practical security

PO Box 8021

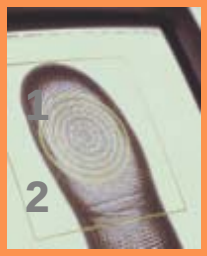
Rancho Santa Fe

California 92067

858.259.6204 tel

858.259.0309 fax

www.practicalsecurity.com



HIPAA Service Description

February 2003

3 PSI HIPAA Services Offering

The Department of Health and Human Services estimates that there are 200,000 small health care providers in the United States that are considered “Covered Entities” under HIPAA legislation. These organizations must address HIPAA privacy requirements by April 14, 2003 and HIPAA information security requirements by 2005 or risk suspension of payment, expulsion from Medicare, and significant penalties.

Practical Security, Inc. has established a fixed price offering to assist small providers in addressing HIPAA requirements for privacy and security. The intent of this offering is to provide a reasonably priced HIPAA compliance support service to smaller covered entities.

3.1 Background on HIPAA

The Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986, is also known as the Kennedy-Kassebaum Act.

Title II includes a section, Administrative Simplification, requiring:

1. Improved efficiency in healthcare delivery by standardizing electronic data interchange, and
2. Protection of confidentiality and security of health data through setting and enforcing standards.

More specifically, HIPAA calls for:

1. Standardization of electronic patient health, administrative and financial data
2. Unique health identifiers for individuals, employers, health plans and health care providers
3. Security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

The bottom line: sweeping changes in most health care transaction and administrative information systems.

3.2 Elements of the Final Security Rule

3.2.1 Administrative Safeguards §.308

These are documented practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

- Security Management Process §.308(a)(1)
  - Risk Analysis (Required)
  - Risk Management (Required)
  - Sanction Policy (Required)
  - Information System Activity Review (Required)
- Assigned Security Responsibility §.308(a)(2) (Required)

- Work Force Security §.308 (a)(3)
  - Authorization and/or Supervision (Addressable)
  - Workforce Clearance Procedure (Addressable)
  - Termination Procedures (Addressable)
- Information Access Management §.308(a)(4)
  - Isolating Health Care and Clearinghouse Function (Required)
  - Access Authorization (Addressable)
  - Access Establishment and Authorization (Addressable)
- Security Awareness and Training §.308(a)(5)
  - Security Reminders (Addressable)
  - Protection from Malicious Software (Addressable)
  - Log-in Monitoring (Addressable)
  - Password Management (Addressable)
- Security Incident Procedures §.308(a)(6)
  - Response and Reporting (Required)
- Contingency Plan §.308(a)(7)
  - Data Backup Plan (Required)
  - Disaster Recovery Plan (Required)
  - Emergency Mode Operations Plan (Required)
  - Testing and Revision Procedure (Addressable)
  - Applications and Data Criticality Analysis (Addressable)
- Evaluation §.308(a)(8) (Required)
- Business Associates Contracts and Other Arrangements §.308(b)(1)
  - Written Contract or Other Arrangement (Required)

3.2.2 Physical Safeguards §.310

These relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. It covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

- Facility Access Controls§.310(a)(1)
  - Contingency Operations (Addressable)
  - Access Control and Validation Procedures (Addressable)
  - Workstation Use §.310(b) (Required)
- Workstation Security §.310(c) (Required)
- Device and Media Controls §.310(d)(1)
  - Media Re-use (Required)
  - Data Backup and Storage (Addressable)

3.2.3 Technical Safeguards §.312

These are the processes that are put into place to protect information and to control individual access to information.

- Access control §.312(a)(1)
  - Emergency Access Procedures (Required)
  - Encryption and Decryption (Addressable)
- Audit Controls §.312(b) (Required)
- Integrity §.312(c)(1)
  - Person or Entity Authentication §.312(d) (Required)
- Transmission Security §.312 (e)(1)
  - Encryption (Addressable)

4 HIPAA Self-Certification

Final security rules for HIPAA were approved on February 13, 2003. The final privacy rule was released in August, 2002. At this time, there are no specific organizations that are "authorized" to perform certifications and this is not expected to change because HHS feels that this is best left to the market. However, there are some basic recommendations that can be followed to create a self-certification to meet the requirements of the HIPAA security rule:

- be performed by individuals who are not responsible for the maintenance, supervision, or execution of the specified IT controls;
- be an on-going process;
- include due diligence as a requirement;
- include documentation as a key part of the process;
- be performed by individuals with adequate training regarding generally accepted security guidelines and principles;
- be performed by internal or external parties;
- include an examination of evidential matter sufficient to obtain an understanding of the design and effectiveness of controls for each HIPAA security requirement and implementation;
- recommend monitoring the certification cycle at a minimum of once a year due to the changing nature of computer systems and accelerating rate of change of IT related security risks;
- be maintained for three years to provide for an adequate history of certification information and an audit trail of certification for reviewing bodies; and
- be reviewed and authorized by executive management.

Following these recommendations, PSI acts as an external party with adequate training regarding generally accepted security guidelines and principles. Although the recommendations suggest that an internal party may perform self-certification work, this internal party would also need to have adequate training and be individuals who are not responsible for the maintenance, supervision, or execution of the specified IT controls. Typically, when small organizations have someone with the proper training these are the same individuals responsible for the management of the systems being certified. Objectivity is crucial to the validity of the self-certification.

This self-certification is documented in a letter in management representation form signed by the organization's executive management and compliance officer that states 1) the compliance status by each HIPAA requirement and element, 2) management's action plans to address areas of control deficiency, and 3) any instances in which management is aware of security related control issues or deficiencies. This letter clearly states management's responsibility for the effectiveness of the information security control structure.

4.1 Motivations for Small Providers to Use this Offering

To avoid risking payment suspension, significant fines, and Medicare exclusion, small providers need this offering to prepare for HIPAA compliance. Although there are no HIPAA "police" and the requirements are defined in such a way that it is difficult to determine exactly what comprises compliance, there are some time-tested practices in enforcement that are likely. Some of the best guidance in this area comes from the practice of due care and due diligence.

Healthcare providers today need to protect themselves from downstream liabilities by exercising due care and due diligence. Downstream liabilities mean that your organization can be held liable in a civil case if another

organization is damaged by a lack of security controls. Due care means that you did all you could to reasonably protect your organization from known threats. Due diligence means that you kept up with these practices in a diligent manner, rather doing them once and then forgetting about them.

Senior management is responsible for protecting the organization from a long-list of actions that can have a negative impact including protecting personal privacy, leaving yourself open to hacker attack, malicious code, and violation of the law. Management must follow the prudent person rule which requires them to perform duties that prudent people would follow in similar circumstances using due care and due diligence.

In practice (in a court of law), due care and due diligence are subjective and usually defined by what other companies are doing and what a prudent management team would do. In other words, if most other companies are doing third party audits to check their own security measures and you have not performed one then you could be held liable for not having done prudent and reasonable actions to prevent misuse. On the other hand, if you have done reasonable and prudent things, such as a third-party audit, then, even if your machines were misused resulting in a compromise of PHI, you have some protection against liability. At the very least these actions would count in your favor.

5 Specific Services Provided in this Offering

5.1.1 Security Support

- Support for self-certification including a boilerplate letter that may be used for documenting self-certification.
- A boilerplate business associate contract and tailored to your specific organization. PSI does not provide legal advice or construct individual agreements for every business associate.
- A contingency plan tailored to your organization.
- Guidance for constructing a formal mechanism and review of final creation.
- Review and development of access control policies and procedures tailored to your specific organizational needs.
- Review and development of internal audit policies and procedures.
- Review and development of personnel security policies and procedures.
- Review and development of security configuration policies and procedures.
- Review and development of security incident procedures.
- A documented security management process.
- Review and development of termination procedures.
- Creation of a tailored security awareness program. PSI can provide this training for an additional charge.
- Assist in the selection and training of the individual with security responsibility.
- Review and development of media controls policies and procedures.
- Review and development of physical access policies and procedures tailored to your specific organizational needs.
- Review and development of workstation guideline policies.
- Provide guidance in establishing a secure workstation area.
- Review and development of applicable access control policies and procedures tailored to your specific organizational needs.
- Review and development of audit policies and procedures.
- Review and development of authorization policies and procedures tailored to your specific organizational needs.
- Review and development of data authentication procedures.
- Review and development of authentication policies and procedures tailored to your specific organizational needs.

5.1.2 Privacy Support

- A boilerplate notice agreement and guidance on customization.
- A boilerplate authorization agreement and guidance on customization.
- Review and development of notification and authorization procedures.

- Guidance in defining the minimum necessary activities for PHI to be covered under the notice and authorization procedures.
- Review and development of privacy for oral communications.
- A boilerplate business associates agreement and guidance for customization and execution.
- Guidance for policies and procedures regarding privacy of PHI between minors and parents.
- Guidance and procedures for understanding the rules of health-related communications and marketing.
- Guidance on the appropriate use of PHI in research.
- Guidance and procedures for the disclosure of PHI related to payment for services.

6 Security Requirements

These security requirements reflect the final security rule approved by Health and Human Services Secretarty Tommy Thompson on February 13, 2003. This document is still being updated with the specific offering information from Practical Security, Inc.

6.1 Administrative Safeguards §.308

The administrative requirements and supporting implementation features are presented at § 164.308. Each entity must maintain documentation demonstrating the development, implementation, and maintenance of appropriate security measures that include, at a minimum, the requirements and implementation features set forth in this section. In addition, entities must maintain necessary documentation to demonstrate that these measures have been periodically reviewed, validated, updated, and kept current.

6.1.1 Standard: Security Management Process §.308(a)(1)

A process for security management is required. This involves creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches. We would require the organization to have a formal security management process in place to address the full range of security issues. Security management includes the following implementation features:

- Risk analysis (Required)
- Risk management (Required)
- A sanction policy (Required)
- Information System Activity Review (Required)

PSI Provides: A documented security management process.

6.1.1.1 Implementation Specification: Risk Analysis (Required)

6.1.1.2 Implementation Specification: Risk Management (Required)

6.1.1.3 Implementation Specification: Sanction Policy (Required)

6.1.1.4 Implementation Specification: Information System Activity Review (Required)

There is a requirement for an ongoing in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an entity. This is important to enable the organization to identify potential security violations.

PSI Provides: Review and development of internal audit policies and procedures tailored to your specific organizational needs.

6.1.2 Standard: Assigned Security Responsibility §.308(a)(2)

Security responsibility is required to be assigned to a specific individual or organization, and the assignment be documented. These responsibilities include the management and supervision of (1) the use of security measures to

protect data, and (2) the conduct of personnel in relation to the protection of data. This assignment is important to provide an organizational focus and importance to security and to pinpoint responsibility.

PSI Provides: Assists in the selection and training of the individual with security responsibility.

6.1.3 Standard: Workforce Security §.308(a)(3)

There is a requirement that all personnel with access to health information must be authorized to do so after receiving appropriate clearances. This is important to prevent unnecessary or inadvertent access to secure information.

Workforce Security includes the following implementation features:

- Authorization and/or Supervision (Addressable)
- Workforce Clearance Procedure (Addressable)
- Sanction Policy (Required)
- Termination Procedures (Addressable)

PSI Provides: Review and development of personnel security policies and procedures.

6.1.3.1 Implementation Specification: Authorization and/or Supervision (Addressable)

6.1.3.2 Implementation Specification: Workforce Clearance Procedure (Addressable)

6.1.3.3 Implementation Specification: Sanction Policy (Required)

6.1.3.4 Implementation Specification: Termination Procedures (Addressable)

There is a requirement to implement termination procedures, which are formal, documented instructions, including appropriate security measures, for the ending of an employee's employment or an internal/external user's access. These procedures are important to prevent the possibility of unauthorized access to secure data by those who are no longer authorized to access the data. Termination procedures include the following mandatory implementation features:

- Changing combination locks
- Removal from access lists
- Removal of user account(s)
- Turning in keys, tokens, or cards that allow access

PSI Provides: Review and development of termination procedures.

6.1.4 Standard: Information Access Management §.308(a)(4)

Information Access Management includes the following implementation features:

- Isolating Health Care and Clearinghouse Function (Required)
- Access Authorization (Addressable)
- Access Establishment and Authorization (Addressable)

PSI Provides: Review and implementation.

6.1.4.1 Implementation Specification: Isolating Health Care and Clearinghouse Function (Required)

6.1.4.2 Implementation Specification: Access Authorization (Addressable)

There is a requirement to put in place a mechanism for notification and obtaining consent (where applicable) for the use and disclosure of health information. These controls are necessary to ensure that only properly authorized individuals use health information. Either of the following implementation features may be used:

- Role-based access
- User-based access

PSI Provides: Review and development of authorization policies and procedures tailored to your specific organizational needs.

6.1.4.3 Implementation Specification: Access Establishment and Authorization (Addressable)

6.1.5 Standard: Security Awareness and Training §.308(a)(5)

Security training is required for all staff regarding the vulnerabilities of the health information in an entity's possession and procedures that must be followed to ensure the protection of that information. This is important because employees need to understand their security responsibilities and make security a part of their day-to-day activities. Security Awareness and Training includes the following implementation features:

- Security Reminders (Addressable)
- Protection from Malicious Software (Addressable)
- Log-in Monitoring (Addressable)
- Password Management (Addressable)

PSI Provides: Creation of a tailored security awareness program. PSI can provide this training for an additional charge.

6.1.5.1 Implementation Specification: Security Reminders (Addressable)

6.1.5.2 Implementation Specification: Protection from Malicious Software (Addressable)

6.1.5.3 Implementation Specification: Log-in Monitoring (Addressable)

6.1.5.4 Implementation Specification: Password Management (Addressable)

6.1.6 Standard: Security Incident Procedures §.308(a)(6)

There is a requirement to implement accurate and current security incident procedures. These are formal, documented instructions for reporting security breaches, so that security violations are reported and handled promptly. Security Incident Procedures includes the following implementation feature:

- Response and Reporting (Required)

PSI Provides: Review and development of security incident procedures.

6.1.6.1 Implementation Specification: Response and Reporting (Required)

6.1.7 Standard: Contingency Plan §.308(a)(7)

Contingency Plan includes the following implementation features:

- Data Backup Plan (Required)
- Disaster Recovery Plan (Required)
- Emergency Mode Operations Plan (Required)
- Testing and Revision Procedure (Addressable)
- Applications and Data Criticality Analysis (Addressable)

PSI Provides: Review and implementation.

6.1.7.1 Implementation Specification: Data Backup Plan (Required)

6.1.7.2 Implementation Specification: Disaster Recovery Plan (Required)

6.1.7.3 Implementation Specification: Emergency Mode Operations Plan (Required)

6.1.7.4 Implementation Specification: Testing and Revision Procedure (Addressable)

6.1.7.5 Implementation Specification: Applications and Data Criticality Analysis (Addressable)

6.1.8 Standard: Evaluation §.308(a)(8) (Required)

This is a requirement for due care (do it right the first time) and due diligence (continue to review and improve procedures). The law recognizes that you must continually revisit your implementation of security for it to remain effective.

PSI Provides: Review and implementation.

6.1.9 Standard: Business Associates Contracts and Other Arrangements §.308(b)(1)

If data is processed through a third party, the parties would be required to enter into a chain of trust partner agreement. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver are required, and depend upon each other, to maintain the integrity and confidentiality of the transmitted information. These agreements are important so that the same level of security will be maintained at all links in the chain when information moves from one organization to another.

Business Associates Contracts and Other Arrangements includes the following implementation feature:

- Written Contract or Other Arrangement (Required)

PSI Provides: We will provide your organization with a boilerplate Business Associates Contracts and tailor it to your specific organization. We do not provide legal advice or construct individual agreements for every business associate.

6.1.9.1 Implementation Specification: Written Contract or Other Arrangement (Required)

6.2 Physical Safeguards

The requirements and implementation features for physical safeguards are presented at § 164.310 of the final rule. Each entity must maintain documentation demonstrating the development, implementation, and maintenance of appropriate security measures that include, at a minimum, the requirements and implementation features set forth in this section. In addition, entities must maintain necessary documentation to demonstrate that these measures have been periodically reviewed, validated, updated, and kept current.

6.2.1 Standard: Facility Access Controls §.310(a)(1)

Facility Access Controls includes the following implementation features:

- Contingency Operations (Addressable)
- Facility Security Plan (Addressable)
- Access Control and Validation Procedures (Addressable)
- Maintenance Records (Addressable)

PSI Provides: Review and implementation.

6.2.1.1 Implementation Specification: Contingency Operations (Addressable)

A contingency plan is required to be in effect for responding to system emergencies. The organization would be required to perform periodic backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place.

PSI Provides: A contingency plan tailored to your organization.

6.2.1.2 Implementation Specification: Facility Security Plan (Addressable)

6.2.1.3 Implementation Specification: Access Control and Validation Procedures (Addressable)

6.2.1.4 Implementation Specification: Maintenance Records (Addressable)

6.2.2 Standard: Workstation Use §.310(b) (Required)

Each organization is required to have a policy/guideline on workstation use. These documented instructions/procedures delineate the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a terminal unattended). This is important so that employees understand the manner in which workstations must be used to maximize the security of health information.

PSI Provides: Review and development of workstation guideline policies.

6.2.3 Standard: Workstation Security §.310(c) (Required)

Each organization is required to put in place physical safeguards to eliminate or minimize the possibility of unauthorized access to information. This is important especially in public buildings, provider locations, and in areas where there is heavy pedestrian traffic.

PSI Provides: Provides guidance in establishing a secure workstation area.

6.2.4 Standard: Device and Media Controls §.310(d)(1)

Media controls are required in the form of formal, documented policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility. They are important to ensure total control of media containing health information. Device and Media Controls includes the following implementation features:

- Disposal (Required)
- Media Re-use (Required)
- Accountability (Addressable)
- Data Backup and Storage (Addressable)

PSI Provides: Review and development of media controls policies and procedures.

6.2.4.1 Implementation Specification: Disposal (Required)

6.2.4.2 Implementation Specification: Media Re-use (Required)

6.2.4.3 Implementation Specification: Accountability (Addressable)

6.2.4.4 Data Backup and Storage (Addressable)

6.3 Technical Safeguards §.312

Each entity must maintain documentation demonstrating the development, implementation, and maintenance of appropriate security measures that include, at a minimum, the requirements and implementation features set forth in this section. In addition, entities must maintain necessary documentation to demonstrate that these measures have been periodically reviewed, validated, updated, and kept current.

6.3.1 Standard: Access Control §.312(a)(1)

There is a requirement for access control that restricts access to resources and allows access only by privileged entities. It is important to limit access to health information to those employees who have a business need to access it. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation. Access Control includes the following implementation feature:

- Unique User Identification (Required)
- Emergency Access Procedures (Required)
- Automatic Logoff (Addressable)
- Encryption and Decryption (Addressable)

PSI Provides: Review and development of applicable access control policies and procedures tailored to your specific organizational needs.

6.3.1.1 Implementation Specification: Unique User Identification (Required)

6.3.1.2 Implementation Specification: Emergency Access Procedures (Required)

6.3.1.3 Implementation Specification: Automatic Logoff (Addressable)

6.3.1.4 Encryption and Decryption (Addressable)

6.3.2 Standard: Audit Controls §.312(b) (Required)

There is a requirement for an ongoing in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an entity. This is important to enable the organization to identify potential security violations.

PSI Provides: Review and development of internal audit policies and procedures tailored to your specific organizational needs.

6.3.3 Standard: Integrity §.312(c)(1)

Each organization is required to be able to provide corroboration that data in its possession has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, a message authentication code, or digital signature. Integrity includes the following implementation feature:

- Mechanism to authenticate electronic protected health information (Addressable)

  PSI Provides: Review and development of integrity procedures.

6.3.3.1 Implementation Specification: Mechanism to authenticate electronic protected health information (Addressable)

6.3.4 Standard: Person or Entity Authentication §.312(d) (Required)

Each organization is required to implement entity authentication, which is the corroboration that an entity is who it claims to be. Authentication is important to prevent the improper identification of an entity that is accessing secure data.

PSI Provides: Review and development of authentication policies and procedures tailored to your specific organizational needs.

6.3.5 Standard: Transmission Security §.312 (e)(1)

Transmission Security includes the following implementation features:

- Integrity Controls (Addressable)
- Encryption (Addressable)

PSI Provides: Review and implementation.

6.3.5.1 Implementation Specification: Integrity Controls (Addressable)

6.3.5.2 Implementation Specification: Encryption (Addressable)

7 Privacy Regulation

What a provider has to do to meet the privacy regulations:

- **Provide information to patients** about their privacy rights and how their information can be used.
- Adopt clear privacy **procedures** for its practice.
- **Train employees** so that they understand the privacy procedures.
- **Designate an individual to be responsible** for seeing that the privacy procedures are adopted and followed.
- **Secure patient records** containing individually identifiable health information so that they are not readily available to those who do not need them.

7.1 Notice (Previously Consent)

[*45 CFR § 164.506*]

Consent — Under the final modifications, direct treatment providers *are no longer required to obtain consent* prior to the use or disclosure of protected health information (PHI). The decision on whether or not to obtain consent, and the form of that consent (if any) will now be entirely optional and left to providers' discretion, except to the extent required by state law.

Notice of Privacy Practices — In lieu of consent, direct providers are obligated to make a good faith attempt to obtain an individual's written acknowledgement of receipt of the Notice of Privacy Practices (NPP). The NPP must be provided on or before the first delivery of service, except in emergency treatment situations. This requirement is applicable regardless of the form of service delivery, although the modifications do take into account practical considerations. For example, if a provider's first encounter with a patient is via telephone, the NPP requirement is satisfied if the provider mails the NPP to that individual the day following the conversation. Even if the individual fails to return the acknowledgement to the provider, the provider will be deemed to have made the required "good faith" attempt to obtain the written acknowledgement.

In response to concerns that the required NPP was too lengthy, the preamble to the final modifications recommends use of a "layered notice." This layered notice consists of a short cover page, containing a summary of the NPP, followed by the lengthier and more detailed NPP.

Authorizations — Although the modifications make consent optional for purposes of treatment, payment, and health care operations (TPO), the Privacy Rule still requires patient authorization for non-TPO uses of PHI.

The modified rule simplifies the authorization requirements by mandating the use of one standard authorization format as opposed to the three different context-specific format set forth under the Privacy Rule in its original form. The core elements of an authorization have been condensed to the following:

- description of the information to be used or disclosed,
- the identification of the persons or class of persons authorized to make the use or disclosure of the protected health information,
- the identification of the persons or class of persons to whom the covered entity is authorized to make the use or disclosure,

- a description of each purpose of the use or disclosure,
- an expiration date or event,
- the individual's signature and date, and
- if signed by a personal representative, a description of his or her authority to act for the individual.

7.2 Minimum Necessary

[*45 CFR §§ 164.502(b), 164.514(d)*]

Providers must define the minimum necessary activities for which PHI will be used. This is important because it must be stated clearly in the notification and any use of PHI beyond the minimum necessary use needs to be specifically authorized using another form.

The “minimum necessary” use and disclosure of personal health information to accomplish the intended purpose does *not* apply to:

- Disclosures to providers for treatment purposes;
- Disclosures to the patient himself;
- Uses or disclosures for which an individual has signed an authorization;
- Uses or disclosures required to comply with HIPAA transactions;
- Disclosures to DHHS that are needed in order to enforce HIPAA; and
- Uses or disclosures that are required by other law.

For routine disclosures, covered entities may rely on policies and procedures as standard protocols if they define “minimum necessary” for staff to carry out their jobs. If it is non-routine, a disclosure must be reviewed individually using reasonable criteria.

7.3 Oral Communications

[*45 CFR §§ 160.103, 164.501*]

Providers understand the sensitivity of oral information. For example, many hospitals already have confidentiality policies and concrete procedures for addressing privacy, such as posting signs in elevators that remind employees to protect patient confidentiality. If oral communications were not covered, any health information could be disclosed to any person, so long as the disclosure was spoken.

Covered entities must **reasonably safeguard protected health information** (PHI). Many health care providers already make it a practice to ensure reasonable safeguards for oral information – for instance, by **speaking quietly when discussing a patient's condition with family members in a waiting room or other public area, and by avoiding using patients' names in public hallways and elevators**.

Protection of patient confidentiality is an important practice for many health care and health information management professionals; covered entities can build upon those codes of conduct to develop the reasonable safeguards required by the Privacy Rule.

7.4 Business Associates

[*45 CFR §§ 160.103, 164.502(e), 164.514(e)*]

Most health care providers do not carry out all of their health care activities and functions by themselves; they require assistance from a variety of contractors and other businesses if the business associate maintains the only copy of information, it must promise to cooperate with the covered entity to provide individuals access to information upon request. PHI may be disclosed to a business associate *only* to help the providers and plans carry out their health care functions, not for the business associate to use independently.

A health care provider, health plan, or other covered entity is not liable for privacy violations of a business associate.

If the covered entity becomes aware of a pattern or practice of the business associate that constitutes a material breach or violation of the business associate's obligations under its contract, the covered entity must take "reasonable steps" to cure the breach or to end the violation.

7.5 Parents and Minors

[*45 CFR § 164.502(g)*]

Because a parent usually has authority to make health care decisions about his or her minor child, a parent is generally a "personal representative" of his or her minor child under the Privacy Rule and has the right to obtain access to health information about that minor child. This would also be true in the case of a guardian or other person acting *in loco parentis* of a minor.

7.6 Health-Related Communications and Marketing

[*45 CFR §§ 164.501, 164.514(e)*]

The Privacy Rule addresses the use and disclosure of protected health information (PHI) for marketing purposes in the following ways:

- Defines what is "marketing" under the rule;
- Removes from that definition certain treatment or health care operations activities;
- Sets limits on the kind of marketing that can be done as a health care operation; and
- Requires individual authorization for all other uses or disclosures of PHI for marketing purposes.

7.7 Research

[*45 CFR §§ 164.501, 164.508(f), 164.512(i)*]

The Privacy Rule establishes the conditions under which protected health information (PHI) may be used or disclosed by covered entities for research purposes. A covered entity may always use or disclose for research purposes health information, which **has been de-identified** (in accordance with §§ 164.502(d), 164.514(a)-(c) of the rule) without regard to the provisions below.

The Privacy Rule also defines the means by which individuals/human research subjects are informed of how medical information about them will be used or disclosed and their rights with regard to gaining access to information about themselves, when such information is held by covered entities.

In the course of conducting research, researchers may create, use, and/or disclose individually identifiable health information. **Under the Privacy Rule, covered entities are permitted to use and disclose PHI for research with individual authorization**, or without individual authorization under limited circumstances set forth in the Privacy Rule.

7.8 Payment

[*45 CFR 164.501*]

As provided for by the Privacy Rule, a covered entity may use and disclose protected health information (PHI) for payment purposes. “Payment” is a defined term that encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and for a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

In addition to the general definition, the Privacy Rule provides examples of common payment activities that include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims;
- Risk adjustments;
- Billing and collection activities;
- Reviewing health care services for medical necessity, coverage, justification of charges, and the like;
- Utilization review activities; and
- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).