U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Fast Facts for Covered Entities

The Privacy Rule provides federal protections for personal health information held by covered entities, and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

The Privacy Rule does not require you to obtain a signed consent form before sharing information for treatment purposes. Health care providers can freely share information for treatment purposes without a signed patient authorization.

The Privacy Rule does not require you to eliminate all incidental disclosures. The Privacy Rule recognizes that it is not practicable to eliminate all risk of incidental disclosures. In August 2002, specific modifications to the Rule were adopted to clarify that incidental disclosures do not violate the Privacy Rule when you have policies which reasonably safeguard and appropriately limit how protected health information is used and disclosed.

The Privacy Rule does not cut off all communications between you and the families and friends of patients. As long as the patient does not object, The Privacy Rule permits you to:

- share needed information with family, friends, or anyone else a patient identifies as involved in his or her care;
- disclose information when needed to notify a family member or anyone responsible for the

Guidance Materials for Covered Entities

- Summary of the Privacy Rule
- Guidance on Significant Aspects of the Privacy Rule
- Fast Facts for Covered Entities
- Provider Guide: Communicating With a Patient's Family, Friends, or Other Persons Identified by the Patient
- Guidance on the Application of FERPA and HIPAA to Student Health Records
- Sample Business Associate Contract
- Misleading Marketing Claims
- Sign Up for the OCR Privacy Listserv

patient's care about the patient's location or general condition;
- share the appropriate information for these purposes even when the patient is incapacitated if doing so is in the best interest of the patient.

The Privacy Rule does not stop calls or visits to hospitals by family, friends, clergy or anyone else. Unless the patient objects, basic information such as phone number, room number and general condition can:

- be listed in the hospital directory;
- be given to people who call or visit and ask for the patient;
- be given to clergy along with religious affiliation--when provided by the patient--even if the patient is not asked for by name.

The Privacy Rule does not prevent child abuse reporting. You may continue to report child abuse or neglect to appropriate government authorities.

The Privacy Rule is not anti-electronic. You can communicate with patients, providers, and others by e-mail, telephone, or facsimile, with the implementation of appropriate safeguards to protect patient privacy.

Please view our Frequently Asked Questions about the Privacy Rule.

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?

Answer:

The Privacy Rule is balanced to protect an individual's privacy while allowing important law enforcement functions to continue. The Rule permits covered entities to disclose protected health information (PHI) to law enforcement officials, without the individual's written authorization, under specific circumstances summarized below. For a complete understanding of the conditions and requirements for these disclosures, please review the exact regulatory text at the citations provided. Disclosures for law enforcement purposes are permitted as follows:

- **To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.** The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information (45 CFR 164.512(f)(1)(ii)(A)-(B)).

- **To respond to an administrative request**, such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used (45 CFR 164.512(f)(1)(ii)(C)).

- **To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures** of PHI to name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request (45 CFR 164.512(f)(2)).

  This same limited information may be reported to law enforcement:

  - **About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity's workforce** (45 CFR 164.502(j)(2));

  - **To identify or apprehend an individual who has admitted participation in a violent crime** that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual's request for therapy, counseling, or treatment related to the propensity to commit this type of violent act (45 CFR 164.512(j)(1)(ii)(A), (j)(2)-(3)).

- **To respond to a request for PHI about a victim of a crime, and the victim agrees.** If, because of an emergency or the person's incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law,

the investigation would be materially and adversely affected by waiting until the victim could agree, and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested (45 CFR 164.512(f)(3)).

Where child abuse victims or adult victims of abuse, neglect or domestic violence are concerned, other provisions of the Rule apply:

- **Child abuse or neglect may be reported** to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required (45 CFR 164.512(b)(1)(ii)).
- **Adult abuse, neglect, or domestic violence may be reported** to a law enforcement official authorized by law to receive such reports (45 CFR 164.512(c)):
  - If the individual agrees;
  - If the report is required by law; or
  - If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations (see 45 CFR 164.512(c)(1)(iii)(B)).
  - Notice to the individual of the report may be required (see 45 CFR 164.512(c)(2)).

- **To report PHI to law enforcement when required by law** to do so (45 CFR 164.512(f)(1)(i)). For example, state laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.

- **To alert law enforcement to the death of the individual**, when there is a suspicion that death resulted from criminal conduct (45 CFR 164.512(f)(4)).
  - Information about a decedent may also be shared with **medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties** *(45 CFR 164.512(g)(1)).*

- **To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity's premises** (45 CFR 164.512(f)(5)).

- **When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity,** specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime (45 CFR 164.512(f)(6)). This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence; see above Adult abuse, neglect, or domestic violence for when reports to law enforcement are allowed under 45 CFR 164.512(c).

- When consistent with applicable law and ethical standards:
  - To a law enforcement official reasonably able to **prevent or lessen a serious and imminent threat to the health or safety of an individual or the public** (45 CFR 164.512(j)(1)(i)); or

- **To identify or apprehend an individual who appears to have escaped from lawful custody** (45 CFR 164.512(j)(1)(ii)(B)).

- **For certain other specialized governmental law enforcement purposes**, such as:

  - **To federal officials authorized to conduct** intelligence, counter-intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3));

  - **To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody** of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the health and safety of the individual, other inmates, officers or employees of or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility (45 CFR 164.512(k)(5)).

Except when required by law, the disclosures to law enforcement summarized above are subject to a minimum necessary determination by the covered entity (45 CFR 164.502(b), 164.514(d)). When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose (45 CFR 164.514(d)(3)(iii)(A)). Moreover, if the law enforcement official making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information (45 CFR 164.514(h)).

Date Created: 07/23/2004

Last Updated: 08/08/2005

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Personal Representatives

45 CFR 164.502(g) (Download a copy in PDF)

Guidance: Significant Aspects of the Privacy Rule

Background

The HIPAA Privacy Rule establishes a foundation of Federally-protected rights which permit individuals to control certain uses and disclosures of their protected health information. Along with these rights, the Privacy Rule provides individuals with the ability to access and amend this information, and the right to an accounting of certain disclosures. The Department recognizes that there may be times when individuals are legally or otherwise incapable of exercising their rights, or simply choose to designate another to act on their behalf with respect to these rights. Under the Rule, a person authorized (under State or other applicable law, e.g., tribal or military law) to act on behalf of the individual in making health care related decisions is the individual's "personal representative." Section 164.502(g) provides when, and to what extent, the personal representative must be treated as the individual for purposes of the Rule. In addition to these formal designations of a personal representative, the Rule at 45 CFR 164.510(b) addresses situations in which persons are involved in the individual's health care but are not expressly authorized to act on the individual's behalf.

How the Rule Works General Provisions

Except as otherwise provided in 45 CFR 164.502(g), the Privacy Rule requires covered entities to treat an individual's personal representative as the individual with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule. The personal representative stands in the shoes of the individual and has the ability to act for the individual and exercise the individual's rights. For instance, covered entities must provide the individual's personal representative with an accounting of disclosures in accordance with 45 CFR 164.528, as well as provide the personal representative access to the individual's protected health information in accordance with 45 CFR 164.524 to the extent such information is relevant to such representation. In addition to exercising the individual's rights under the Rule, a personal representative may also authorize disclosures of the individual's protected health information. In general, the scope of the personal representative's authority to act for the individual under the Privacy Rule derives from his or her authority under applicable law to make health care decisions for the individual. Where the person has broad authority to act on the behalf of a living individual in making decisions related to health care, such

as a parent with respect to a minor child or a legal guardian of a mentally incompetent adult, the covered entity must treat the personal representative as the individual for all purposes under the Rule, unless an exception applies. (See below with respect to abuse, neglect or endangerment situations, and the application of State law in the context of parents and minors). Where the authority to act for the individual is limited or specific to particular health care decisions, the personal representative is to be treated as the individual only with respect to protected health information that is relevant to the representation. For example, a person with an individual's limited health care power of attorney regarding only a specific treatment, such as use of artificial life support, is that individual's personal representative only with respect to protected health information that relates to that health care decision. The covered entity should not treat that person as the individual for other purposes, such as to sign an authorization for the disclosure of protected health information for marketing purposes. Finally, where the person has authority to act on the behalf of a deceased individual or his estate, which does not have to include the authority to make decisions related to health care, the covered entity must treat the personal representative as the individual for all purposes under the Rule. State or other law should be consulted to determine the authority of the personal representative to receive or access the individual's protected health information.

Who Must Be Recognized as the Individual's Personal Representative

The following displays who must be recognized as the personal representative for a category of individuals:

If the Individual Is: An Adult or An Emancipated Minor

The Personal Representative Is: A person with legal authority to make health care decisions on behalf of the individual

Examples: Health care power of attorney Court appointed legal guardian General power of attorney

If the Individual Is: An Unemancipated Minor

The Personal Representative Is: A parent, guardian, or other person acting in loco parentis with legal authority to make health care decisions on behalf of the minor child

Exceptions: See parents and minors discussion below.

If the Individual Is: Deceased

The Personal Representative Is: A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions)

Examples: Executor of the estate Next of kin or other family member Durable power of attorney

Parents and Unemancipated Minors

The Privacy Rule defers to State or other applicable laws that address the ability of a parent, guardian, or other person acting in loco parentis (collectively, "parent") to obtain health information about a minor child. In most cases under the Rule, the parent is the personal representative of the minor child and can exercise the minor's rights with respect to protected health information, because the parent usually has the authority to make health care decisions about his or her minor child. Regardless of whether a parent is the personal representative, the Privacy Rule permits a covered entity to disclose to a parent, or provide the parent with access to, a minor child's protected health information when and to the extent it is expressly permitted or required by State or other laws (including relevant case law). Likewise, the Privacy Rule prohibits a covered entity from disclosing a minor child's protected health information to a parent, or providing a parent with access to, such information when and to the extent it is expressly prohibited under State or other laws (including relevant case law). Thus, State and other applicable law governs when such law explicitly requires, permits, or prohibits the disclosure of, or access to, the health information about a minor child. The Privacy Rule specifies three circumstances in which the parent is not the "personal representative" with respect to certain health information about his or her minor child. These exceptions generally track the ability of certain minors to obtain specified health care without parental consent under State or other laws, or standards of professional practice. In these situations, the parent does not control the minor's health care decisions, and thus under the Rule, does not control the protected health information related to that care. The three exceptional circumstances when a parent is not the minor's personal representative are:

- When State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service; Example: A State law provides an adolescent the right to obtain mental health treatment without the consent of his or her parent, and the adolescent consents to such treatment without the parent's consent.
- When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor; Example: A court may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court
- When a parent agrees to a confidential relationship between

the minor and the physician. Example: A physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees.

Even in these exceptional circumstances, where the parent is not the "personal representative" of the minor, the Privacy Rule defers to State or other laws that require, permit, or prohibit the covered entity to disclose to a parent, or provide the parent access to, a minor child's protected health information. Further, in these situations, if State or other law is silent or unclear concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent with access to the minor's health information, if doing so is consistent with State or other applicable law, and provided the decision is made by a licensed health care professional in the exercise of professional judgment.

Abuse, Neglect, and Endangerment Situations

When a physician or other covered entity reasonably believes that an individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse or neglect by the personal representative, or that treating a person as an individual's personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual's personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual. For example, if a physician reasonably believes that disclosing information about an incompetent elderly individual to the individual's personal representative would endanger that individual, the Privacy Rule permits the physician to decline to make such disclosure.

Please review the Frequently Asked Questions about the Privacy Rule.

OCR HIPAA Privacy December 3, 2002 Revised April 3, 2003

Back to Top

A HEALTH CARE PROVIDER'S GUIDE TO THE HIPAA PRIVACY RULE:

Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care

U.S. Department of Health and Human Services • Office for Civil Rights

This guide explains when a health care provider is allowed to share a patient's health information with the patient's family members, friends, or others identified by the patient as involved in the patient's care under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. HIPAA is a Federal law that sets national standards for how health plans, health care clearinghouses, and most health care providers are to protect the privacy of a patient's health information.[1]

Even though HIPAA requires health care providers to protect patient privacy, providers are permitted, in most circumstances, to communicate with the patient's family, friends, or others involved in their care or payment for care. This guide is intended to clarify these HIPAA requirements so that health care providers do not unnecessarily withhold a patient's health information from these persons. This guide includes common questions and a table that summarizes the relevant requirements.[2]

COMMON QUESTIONS ABOUT HIPAA

1. If the patient is present and has the capacity to make health care decisions, when does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?

If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object. In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care.

Here are some examples:

- An emergency room doctor may discuss a patient's treatment in front of the patient's friend if the patient asks that her friend come into the treatment room.
- A doctor's office may discuss a patient's bill with the patient's adult daughter who is with the patient at the patient's medical appointment and has questions about the charges.
- A doctor may discuss the drugs a patient needs to take with the patient's health aide who has accompanied the patient to a medical appointment.
- A doctor may give information about a patient's mobility limitations to the patient's sister who is driving the patient home from the hospital.

[1] The HIPAA Privacy Rule applies to those health care providers that transmit any health information in electronic form in connection with certain standard transactions, such as health care claims. See the definitions of "covered entity," "health care provider," and "transaction" at 45 C.F.R. § 160.103.

[2] The full text of these requirements can be found at 45 C.F.R. § 164.510(b). Note that this guide does not apply to a health care provider's disclosure of psychotherapy notes, which generally requires a patient's written authorization. See 45 C.F.R. § 164.508(a)(2).

- A nurse may discuss a patient's health status with the patient's brother if she informs the patient she is going to do so and the patient does not object.

BUT:

- A nurse may not discuss a patient's condition with the patient's brother after the patient has stated she does not want her family to know about her condition.

2. If the patient is not present or is incapacitated, may a health care provider still share the patient's health information with family, friends, or others involved in the patient's care or payment for care?

Yes. If the patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others as long as the health care provider determines, based on professional judgment, that it is in the best interest of the patient. When someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care. The health care provider may discuss only the information that the person involved needs to know about the patient's care or payment.

Here are some examples:

- A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.
- A pharmacist may give a prescription to a patient's friend who the patient has sent to pick up the prescription.
- A hospital may discuss a patient's bill with her adult son who calls the hospital with questions about charges to his mother's account.
- A health care provider may give information regarding a patient's drug dosage to the patient's health aide who calls the provider with questions about the particular prescription.

BUT:

- A nurse may not tell a patient's friend about a past medical problem that is unrelated to the patient's current condition.
- A health care provider is not required by HIPAA to share a patient's information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.

3. Does HIPAA require that a health care provider document a patient's decision to allow the provider to share his or her health information with a family member, friend, or other person involved in the patient's care or payment for care?

No. HIPAA does not require that a health care provider document the patient's agreement or lack of objection. However, a health care provider is free to obtain or document the patient's agreement, or lack of objection, in writing, if he or she prefers. For example, a provider may choose to document a patient's agreement to share information with a family member with a note in the patient's medical file.

4. May a health care provider discuss a patient's health information over the phone with the patient's family, friends, or others involved in the patient's care or payment for care?

Yes. Where a health care provider is allowed to share a patient's health information with a person, information may be shared face-to-face, over the phone, or in writing.

5. If a patient's family member, friend, or other person involved in the patient's care or payment for care calls a health care provider to ask about the patient's condition, does HIPAA require the health care provider to obtain proof of who the person is before speaking with them?

No. If the caller states that he or she is a family member or friend of the patient, or is involved in the patient's care or payment for care, then HIPAA doesn't require proof of identity in this case. However, a health care provider may establish his or her own rules for verifying who is on the phone. In addition, when someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care.

6. Can a patient have a family member, friend, or other person pick up a filled prescription, medical supplies, X-rays, or other similar forms of patient information, for the patient?

Yes. HIPAA allows health care providers to use professional judgment and experience to decide if it is in the patient's best interest to allow another person to pick up a prescription, medical supplies, X-rays, or other similar forms of information for the patient.

For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for a patient effectively verifies that he or she is involved in the patient's care. HIPAA allows the pharmacist to give the filled prescription to the relative or friend. The patient does not need to provide the pharmacist with their names in advance.

7. May a health care provider share a patient's health information with an interpreter to communicate with the patient or with the patient's family, friends, or others involved in the patient's care or payment for care?

Yes. HIPAA allows covered health care providers to share a patient's health information with an interpreter without the patient's written authorization under the following circumstances:

- A health care provider may share information with an interpreter who works for the provider (e.g., a bilingual employee, a contract interpreter on staff, or a volunteer).

  For example, an emergency room doctor may share information about an incapacitated patient's condition with an interpreter on staff who relays the information to the patient's family.

- A health care provider may share information with an interpreter who is acting on its behalf (but is not a member of the provider's workforce) if the health care provider has a written contract or other agreement with the interpreter that meets HIPAA's business associate contract requirements.

  For example, many providers are required under Title VI of the Civil Rights Act of 1964 to take reasonable steps to provide meaningful access to persons with limited English proficiency. These providers often have contracts with private companies, community-based organizations, or telephone interpreter service lines to provide language interpreter services. These arrangements must comply with the HIPAA business associate agreement requirements at 45 C.F.R. 164.504(e).

- A health care provider may share information with an interpreter who is the patient's family member, friend, or other person identified by the patient as his or her interpreter, if the patient agrees, or does not object, or the health care provider determines, using his or her professional judgment, that the patient does not object.

For example, health care providers sometimes see patients who speak a certain language and the provider has no employee, volunteer, or contractor who can competently interpret that language. If the provider is aware of a telephone interpreter service that can help, the provider may have that interpreter tell the patient that the service is available. If the provider decides, based on professional judgment, that the patient has chosen to continue using the interpreter, the provider may talk to the patient using the interpreter.

8. Where can I find additional information about HIPAA?

The Office for Civil Rights, part of the Department of Health and Human Services, has more information about HIPAA on its Web site. Visit http://www.hhs.gov/ocr/hipaa for a wide range of helpful information, including the full text of the Privacy Rule, a HIPAA Privacy Rule Summary, fact sheets, over 200 Frequently Asked Questions, as well as many other resources to help health care providers and others understand the law.

HIPAA Privacy Rule Disclosures to a Patient's Family, Friends, or Others Involved in the Patient's Care or Payment for Care

	Family Member or Friend	Other Persons
Patient is present and has the capacity to make health care decisions	Provider may disclose relevant information if the provider does one of the following: (1) obtains the patient's agreement (2) gives the patient an opportunity to object and the patient does not object (3) decides from the circumstances, based on professional judgment, that the patient does not object Disclosure may be made in person, over the phone, or in writing.	Provider may disclose relevant information if the provider does one of the following: (1) obtains the patient's agreement (2) gives the patient the opportunity to object and the patient does not object (3) decides from the circumstances, based on professional judgment, that the patient does not object Disclosure may be made in person, over the phone, or in writing.
Patient is not present or is incapacitated	Provider may disclose relevant information if, based on professional judgment, the disclosure is in the patient's best interest. Disclosure may be made in person, over the phone, or in writing. Provider may use professional judgment and experience to decide if it is in the patient's best interest to allow someone to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of health information for the patient.	Provider may disclose relevant information if the provider is reasonably sure that the patient has involved the person in the patient's care and in his or her professional judgment, the provider believes the disclosure to be in the patient's best interest. Disclosure may be made in person, over the phone, or in writing. Provider may use professional judgment and experience to decide if it is in the patient's best interest to allow someone to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of health information for the patient.

HIPAA Security Series

What is the Security Series?

The security series of papers provides guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled "Security Standards for the Protection of Electronic Protected Health Information," found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement a provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series contains seven papers, each focused on a specific topic related to the Security Rule (see left panel). The papers are designed to give HIPAA covered entities insight into the Security Rule and to assist them with implementation of the standards. This series explains specific requirements (provisions of the rule), and possible ways to address those provisions.

CMS recommends that all covered entities read the first paper in this series, "Security 101 for Covered Entities" before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation and maintain an ongoing security program. This seventh paper in the series is devoted to implementation of the Security Rule standards, implementation specifications and requirements as they relate to covered entities that are sole practitioners or otherwise considered small providers. It assumes the reader has a basic understanding of the Security Rule.

Background

Identity theft, stolen computer disks, malfunctioning computers, hackers, and other preventable losses of information - these are just a few of the hazards facing all businesses that receive, store, and transmit data in electronic form. Many health care providers too face these same hazards. Much of the electronic protected health information (EPHI) they hold is critical to their business and vital to the care of their patients. Providers face major problems if their patient's sensitive information is stolen, misused, or unavailable.

The HIPAA Security Standards provide a structure for covered entities (health plans, clearinghouses, or covered health care providers) to develop and implement policies and procedures to guard against and react to security incidents. The Security Rule provides a flexible, scalable and technology neutral framework to allow all covered entities to comply in a manor that is consistent with the unique circumstances of their size and environment.

All covered entities must comply with the applicable standards, implementation specifications, and requirements of the Security Rule with respect to EPHI (see 45 C.F.R § 164.302.). Small providers that are covered entities have unique business and technical environments that provide both opportunities and challenges related to compliance with the Security Rule. As such, this

paper provides general guidance to providers such as physicians and dentists in solo or small group practices, small clinics, independent pharmacies, and others who may be less likely to have IT staff and whose approach to compliance would generally be very different from that of a large health care system. It is important to note however, that this paper does not define a small provider, nor does it prescribe specific actions that small providers must take to become compliant with the Security Rule.

The objectives of this paper are to:

- Help small providers understand the Security Rule standards, implementation specifications, and requirements as they relate to their organization.
- Provide sample questions and scenarios that small providers may want to consider when addressing the Security Rule requirements.
- Reference industry resources that provide additional information regarding compliance with the Security Rule.

Security Rule Overview for Small Providers

To understand the requirements of the Security Rule, it is helpful to be familiar with the basic concepts that comprise the security standards and implementation specifications. The Security Rule is divided into six main sections – each representing a set of standards and implementation specifications that must be addressed by all covered entities. Each Security Rule *standard* is a requirement: a covered entity must comply with all of the standards of the Security Rule with respect to the EPHI it creates, transmits or maintains.

Many of the standards contain *implementation specifications*. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard. Implementation specifications are either *required or addressable*. Regardless of whether a standard includes one or more implementation specifications, covered entities must comply with each standard. Where there is no implementation specification for a particular standard, such as the "Workstation Use" and "Person or Entity Authentication" standards, compliance with the standard itself is required.

- A **required** implementation specification is similar to a standard, in that a covered entity must comply with it. For example, all covered entities including small providers must conduct a "Risk Analysis" in accordance with Section 164.308(a)(1) of the Security Rule.
- For **addressable** implementation specifications, covered entities must perform an assessment to determine whether the specification is a reasonable and appropriate safeguard in the covered entity's environment. After performing the assessment, a covered entity decides if it will implement the addressable implementation specification; implement an equivalent alternative measure that allows the entity to comply with the standard; or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment. Covered entities are required to document these assessments and all decisions. For example, all covered entities including

small providers must determine whether "Encryption and Decryption" is reasonable and appropriate for their environment in accordance with Section 164.312(a)(1) of the Security Rule.

- Factors that determine what is "reasonable" and "appropriate" include cost, size, technical infrastructure and resources. While cost is one factor entities must consider in determining whether to implement a particular security measure, some appropriate measure must be implemented. An addressable implementation specification is not optional, and the potential cost of implementing a particular security measure does not free covered entities from meeting the requirements identified in the rule.

Using This Resource

The tables and sample questions provided here relate to the Administrative, Technical and Physical Safeguard requirements from the Security Rule and are relevant for small providers seeking to evaluate and/or establish EPHI security practices. The tables and sample questions in this document do not represent a complete list of Security Rule requirements, but provide insight into the key HIPAA Security requirements applicable to a small provider.

HIPAA Security Series

Administrative Safeguards – These provisions are defined in the Security Rule as the "administrative actions, 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."

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
SECURITY MANAGEMENT PROCESS § 164.308(a)(1) *"Implement policies and procedures to prevent, detect, contain and correct security violations."*	RISK ANALYSIS (R) *§ 164.308(a)(1)(ii)(A)* *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."*	Have you identified the EPHI within your organization? This includes EPHI that you create, receive, maintain or transmit. Please note that EPHI may be resident on computer workstations, servers or on portable devices such as laptops, and PDAs.
	RISK MANAGEMENT (R) *§164.308(a)(1)(ii)(B)* *"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)."*	What security measures are already in place to protect EPHI – this can be a comprehensive view of all measures, whether administrative, physical or technical, such as an over arching security policy; door locks to rooms where EPHI is stored; or the use of password-protected files.

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
	SANCTION POLICY (R) *§ 164.308(a)(1)(ii)(C)* *"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."*	Have you developed, applied and implemented policies specific to violations of the security policies and procedures? If so, do they provide appropriate sanctions for workforce members who fail to comply with your security policies and procedures? (i.e., have you included your sanction policy in your workforce manual and trained your staff on the policy?)
WORKFORCE SECURITY § 164.308(a)(3)(i) *"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information."*	AUTHORIZATION AND/OR SUPERVISION (A) *§ 164.308(a)(3)(ii)(A)* *"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."*	Are the procedures used by your workforce consistent with your access policies (i.e., do people who should have access actually have that access? Are people who should not have access prevented from accessing the information?)

HIPAA Security Series

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
SECURITY AWARENESS AND TRAINING § 164.308(a) (5) (i) *"Implement a security awareness and training program for all members of its workforce (including management)."*	PASSWORD MANAGEMENT (A) *§ 164.308(a)(5)(ii)(D)* *"Implement procedures for creating, changing, and safeguarding passwords."*	Does your workforce training address topics such as not sharing passwords with other workforce members or not writing down passwords and leaving them in open areas?
CONTINGENCY PLAN § 164.308(a) (7) (i) *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."*	DATA BACKUP PLAN (R) *§ 164.308(a)(7)(ii)(A)* *"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."*	Do your procedures identify all sources of EPHI that must be backed up such as patient accounting systems, electronic medical or health records, digital recordings of diagnostic images, electronic test results, or any other electronic documents created or used that contain EPHI?

SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS § 164.308(b)(1) *"A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information."*	WRITTEN CONTRACT OR OTHER ARRANGEMENTS (R) *§ 164.308(b)(4)* "Document the satisfactory assurances required by this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a) [(the Business Associate Contracts or Other Arrangements Standard)]."	Do you have contracts in place with outside entities entrusted with health information generated by your office? If so, do the contracts provide assurances that the information will be properly safeguarded? For example, if you contract with a software vendor for your practice management system, what assurances do you have that the vendor's products are HIPAA compliant?

Physical Safeguards – These provisions are defined as the "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."

SAMPLE PHYSICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
FACILITY ACCESS CONTROLS § 164.310(a)(1) *"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."*	FACILITY SECURITY PLAN (A) *§ 164.310(a)(2)(ii)* *"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."*	Do your office policies and procedures identify controls to prevent unauthorized physical access, tampering, and theft of EPHI? These could include locked doors, signs warning of restricted areas, surveillance cameras, alarms, and identification numbers and security cables on computers.
	MAINTENANCE RECORDS (A) *§ 164.310(a)(2)(iv)* *"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks)."*	Has your office implemented policies and procedures that specify how repairs and modifications to a building or facility will be documented to demonstrate that the EPHI is protected?

SAMPLE PHYSICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
WORKSTATION USE § 164.310(b) *"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."*	*This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required (R).*	Do your office policies and procedures specify the use of additional security measures to protect workstations with EPHI, such as using privacy screens, enabling password protected screen savers or logging off the workstation?
DEVICE AND MEDIA CONTROLS § 164.310(d)(1) *"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility."*	DISPOSAL (R) *§ 164.310(d)(2)(i)* *"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."*	Does your office have a method of destroying EPHI on equipment and media you are no longer using? For example, have you considered purchasing hard drive erasure software for a planned upgrade of office computers?
	DATA BACKUP AND STORAGE (A) *§ 164.310(d)(2)(iv)* *"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."*	Do you have a process in place to create a retrievable, exact copy of EPHI before the equipment on which it is stored is moved?

Technical Safeguards – These provisions are defined as the "technology and the policy and procedures that protect electronic protected health information and control access to it (the EPHI)."

SAMPLE TECHNICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
ACCESS CONTROL § 164.312(a)(1) *"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)) [(Information Access Management)]."*	UNIQUE USER IDENTIFICATION (R) *§ 164.312(A)(2)(I) "Assign a unique name and/or number for identifying and tracking user identity."*	Do you have a process in place to assign each user of your system a unique user identifier? If so, can the identifier be used to track user activity within information systems that contain EPHI? This may or may not be reasonable or appropriate for a solo clinician where access has been granted to all office staff.

SAMPLE TECHNICAL SAFEGUARDS FOR SMALL PROVIDERS		
Standard	**Sample Implementation Specifications (R)= Required, (A)= Addressable**	**Sample Question**
	AUTOMATIC LOGOFF (A) *§ 164.312(a)(2)(iii)* *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."*	Do your current information systems have an automatic logoff capability to ensure that unauthorized users do not access data on unattended workstations?
PERSON OR ENTITY AUTHENTICATION § 164.312(d) *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*	*This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required (R).*	Does your system require the input of something known only to the person or entity seeking access to EPHI, (such as a password or PIN) prior to granting the requested access?
TRANSMISSION SECURITY § 164.312(e)(1) *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."*	ENCRYPTION (A) § 164.312(e)(2)(ii) *"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."*	Based on your required risk analysis, is encryption needed to protect the transmission of EPHI between your office and outside organizations? If not, what measures do you have in place to ensure the protection of this information? Some small providers might consider password protection of documents or files containing EPHI and/or prohibiting the transmission of EPHI via email.

Additional Requirements

Please note also that the Security Rule contains organizational and documentation requirements that must be addressed by all covered entities. Organizational requirements include standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans. Policies, procedures, and documentation requirements address how each of the requirements are documented, reviewed, updated and communicated to the workforce.

In Summary

Information security is a necessity in today's world. Preventing unauthorized use of sensitive health information is a core goal of every participant in the health care industry. The Security Rule allows covered entities, including small providers, to implement reasonable and appropriate measures that enable them to comply with the Rule.

The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts.

Resources

Covered entities should periodically check the CMS website at: http://www.cms.hhs.gov/SecurityStandard/ for additional HIPAA security information and resources as they work through the security implementation process. While CMS does not endorse guidance provided by other organizations, covered entities may also want to check with other local and national professional health care organizations, such as national provider and health plan associations for additional information. Consider obtaining and reviewing the resources available through the Workgroup for Electronic Data Interchange (WEDI), at www.wedi.org. WEDI has numerous white papers and educational resources aimed at all types of covered entities, and many directed specifically to the smaller physician office. The National Institute of Standards and Technology (NIST) at www.nist.gov also has a wide range of documents and resources to assist to entities in understanding how to comply with the spirit of the regulation.