health center from liability arising from the errors or mistakes caused by the center's health records vendor.

Is a Health Center Required to Retain Paper Records after Converting to an Electronic Record System?

Health centers and other health care providers are required to retain patient records after the completion of treatment.[7] To determine the applicable legal requirements, health centers should:

- Review any applicable federal law;
- Consult state law for specific record retention requirements for patient records, noting any distinctions based on the patient's status; and
- Determine whether the laws require the medical records to be stored in any particular format.

Federal Law Pertaining to Record Retention

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a covered entity[8] (here, a health center) must take certain steps to protect patient information stored in medical records. HIPAA designates the information to which it applies as "individually identifiable health information."[9] There are two sets of regulations that apply to individually identifiable health information.

The HIPAA Privacy Rule — applies to health information stored in both paper and electronic formats. Under the Privacy Rule, a health center must be able to produce a patient record upon request or proper authorization.[10] HIPAA does not specify whether this record must be paper or electronic, just that an individual has a right to a copy of his or her record.[11] If the health center chooses to send copies of its records to an outside contractor to be scanned or otherwise imported into the electronic records system, the health center:

- Must retain the ability to produce the records for a patient with a valid authorization;[12]

7 Additional information regarding document retention and destruction is available in Risk Management Information Bulletin #18, *Record Retention Requirements for Business, Financial, and Clinical Information -- Risk Management Series*, which is available on-line at http://www.nachc.com/client/documents/publications-resources/rm_18_07.pdf.

8 Covered entities are defined as healthcare clearinghouses, health plans, and healthcare providers that transmit health information in an electronic format that pertains to claims processing, eligibility, enrollment, or payment. 45 C.F.R. § 160.103.

9 Individually identifiable health information is "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) related to the past, present, or future physical or mental 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. *Id.*

10 45 C.F.R. § 164.524.

11 The HIPAA Privacy Rule's Right of Access and Health Information Technology, U.S. Department of Health and Human Services, Office of Civil Rights (December 15, 2008), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/index.html (accessed June 5, 2008). However, the HITECH Act requires that covered entities under HIPAA using electronic health records be able to produce an electronic copy of an individual's record for an individual who so requests. *See* Pub. L. 111-005, Title XIII, Section 13405(e).

12 If the health center is using an outside source to convert the records, then HIPAA requires that a business associate agreement be in place between the two organizations. The ARRA also makes significant changes to business associate agreements. Business associate agreements are discussed in the next section, *Storing Electronic Health Records.*

- Should keep a list of all records that have been given to the contractor in the event that the contractor loses a record or claims it never received a record.

To ensure compliance with this provision, paper records should be kept for a reasonable amount of time after conversion in case there are any errors or problems with retrieving records.

The HIPAA Security Rule — applies only to health information that is stored in an electronic format.[13] The HIPAA Security Rule is discussed in greater detail in the next section, *Storing Electronic Health Records*.

State Laws Pertaining to Record Retention

State law governs how long and in what format(s) medical records must be retained. State law may also dictate who owns the medical record (which, in most cases, is the provider, not the patient).

The Uniform Electronic Transactions Act — Regarding electronic records, many states have adopted the Uniform Electronic Transactions Act (UETA).[14] This set of uniform laws contains definitions and requirements for electronic records and transactions and likely applies to electronic records systems. In states that have enacted the UETA, an electronic record can be an original record in certain situations. For example, in Maryland the electronic record is an original record if it accurately sets forth the information in the record at the time it was created and remains accessible for later reference.[15] Three states have not yet adopted the UETA.[16] In those states, and even in states that have adopted the UETA, it may be permissible to store records in microfiche or other reproducible, accessible electronic storage format.

Confidentiality rules — State law may also have confidentiality rules or other privacy protections that apply. It is important to note that if any confidentiality or privacy protections found in state law offer more protection to the patient than the protection provided in HIPAA, the health center must follow the state law. In any event, it is important to check state law before beginning conversion, so that the health center can make informed decisions about record retention and other aspects of the conversion process.

Recommendations Pertaining to Record Retention

At a minimum, health centers should have copies of patients' medical records that:

- Are easily accessible to a clinician to review;
- Can be provided to the patient upon request; and
- Meet their particular state's record retention requirements.

Even if a state permits a provider to store an electronic version of the original paper medical record (such as a scanned electronic copy), paper records should be maintained until the information in the electronic record has been verified as true and accurate, and the system has been tested for errors. Following such verification, paper records should be retained for a reasonable period of time (even if stored off-site), as determined by the health center prior to any document destruction. The safest approach would be to retain paper records for the full retention period under state law, if not overly burdensome or expensive.

13 In addition, different federal agencies within HHS are charged with implementation and enforcement of these Rules. The Privacy Rule is enforced by the Office of Civil Rights (OCR), while the Security Rule is enforced by the Centers for Medicaid and Medicare Services (CMS).

14 Uniform rules are created by the National Conference on Uniform State Laws to create uniformity among state laws in certain areas. However, each state may adopt or amend the laws as it sees fit.

15 Md. Code Ann. Com. Law § 21-111 (2008).

16 Those three states are: Illinois, New York, and Washington. *See* http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-ueta.asp (accessed June 5, 2009).

STORING ELECTRONIC HEALTH RECORDS

Storing electronic health records involves many of the same considerations as storing paper records. For example, electronic hardware, like paper records, will need to be secured to prevent theft and tampering, and should maintain confidentiality of the information. But unlike paper records, the HIPAA Security Rule places strict requirements on the hardware and software used for electronic records.

What are the General Requirements of the HIPAA Security Rule?

The Security Rule requires covered entities to follow four general requirements:

1. Ensure the confidentiality, integrity, and availability of all "electronic protected health information" (ePHI) the covered entity creates, receives, maintains, or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and
4. Ensure compliance with the provisions of the Security Rule by its workforce.

To comply with these principles, a health center must implement the administrative, physical and technical safeguards described in the HIPPA Security Rule.[17]

Administrative Safeguards

These are defined as "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."

Physical Safeguards

Physical safeguards are "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

Technical Safeguards

These are defined as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

These safeguards include a "Security Management Process" consisting of "policies and procedures to prevent, detect, contain and correct security violations."[18] The Security Management Process requires covered entities to:

- Conduct a risk analysis;
- Engage in risk management practices;
- Create and enforce a sanctions policy; and
- Routinely conduct an information system activity review.

The risk analysis should be conducted early on in the conversion process, during a test phase if there is one, so that the health center can correct or mitigate any existing threats or vulnerabilities.

17 45 C.F.R. § 164.304.

18 45 C.F.R. § 164.308(a)(1)(i).

What are the Technical Requirements Related to the Physical Storage of Health Information?

In regard to the storage of electronic records, the HIPPA Security Rule imposes technical requirements relating to the physical storage of health information. These physical safeguards protect the facility and physical equipment that store or transmit electronic protected health information (ePHI).

Physical Access and Workstations

Health centers that are converting from paper medical records to electronic format must have methods to limit physical access to the hardware or to workstations that permit access to electronic records software, such as key locks or access codes. Generally, health centers should consider placing workstations in restricted areas to limit access to employees and authorized users. In addition, there should be methods to limit access to certain classes of employees.

Controls for Laptops or Other Mobile Devices

If a health center plans to use laptops or mobile devices as part of its electronic records system, there should be a log tracking which employee took which laptop, when the laptop was taken, and when it was returned. Further, before the laptop is taken off-site from the health center, any data on the laptop should be backed up onto a drive that remains on-site at the health center. These same laptops should be password protected to prevent unauthorized access.

Safeguards for Software Systems

In addition, a health center's hardware and software systems that are used to create, transmit, or store ePHI must comply with certain technical safeguards. Under the Security Rule, software must have the capability to create an audit trail of a user's activity on any machine that is used for the creation, transmission, or storage of ePHI[19] and use "electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner". [20] These specifications should be discussed with a health center's vendor of electronic records to ensure that the software complies with the Security Rule.

If a Health Center Stores Its Electronic Records Off-Site at a Third Party Data Center, How Do the HIPAA Security Rules Apply?

Business Associate Arrangements

For the records stored off-site, the health center must have in place a written business associate agreement with the third party storing the information.[21] As long as a health center obtains "satisfactory assurances that the business associate will appropriately safeguard the information," it may disclose protected health information[22] (PHI) and ePHI (PHI stored in an electronic format) to business associates. Further, the health center's business associates may create or receive PHI/ePHI on the health center's behalf, in accordance with the Privacy and Security Rules.[23]

During the transition phase to electronic records, it is fairly common to store existing paper records by scanning to an electronic file and adding the files to the electronic record. This eliminates the bulk of the paper records, but maintains their authenticity, by taking a digital, photographic image of the paper record. Maintaining a static electronic copy of the record also allows the records to be easily accessed during the transition period, to verify information, or

19 45 C.F.R. § 164.312(b).

20 45 C.F.R. § 164.312(c)(2).

21 *See* 45 C.F.R. § 160.103; 45 C.F.R. § 164.308(b)(4).

22 Protected health information is defined in the HIPAA regulations as individually identifiable health information that is stored or transmitted in any electronic or other form or medium. 45 C.F.R. § 160.103.

23 45 C.F.R. § 164.502(e)(1)(i).

to import information into the new electronic record template. Further, the electronic copy can be locked to prevent any modifications of the record, so there is a complete copy of the record as it was on the day that it was scanned.

If the records are going to be scanned by an independent contractor or other specialist, a business associate agreement must be executed with those individuals, as they will have access to PHI on behalf of the health center. Since the scans will result in electronic information, the business associate agreement should cover the HIPPA Security and Privacy Rules. The same rules that apply to business associate agreements for organizations that are responsible for converting the records will apply to organizations that are responsible for permanent storage and maintenance of the electronic hardware and data for a health center's electronic records system.

ARRA-Related Changes to Business Associate Arrangements

ARRA makes significant changes to the relationship between a covered entity (the health center) and its business associates. Effective February 17, 2010, business associates are independently responsible for protecting the ePHI (and PHI) that they create, maintain, or receive from a covered entity and must comply with the safeguards and implementation specifications listed in the Security Rule. In addition, business associates will be subject to civil and criminal penalties for violations of the Security and Privacy Rules.[24]

Despite a business associate's liability for failing to comply with the Security Rule, covered entities will continue to be responsible for ensuring the business associate's compliance with the business associate agreement. For example, a health center is required to terminate a business associate agreement if the center determines that the business associate is exhibiting a pattern of behavior that constitutes a material breach of the contract.[25]

ARRA also expands the class of entities defined as business associates. Business associates will include the following types of organizations:

- An organization that provides data transmission of PHI for a covered entity and that requires access on a routine basis to PHI, such as:
  - Health Information Exchange Organization
  - Regional Health Information Organization
  - E-Prescribing Gateway
- A vendor that contracts with a health center to allow it to offer a personal health record to patients as a part of their electronic health record.

If a health center contracts with or participates in any of these arrangements, under ARRA it must now have business associate agreements in place with the organizations involved. This will offer additional protection to a health center by directly applying the Privacy Rule, Security Rule, and associated civil and criminal penalties to those organizations that deal with large quantities of ePHI.

What Should a Health Center Do If It Experiences a Power Outage or Other Emergency Situation or Natural Disaster?

The HIPPA Security Rule requires a covered entity to have a disaster recovery plan, which will likely include off-site, electronic back-up of records. Such off-site services should be accessible in the event

24 "In the case of a business associate that violates any security provision specified in subsection (a), sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision." American Recovery and Reinvestment Act, Pub. L. 111-005, Title XIII, Subtitle D, Part 1, Section 13401(b).

25 This obligation runs both ways. The new ARRA provisions also create a responsibility for business associates to terminate business associate agreements with any covered entities that are exhibiting a pattern of behavior that constitutes a material breach of the covered entity's obligations under the business associate agreement. Similar to covered entities, however, the business associate may not have to terminate the agreement if the covered entity takes reasonable steps to end the violation.

of an emergency. To ensure than off-site records are current, records should be backed up periodically so that the back-up record is as close a copy of the current record as possible. This will ensure compliance with the Security Rule and reduce the risk of error.

In addition, health centers should consider having back-up power supplies or generators sufficient to run their information technology, or at least a minimum version of it. Alternatively, health centers might consider utilizing off-site data centers that would allow remote access in case of an emergency. An off-site data center will allow a health center to still access information, but may require less power than if the health center operated its own.

SHARING ELECTRONIC RECORDS

If a health center decides to share electronic records with other providers or to participate in health information exchange, there are several legal issues to consider. The first issue to consider in sharing electronic records, which contain ePHI, is whether a business associate agreement is required. Other issues with sharing electronic records include interoperability and security standards. These issues are discussed in further detail below.

Do Electronic Records Have to Be Interoperable?

Although electronic records are not required to be interoperable, there are several advantages to using interoperable electronic records, including:[26]

- If the records are not interoperable, it will be extremely difficult, if not impossible to share those records electronically with other providers, like a nearby hospital.
- ARRA establishes certain financial incentives for health centers and other entities to adopt interoperable records that "support the nationwide electronic exchange and use of health information in a secure, private, and accurate manner…"[27]
- Federal policy, as reflected in ARRA, defines "EHRs" and "certified EHRs" as interoperable. Therefore, a health center should consider using interoperable medical record systems.

How Does the HIPAA Security Rule Apply to Sharing Records?

The HIPPA Security Rule contains requirements that apply to the sharing of ePHI, including electronic health records. The technical safeguards for "transmission security" require a covered entity to "implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network." An electronic communications network includes the internet, telephone lines, and fax lines.

Compliance with this technical safeguard can be accomplished by encrypting data during transfer over an electronic communications network, such as when sending emails or faxes. A business associate agreement may also be necessary for sharing records electronically. If electronic medical records will be shared through a health information exchange, a regional health information organization, or an e-prescribing gateway, then a common business associate agreement must be in place between the health center and each of the other organizations.

26 It is likely that the electronic records system is interoperable, but to verify check with the vendor of your electronic records system.

27 Pub. L. 111-005, Title XIII, Section 13301 (February 17, 2009).

How Does a Health Center Document a Patient's Authorization for Release of Protected Health Information Stored in an Electronic Record?

To document a patient's authorization for the release of electronic records, health centers can use either the same paper authorization that they used before converting to electronic format or they can obtain an electronic signature from the patient. Under the Electronic Signatures in Global and National Commerce Act (ESIGN) (Pub. L. 106-229 (June 30, 2000), a signature cannot be denied legal effect simply because it is in an electronic format.[28] However, health centers should consider taking measures to authenticate and verify an electronic signature of any patient.

DESTROYING ELECTRONIC RECORDS

Pursuant to the HIPPA Security Rule, a health center using electronic records must have policies and procedures in place for the final disposal of ePHI and hardware and other electronic media when it is no longer needed. For example:

- If a health center wants to change the way it uses a particular computer, it must first remove any ePHI stored on the computer.
- A computer or hard drive that is no longer needed must be erased prior to destruction so that any ePHI once stored on the machine is irretrievable.
- Other procedures for destroying records must conform to current technology standards.

CONCLUSION

There can be no doubt that converting to an electronic records system from paper format implicates a broad range of legal requirements. Nevertheless, the federal government has invested in health information technology such technology is expected to transform primary care practice at health centers and other providers. The best approach is to address the legal requirements at each step, create an effective plan to manage the associated compliance risks, and regularly re-evaluate compliance with the legal requirements.

28 Pub. L. 106-229 at Section 101(a)(1).

Glossary

Personal Health Record — A personal health record (PHR) is "an electronic record of PHR identifiable health information … on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[29] "PHR identifiable information" is individually identifiable health information that is provided by or on behalf of an individual and identifies or could reasonably be used to identify the individual.[30] Thus, the distinguishing characteristic of a PHR is that the information is controlled and edited by the consumer.

Electronic Health Record — An electronic health record is "[a]n electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization."[31] The Medicare program defines an 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."[32] The Health Information Technology for Economic and Clinical Health Act (HITECH Act)[33] within ARRA also includes a definition of a "qualified electronic health record" that is an electronic record of health related information that "includes patient demographic and clinical health information" and has the capacity to:

- Provide clinical decision support;
- Support physician order entry;
- Capture and query information relevant to health care quality;
- Exchange electronic health information with, and integrate such information from other sources.[34]

The key distinction between an ***electronic health record*** and an ***electronic medical record*** is that an electronic health record has the capability to operate across more than one organization or platform.[35] However, by tying the federal grants, loans, and other financial incentives related to Health IT to the implementation of electronic health records, the HITECH Act makes it clear that the government is strongly encouraging the development and use of qualified electronic health records, with the goal of creating nationwide health information exchange.[36] This policy favors the interoperable electronic health record because it does not confine data to one organization.[37] One report has gone so far as to say that "the term EMR is on course for eventual retirement."[38]

Computerized Provider Order Entry (CPOE) — A computer application that allows a physician's orders for diagnostic and treatment services (such as medications, laboratory, and other tests) to be entered electronically instead of being recorded on order sheets or prescription pads. A CPOE compares the physician's order with dosage standards, patient allergies, and adverse interactions with existing medications.

Interoperable — Technology that is able to communicate and exchange data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks, in various settings; and exchange data such that the clinical or operational purpose and meaning of the data are preserved and unaltered." 42 C.F.R. § 411.351.

Electronic Prescribing — A type of computer technology whereby physicians use handheld or personal computer devices to review drug and formulary coverage and to transmit prescriptions to a printer or to a local pharmacy. E-prescribing software can be integrated into existing clinical information systems to allow physician access to patient specific information to screen for drug interactions and allergies.[39]

29 *American Recovery and Reinvestment Act*, Pub.L. 111-005, Title XIII, Section 13400 (February 17, 2009).

30 *Id.* at Section 13407(f)(2).

31 *See* "Defining Key Health Information Technology Terms," The National Alliance for Health Information Technology, Report to the Office of the National Coordinator for Health Information Technology (April 28, 2008), *available at* www.nahit.org/images/pdfs/HITTermsFinalReport_051508.pdf (accessed June 2, 2009), at 6.

32 42 C.F.R. § 411.351. The OIG Safe Harbor regulations for electronic prescribing and electronic health records use the same definition of electronic health record. *See* 42 C.F.R. § 1001.952(y).

33 The HITECH Act is the short title given to Title XIII of the American Recovery and Reinvestment Act ("ARRA"), Pub. L. 111-005, signed by President Obama on February 17, 2009.

34 Pub. L. 111-005, Section 13101.

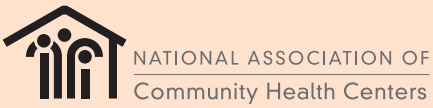
35 Defining Key Health Information Technology Terms, *supra*, at 6.

36 Pub. L. 111-005, Section 13101.

37 An electronic medical record is "[a]n electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization." Defining Key Health Information Technology Terms, *supra*, at 6.

38 *Id.* at 5.

39 *See, e.g.,* http://healthit.hhs.gov/portal/server.pt?open=512&objID=1256&parentname=CommunityPage&parentid=2&mode=2&in_hi_userid=10741&cached=true.



7200 Wisconsin Avenue, Suite 210

Bethesda, MD 20814

Telephone: 301-347-0400

Fax: 301/347-0459

Website: www.nachc.com