

PRIVACY REGULATION OUTLINE

Compliance Date April 14, 2003

The following HIPAA regulation outline must only be used as a high-level reference guide and not as a warranty or representation of Misys Healthcare Systems. You should obtain copies of the HIPAA final and proposed regulations in their entirety for complete details and descriptions.

The Department of Health and Human Services (HHS), the agency responsible for creating rules and regulations to comply with HIPAA, maintains a web site. This web site provides links to the Final and Proposed rules along with Frequently Asked Questions, Press Releases, Milestones, etc. relating only to Administrative Simplification. The HHS web site address is:

www.aspe.hhs.gov/admsimp

Release of Information 164.501

The HIPAA Privacy Standard regulates the ability of Covered Entities to use and disclose Protected Health Information (PHI). PHI includes all individually identifiable health information, including demographic information, maintained or transmitted by a covered entity, whether in electronic or any other form.

Consent 164.502

A covered Health care provider must obtain an individual's consent for use or disclosure of PHI for Treatment, Payment or Health Care Operations.

- Treatment - Treatment includes the provision, coordination or management of health care and related services and extends to consultation between providers or the referral of a patient from one provider to another.
- Payment - Payment applies to a broad range of activities including obtaining premiums, reimbursement, eligibility and coverage determinations, risk adjustment billing and claims management coverage and utilization review activities, as well as disclosure to consumer reporting agencies of certain information.
- Health Care Operations - Health Care Operations generally includes a Covered Entity's daily activities as they relate to the provision of healthcare.

Requirements for Consent 164.506(c)

The consent form must:

- Be in plain language.
- Inform the individual that PHI may be used and disclosed to carry out treatment, payment or health care operations.

- Refer the individual to the covered Entity's Notice of Privacy Practices (Notice) and explain that s/he has a right to review the description of potential uses and disclosures of his or her PHI in that Notice before signing the Consent.
- Alert the individual that the terms of the Notice may change and explain how to obtain a revised Notice.
- Include an explanation that the individual may request restrictions on the Covered Entity's use or disclosure of his or her PHI but that the Covered Entity is not required to comply with that request and is bound only if it expressly agrees to the requested restriction.
- State that the individual has a right to revoke consent, in writing, to the extent that the Covered Entity has not taken any action in reliance upon the Consent.
- Be signed and dated by the individual.

A Consent must be complete to be effective. 164.506(d) If a consent lacks any of the above elements, its is defective. The Consent may not be combined in a single document with the notice.

Exceptions to Consent 164,506(a)(2)

- Indirect treatment relationship with a patient. An indirect provider is a provider who normally delivers health care on the orders of another provider and reports back directly to that provider. A diagnostic radiologist and a clinical laboratory would be examples.
- In an emergency, or if Consent cannot reasonably be obtained due to communication barriers, the provider may wait until after services are provided to seek consent, and may be able to use or disclose PHI in the meantime. This covers only the use or release of information necessary to treat the emergency condition. In either case, the provider must document the attempt to obtain consent and the reason why consent was not obtained.

Obtaining Consent when not Required 164.506(a)(4)

- Even if the Privacy Standards do not require a Consent, a health plan, health care clearinghouse or an indirect Health care provider still may choose to obtain an individual's consent. If obtained, this Consent must meet the Privacy Standards.

Conflicting Consents 164.506(e)(1)

- If a Covered Entity has conflicting consents or authorizations for disclosure of PHI, the most restrictive document controls. The Covered Entity may try to resolve a conflict between the various documents by obtaining a new Consent or by contacting the individual.

Consent in an Organized Health Care Arrangement 164.506(f)

- When multiple providers participate in an organized health care arrangement and use a joint Notice, they may use a joint Consent to comply with the Consent

requirements. A joint Consent must identify the Covered Entities to which the Consent applies. If an individual revokes a joint Consent, then the recipient of the revocation has a responsibility to inform the Covered Entities covered by the joint Consent.

Authorizations 164.508

Authorization is required if a Covered Entity wishes to use or disclose PHI for purposes *other than* Treatment, Payment or Health Care Operations.

Requirements for Authorization 164.508(c)

In general, authorizations must be in plain language and must contain the following core elements:

- A specific description of the information to be used or disclosed.
- The name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure.
- The name or specific identification of the person(s) to whom the use or disclosure is permitted.
- An expiration date (or event that triggers expiration).
- A statement of the individual's right to revoke the authorization in writing.
- A statement that the information used or disclosed may be subject to re-disclosure by the recipient, in which case it is no longer subject to the Privacy Standards.
- The individual's signature and the date.
- If the signature belongs to the individual's personal representative, a description of that person's authority to act for the individual.

If the Authorization is requested by a Covered Entity for its own use, the authorization must, in addition to the core elements provide 164.508(d):

- A statement that the covered entity will not condition treatment, payment, enrollment in the health plan or eligibility for benefits upon authorization.
- A description of each purpose of the requested use or disclosure.
- A statement that the individual may inspect or copy the PHI to be used or disclosed.
- A statement that the individual may refuse to sign the authorization.
- A statement that the use or disclosure will result in remuneration to the Covered Entity by a third party.

Like the Consent, an Authorization must be complete to be effective. An authorization is not valid if it lacks any of the required elements, has expired, has been filled out incorrectly, has been revoked, is improperly combined with other documents or contains material known to be false. A Covered Entity must document and retain all signed and completed authorizations and provide a copy to the individual who signs it. An individual may revoke an Authorization at any time, so long as the revocation is in writing.

Verbal Agreements After the Opportunity to Agree or Object 164.510

In limited circumstances, a Covered Entity may disclose PHI only if the individual has had the opportunity to agree to, prohibit or restrict the disclosure. No written consent or authorization is required as long as the individual is informed in advance. The three circumstances are:

- Directories - Facility directory
- Involvement in Care - Disclosure of PHI to family, relatives or persons identified by the individual.
- Notification - Authorized person to be notified regarding individuals location, general condition or death.

Required Disclosures 164.502(a) & 164.524(a)

The only required disclosures under HIPAA are to patients themselves and to DHHS. Individuals generally have the right to inspect and copy their own PHI with the exception of psychotherapy notes. Disclosure to DHHS would be required as part of a DHHS investigation.

Permitted Uses and Disclosures 164.512

The Privacy Standard identifies certain permissible uses and disclosures without the need to obtain the written Consent or Authorization from the individual. The following are permissible uses and disclosures:

- As requested by law
- For public health activities
- About victims of abuse, neglect, or domestic violence
- For health oversight activities
- For judicial and administrative proceedings
- For law enforcement purposes
- About decedents
- Cadaveric organ, eye or tissue donation purposes
- Research purposes (certain limited uses and disclosures of PHI may occur for research purposes.)
- To avert a serious threat to health or safety
- For specialized government functions (such as military, national security, intelligence)
- Workers' compensation (State law dictates disclosure requirements)

Minimum Necessary Disclosure 164.502(b) & 164.514 (d)

When using or disclosing PHI or requesting PHI from another covered entity, the covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure or request. However, minimum necessary does not apply to requests by a health care provider for treatment, the individual or the Secretary of DHHS.

The Covered Entity must identify persons who need access to PHI and limit access accordingly. Documented policies and procedures regarding routine and recurring disclosures must be in place, along with a review process for other requests to ensure that the information sought is the minimum necessary.

Additional Use and Disclosure Rules.

Marketing and Fundraising 164.501 & 164.501(e) & (f)

In most cases, marketing and fundraising activities are not considered health care operations and would require written authorization. Authorization is not required for marketing of products or services if the communication occurs in a face to face encounter and meets the communications requirements of 164.514(e) (3). Following are the face to face marketing activities:

- Marketing of products or services of nominal value
- Marketing describing the participants or services of a health care network or health plan.
- Marketing by a health care provider tailored to the individual for the purpose of treatment.
- Marketing of health-related products or services.
- Fundraising by the Covered Entity may use or disclose certain PHI to a Business Associate. These disclosures may include:
 - Demographic information
 - Dates of health care provided
- Fundraising by the Covered Entity must include reasonable opt-out abilities available to the patient.
- Fundraising outside of the meaning of Health Care Operations requires Authorization by the patient.

Additional rules regarding use and disclosure: 164.502(c)

1. Eligibility and enrollment determinations
2. Employment determinations
3. Agreed restrictions
4. Deceased individuals
5. Personal representatives
6. Minors
7. Business associates - (this will be covered further in this outline)
8. Psychotherapy notes - 164.508(a)2
9. Research - 164.508(f)

De-Identified Information 164.514

Health information that does not identify an individual and which there is not reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

De-identified information may be used or disclosed freely as long as no means of re-identification is disclosed. Information is presumed to be de-identified if all the specified identifiers are removed.

Identifiers that are removed or concealed:

Name	Address	Relatives	Employer
Dates	Telephone	Fax	e-mail
SSN	MR#	Plan ID	Account #
License #	Vehicle ID	URL	IP Address
Fingerprints	Photographs	Other Unique Identifiers	

Business Associate Agreements 164.502(e) & 164.504(e)

HIPAA regulations define a Business Associate as a person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right.

Who can be Business Associates

Business Associates are persons or organizations who receive PHI from a covered entity and perform a function or task using this PHI.

Examples:

Consultants	Vendors	Management Firms
Clearinghouses	Billing Firms	Lawyers
Other Covered Entities	Accountants	Auditors
Financial Services	Accreditation Organizations	

Who are not Business Associates - Generally

Below are examples of arrangements that will generally not constitute business associate relationships:

Provider and Plan	Hospital and medical staff
Workforce	Provider and Provider for treatment
Financial Institutions	Mail Services

Business Associate Agreement 164.504(e)(2)(B)(ii)

The agreement will be between the covered entity and a business associate, and will establish the permitted and required uses and disclosures of such information by the business associate. This agreement must contain the following assurances from the business associate:

- Not to use or disclose protected health information other than as permitted or required by the contract or as required by law.

- Use appropriate safeguards to prevent use or disclosure of the information other than as provided by its contract.
- Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware.
- Ensure that any agents or subcontractors will agree to the same restrictions and conditions as the business associate.
- Make available protected health information in accordance with 164.524; "Access of individuals to protected health information."
- Make available protected health information for amendment 164.526 and incorporate any amendments of protected health information.
- Make available the information required to provide an accounting of disclosures in accordance with 164.528.
- Make available to the Secretary of DHHS the business associate's internal practices, books and records relating to the use and disclosure of PHI for purposes of determining the covered entity's compliance if requested.
- If termination of the contract return or destroy all PHI, if feasible. If it is not possible to return or destroy the information due to obligations or legal requirements, the protections of the agreement must apply until the information is returned or destroyed.

Other terms and agreements of the Business Associate Agreement

164.504(e)(4)

- Data aggregation services
- Breach and Termination
- Oversight and due diligence of business associates

Individual Patient Rights

HIPAA Privacy Regulations provide individuals with certain rights regarding their PHI. The general provisions of this regulation include the following rights of the individual:

- Adequate notice of disclosures of PHI
- Access to PHI
- Request for amendment and/or correction of PHI
- Request for accounting of disclosures of PHI, other than for treatment, payment or health care operations.
- Restrictions on the disclosure of PHI

Notice of Privacy Practices for Protected Health Information 164.520

With few exceptions, an individual has the right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity. This right allows the individual to understand and control how their PHI will be used and disclosed.

- **Content of Notice**

- The notice must be in plain language.
- The header of the notice must contain the following:
"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION PLEASE REVIEW IT CAREFULLY."
- For uses and disclosures, the notice must contain:
 1. A description, with at least one example of types of uses and disclosures.
 2. A description, of each of the other purposes that the covered entity is permitted without individual's consent.
 3. Other law descriptions that are more stringent.
 4. A description must include sufficient detail.
 5. A statement that other uses and disclosures will be made only with individual's written authorization and that individual may revoke authorization.
- Separate Statements for certain uses/disclosures:
 1. A covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health related benefits and services.
 2. A covered entity may contact the individual to raise funds.
 3. A group health plan may disclose to sponsor of plan.
- Individual Rights
The notice must contain a statement of the individual's rights concerning PHI and a brief description of how the individual may exercise these rights. It must include:
 1. The right to request restrictions on certain uses and disclosures including, and a statement that the covered entity is not required to agree to the requested restriction.
 2. The right to receive confidential communications.
 3. The right to inspect and copy PHI.
 4. The right to amend PHI.
 5. The right to receive an accounting of disclosures.
 6. The right to receive a copy of notice electronically or on paper.
- Covered Entities duties:
 1. A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices.
 2. A statement that the covered entity is required to abide by the terms of the notice.

3. A statement that it reserves the right to change terms of its notice and describe how it will provide individuals with a revised notice.
- **Complaints**
The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated. It must also contain a brief description of how the individual may file a complaint and a statement that the individual will not be penalized for filing a complaint.
 - **Contact**
The notice must contain the name or title and telephone number of a person or office to contact for further information as required by 164.530.
 - **Effective date**
The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.
 - **Specific requirement for Health Plans 164.520 (c)(1)**
 - **Specific requirement for certain covered health care providers 164.520(c)(2)**
 - **Specific requirements for electronic notice 164.520(c)(3)**
 - **Implementation specifications: Joint notice by separate covered entities. Covered entities that participate in organized health care arrangements may comply by joint notice. 164.520(d)**
 - **Implementation specifications: Documentation. A covered entity must document compliance with the notice requirements by retaining copies of the notices issued. 164.520(e)**

Rights to request privacy protection for protected health information 164.522

Right for individuals to request restriction of uses and disclosures.

- Covered entities must permit individuals to request that the covered entity restrict uses and disclosures.
- Covered entities are not required to agree with the restriction.
- A covered entity may terminate its agreement to a restriction.

Confidential Communications

A health plan must permit individuals to request, and must accommodate reasonable requests, to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of the information could endanger the individual.

Conditions for providing confidential communications are outlined in 164.522(3)

Access of individuals to protected health information 164.524

Right of access

- To inspect and obtain a copy of PHI about the individual in a designated record set.
- Except for psychotherapy notes, information compiled for civil, criminal, etc. proceedings, Clinical Laboratory Improvements Amendments of 1988.

Unreviewable grounds for denial

- Promise of confidentiality

Reviewable grounds for denial

- Endangering the life of individual
- Information makes reference to another person

Requests for access and timely action

- Covered entity may require requests in writing
- Covered entity must act no later than 30 days after receipt of request and only one extension is allowed.
- Covered entity must provide the information in the format requested by the individual if readily producible, or in a readable hard copy format, or may provide a summary if the individual agrees.
- May impose reasonable cost-based fee.

Amendment of protected health information 164.526

Right to Amend

- Individuals have the right to have a covered entity amend protected health information or a record in a designated record set.

Covered entity may deny request if:

- Information was not created by the covered entity
- Information is not part of the designated record set
- Information would not be available under the rule
- Information is accurate and complete

Right to Accounting of Disclosures of protected health information 164.528

An individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six (6) years prior to the date on which the accounting is requested, except for disclosures made:

1. To carry out treatment, payment and health care operations
2. To an individual regarding their own information
3. For the facility's directory or to persons involved in the individual's care
4. For national security or intelligence purposes
5. To correctional institutions or law enforcement officials
6. Prior to the compliance implementation date.

A covered entity does not have the right to deny an individual's request to receive an accounting of disclosures.

Implementation Tasks

- Request Form - The covered entity should determine whether to require individuals to make requests for an accounting in writing and if so, they must notify the individuals of this requirement in advance.
- Time to Respond to Request - Upon receipt of request for an accounting, the covered entity should either date stamp the request or enter the request in a date log book.
 1. The covered entity has 60 days to respond
 2. If unable to respond in 60 days then it may extend the time by no more than 30 days, which must be done in writing.
- Responding to a Request for an Accounting of Disclosures
 1. The response must be in writing
 2. It must include disclosures of information that occurred during the six years prior to the date of the request (or shorter time period, if requested by the individual)
 3. It must include disclosures made to or by the Covered Entity's business associates
 4. It must include the dates of each disclosure
 5. It must include a brief description of the information disclosed
 6. It must include a brief statement of the purpose for the disclosure
 7. For multiple disclosures made during an accounting period to the same person or entity for a single purpose or pursuant to a single authorization, the covered entity response must include:
 - The frequency, periodicity, or number of disclosures made during the accounting period
 - The date of the last such disclosure
- Fees - The covered entity must provide the first accounting to an individual in any 12 month period without charge. Thereafter, for any additional accounting request within the 12 month period, the covered entity may charge a reasonable cost based fee. However, to impose such a fee, the covered entity must provide advance notification of the fee so as to provide the individual with an opportunity to withdraw or modify the request.
- Documentation - A covered entity must document the following and retain the documentation.
 1. The information required to be included in an accounting.
 2. The written accounting that is provided to the individual from the request.
 3. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Administrative Requirements 164.530

Personnel designations

- Designate a Privacy Official - individual responsible for development and implementation of the policies and procedures of the covered entity.

- Designate a contact person or office for receiving complaints under the privacy regulations, and who is able to provide further information about such matters.

Training

- A covered entity must train all members of its workforce on the policies and procedures with respect to PHI.
- All workforce members must be trained by the compliance date and updated of any policy or procedure changes. Newly hired individuals must be trained in respect to PHI in a reasonable period of time.
- The covered entity must document that training has been provided.

Standard Requirements under Privacy

- Safeguards - A covered entity must have appropriate administrative, technical and physical safeguards to protect PHI.
- Complaints - Provide individuals with a process to make complaints regarding the covered entity's policies and procedures. The covered entity must also document complaints received and the disposition, if any.
- Sanctions - Covered entity must have appropriate sanctions in place for individuals of the workforce who fail to comply in regards to PHI. These sanctions must be documented.
- Mitigation - Mitigate to a practicable extent.
- Refraining from intimidating or retaliatory acts - A covered entity may not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual or other persons for filing a complaint.
- Waiver of rights - Individual may not be required to waive right as a condition for the provision of treatment, payment, enrollment in a health plan or eligibility of benefits.
- Policies and Procedures - A covered entity must implement reasonable policies and procedures with respect to PHI as set forth in the Privacy Standards.
- Documentation - A covered entity must maintain policies and procedures in written or electronic form, if communication or action is required maintain a copy.