



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

ELECTRONIC MEDICAL RECORDS

Do I need them? What's Required?

Every private physician and small practice is now asking themselves these two questions. There are no laws that specifically say you must convert all your paper patient records to electronic medical records. **NOT YET!!** But many federal and state healthcare agencies and insurance companies now require electronic copies of information. However there are laws that impose heavy fines and penalties for exposing, unauthorized sharing and lack of proper security and maintaining the privacy of Patient Information.

If you have records say:

- Stored in an open office area
- Stored in your basement
- Stored in a storage unit
- Accessible to maintenance or cleaning staff
- If you fax PHI
- Accessible to medical staff with no means of tracking the who, where, and why aspects of access to patients records and protecting the patient's privacy.
- Stored in file cabinets in hallways or an associates office.
- Records taken home by staff for review
- Billing coders access to records
- Share records with other doctors, clinics, and hospitals.

You may be exposed!!!



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

After reading the following rules that apply to patient records you will begin to realize the benefit and importance of converting all PHI in your possession to an electronic format that you can secure and track its use. The most recent Economic Recovery Act of 2009 includes provision for the use of electronic medical records to reduce healthcare cost, expedite patient processing and access to information in an emergency, better records management and to protect PHI.

Under HIPAA there are two aspects of the law.

A. The *medical privacy rule* creates national standards intended to protect individuals' medical records and other personal health information by establishing limits on the use and release of patients' health information. The rule protects patient health records *in any format* -written, typed, oral, and electronic. Generally, the medical privacy rule requires activities, such as the following:

1. Notifying patients about their privacy rights and how their information can be used
2. Adopting and implementing privacy procedures
3. Training employees so that they understand these privacy procedures
4. Designating an individual to be responsible for seeing that these privacy procedures are adopted and followed
5. **Securing patient records containing individually identifiable health information** so that they are not readily available to those who do not need them.

B. The *security rule* is a set of national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. It requires all covered entities to complete an assessment of their risks and vulnerabilities and to implement security measures to reduce those identified to a reasonable and appropriate level. The security rule contains requirements for the following:



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

1. Implementing administrative, physical, and technical safeguards
2. Developing security policies and procedures
3. Documenting the assessment of the reasonableness of certain implementation specifications for the organization
4. Training all of the organization's workforce on the security procedures
5. Revising agreements with business associates to incorporate security obligations for the business associate.

In contrast to the medical privacy rule, the security rule protects *only electronic* health information, addressing all aspects of the security of electronic information while it is in use, in storage, or being exchanged between entities.

Federal Law

HIPAA

The HIPAA Privacy Rule (45 CFR Parts 160 and 164) provides the "federal floor" of privacy protection for health information in the United States, while allowing more protective ("stringent") state laws to continue in force. Under the Privacy Rule, protected health information (PHI) is defined very broadly. PHI includes individually identifiable health information related to the past, present or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Even the fact that an individual received medical care is protected information under the regulation.

The Privacy Rule establishes a federal mandate for individual rights in health information, imposes restrictions on uses and disclosures of individually identifiable health information, and provides for civil and criminal penalties for violations. The complementary Security Rule includes standards for protection of health information in electronic form.

Rights Under the Privacy Rule

The individual, who is the subject of Protected Health Information (PHI), has the following rights under the Privacy Rule:



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

- Right to in an expedient manner access, inspect and copy PHI held by hospitals, clinics, health plans and other "covered entities," with some exceptions
- Right to request amendments to PHI held by "covered entities"
- Right to request an accounting of disclosures that have been made without authorization to anyone other than the individual for purposes other than treatment, payment and health care operations
- Right to receive a Notice of Privacy Practices from doctors, hospitals, health plans and others in the health care system
- Right to request confidential communications of PHI, e.g., having PHI transmitted to a different address or a different telephone number securely.
- Right to request restrictions on uses or disclosures, although the "covered entity" receiving the request is not obligated to accept it
- Right to complain about privacy practices to the "covered entity" and to the Secretary of Health and Human Services

Limits on uses and disclosures

"Covered entities" that hold PHI may use it without an individual's consent for the purposes of providing treatment to the individual, for payment activities such as claims adjudication and premium setting, and for operating their businesses. They are also permitted to use and disclose PHI as required or permitted by other laws, e.g., laws related to reporting of child or elder abuse, public health oversight and national security investigations. However, those who have PHI must obtain an individual's signed authorization for use of PHI in marketing, research, fundraising, or any other activities that are not part of treatment, payment, health care operations, and other categories specifically identified under the Privacy Rule. A few types of disclosures require that the individual be given an opportunity to agree or object to the disclosure, e.g., whether information should be included in a hospital directory or given to clergy. Based on the professional judgment of a health care professional, some disclosures may be made to friends and family who are involved in an individual's care if such disclosures are found to be in the best interest of the individual.

In addition to specific restrictions on uses and disclosures, the Privacy Rule imposes a general "minimum necessary" requirement on those who hold and use PHI. Except for disclosures to the individual who is the subject of PHI or disclosures for treatment purposes, organizations must limit their uses and disclosures to



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

"minimum necessary" information required to perform a task. They must have policies and procedures that specify what PHI can be viewed by different classes of employees within their workforces, what PHI should be released in response to routine inquiries, and must have a process in place for deciding what PHI should be released in response to non-routine requests and a means by which to track these inquiries and released information.

"Covered entities" must also have formal contracts with their business associates, which use PHI to perform functions on their behalf. Examples of business associates include law firms, accounting firms, accreditation organizations, credentialing services, billing services and third-party administrators. Business associate agreements must stipulate that the business associate will safeguard PHI and will assist the "covered entity" in complying with its obligations with regard to individual rights and oversight by the Secretary of Health and Human Services.

Penalties for violations of privacy

The Privacy Rule includes both civil and criminal penalties for violations of privacy. Generally, penalties are expected to be assessed in cases where organizations or individuals act with willful neglect or intent to cause harm. Civil penalties are specified at \$100 per violation, not to exceed \$25,000 per person per year for identical violations. Criminal penalties for wrongful disclosure of PHI can go up to \$250,000 and/or 10 years imprisonment if the offense is committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm.

Security standards

Requirements for safeguarding protected health information (PHI) are found in two separate but complementary Rules under HIPAA. The Privacy Rule requires "covered entities" to have in place "appropriate administrative, physical and technical measures" to safeguard PHI. This obligation must be passed on to business associates in business associate agreements and to researchers in limited data use agreements. The Security Rule, published in final form on February 20, 2003, contains considerably more detail about the meaning of appropriate safeguards.

Although the Privacy Rule applies to PHI in any form, including oral communication, the Security Rule applies only to PHI in electronic form. The standards are divided into three groups: administrative safeguards, physical safeguards, and technical safeguards. Administrative standards include risk analysis and management, assigning security responsibilities, policies and procedures, training of the



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

workforce and contract requirements. Physical safeguards include access to facilities, records and workstations, as well as device and media controls. Technical safeguards include access controls and audits, authentication and transmission security.

The basic principles for security standards can be found in the HIPAA legislation. The law specifies, among other things, that standards must take into account technical capabilities of systems that contain PHI, cost of security measures and scalability issues, particularly as these might affect small and rural providers. The Department of Health and Human Services (HHS) translated these principles into regulation by creating standards (what must be done) and implementation specifications (how the standard can be met). Implementation specifications are further divided into two groups: those that are required (e.g., risk analysis) and those that are "addressable" (e.g., encryption for transmission of PHI). If an entity chooses not to implement an addressable specification, it must document its reasons why the specification would not be reasonable or appropriate, and implement alternative equivalent measures if reasonable and appropriate.

With the compliance date back in April 2005, its impossible at this time to know how doctors, health plans and other entities have interpreted and implemented the Security Rule. The Rule does require that "covered entities" think about and document the risks they identify and measures they take to ensure protection of PHI. These records are likely to be used for both enforcement and legal actions.

Substance Abuse Confidentiality Requirements

Information related to substance abuse and chemical dependency treatment is protected by section 543 of the Public Health Service Act, and its implementing regulation, [42 CFR, Part 2](#). This regulation, which supercedes both HIPAA and all more permissive state laws, requires that any disclosure of information related to substance abuse and chemical dependency treatment be accompanied by the individual's signed authorization. There are no exceptions for disclosures related to treatment, payment or health care operations. The only exception relates to movement of information between different components of the Armed Services, including Veterans Administration. Although the regulation applies only to "federally-assisted" specialized alcohol or drug abuse program, it is widely interpreted as applying to any federally conducted or funded program, any federally licensed or certified program, programs that are tax exempt, and programs that receive federal funds in any form, e.g., via the Medicaid program.



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

Other Federal Laws

In addition to being subject to HIPAA and Substance Abuse Confidentiality Requirements, health care organizations may be subject to several federal laws that touch in some way on privacy of health information. The Preamble to the Privacy Rule lists the following applicable laws: Privacy Act of 1974, Family Educational Rights and Privacy Act, Freedom of Information Act, Employee Retirement Income Security Act of 1974 (ERISA), Gramm-Leach-Bliley Act, federally funded health programs regulations, Food, Drug and Cosmetic Act, Clinical Laboratory Improvement Amendment, federal disability and non-discrimination laws, and U.S. Safe Harbor Privacy Principles (European Union Directive on Data Protection). In addition, many federal regulations require disclosure of specific PHI for specific purposes in specific circumstances.

In the Preamble to the Privacy Rule, HHS states that there should be few instances of conflict between HIPAA regulations and other federal laws because HIPAA permits but does not require many disclosures. Therefore, when disclosures are required under other federal law, PHI may be disclosed as required by other law. If a disclosure is not required but only permitted under other law, an entity must determine whether the disclosure is permissible under HIPAA and then follow HIPAA requirements for making such a disclosure. If another federal law prohibits disclosure that is permitted but not required under HIPAA, entities must comply with the other federal law.

Disclosure of Health Information for Law Enforcement and National Security

The HIPAA Privacy Rule permits but does not require disclosures of PHI required by other laws. Such disclosures must be limited to meet the compliance requirements of those other laws. Substance abuse regulations, which are more stringent than the Privacy Rule, prohibit some disclosures that would otherwise be permitted.

Disclosures to law enforcement officials

The Privacy Rule includes a standard for disclosures to law enforcement officials. The standard permits the following types of disclosures:

- Pursuant to a legal process or otherwise required by law, including disclosures of certain types of wounds, and disclosures in response to court orders, subpoenas, and administrative requests. Administrative requests must be specific and limited, relevant to a legitimate ongoing investigation,



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

- and must demonstrate that de-identified information (that is, information without individual identifiers) cannot be used.
- Limited information disclosures for the location of a fugitive, suspect, material witness or missing person.
- Information about an individual who is or is believed to be a victim of crime if the individual agrees to the disclosure or, under specific rules, if the individual is unable to agree or object.
- Information about decedents.
- Information about crime on the premises of the covered entity if there is a good faith belief that the disclosed PHI is evidence of a crime.
- Limited disclosure in emergencies in order to alert law enforcement about the commission of a crime.

Additional disclosures to law enforcement officials are permitted under other parts of the Privacy Rule. For example, disclosure is permitted if a covered entity believes that an individual may pose serious threat to health and safety and the disclosure may help law enforcement authorities reduce the harm or apprehend the individual.

Although disclosures to law enforcement authorities may be made without individual authorization and, in some cases, without giving the individual an opportunity to agree or object, such disclosures generally become part of Accounting for Disclosures that an individual can request from a covered entity. If a law enforcement official requests that law enforcement-related disclosures not be listed in the Accounting for a specified period of time, the entity providing the Accounting must suspend the individual's right to see a listing of such disclosures.

PHI of inmates and detainees in correctional institutions is generally subject to protections under the Privacy Rule, with some exceptions. The Rule permits covered entities to share inmates' PHI for specified health care and custodial purposes without authorization. Once individuals are released from custody, their PHI becomes subject to all protections under the Privacy Rule.

Some concerns have been raised that health oversight agencies may lawfully obtain PHI under the Privacy Rule and then re-disclose the information to law enforcement authorities. In its comments on the December 2000 Privacy Rule, HHS acknowledged that potentially such re-disclosures could take place, but stated that it does not have statutory authority to regulate health oversight agencies.



Networking Infrastructure Solutions
Business Process and Integration
Information Worker Solutions
ISV/Software Solutions

Regulations dealing with substance abuse are more stringent than the Privacy Rule when it comes to disclosures related to law enforcement. Information related to substance abuse may not be disclosed to law enforcement officials without individual authorization.

Disclosures for National Security

Covered entities are permitted to disclose PHI to authorized federal representatives for conduct of intelligence, counter-intelligence, and other national security activities, as well as to provide protective services to the President and others. These disclosures do not require individual authorization and do not become part of the Accounting for Disclosures. HHS states in the Preamble to the December 2000 Privacy Rule that the Rule does not confer any new authority with regard to disclosures related to national security or protective services because it does not compel covered entities to release information for these purposes. Of course, if new law is passed that requires disclosures of PHI for national security purposes, these disclosures would fall under provisions for disclosures required by law, and covered entities would have to comply with these requirements.