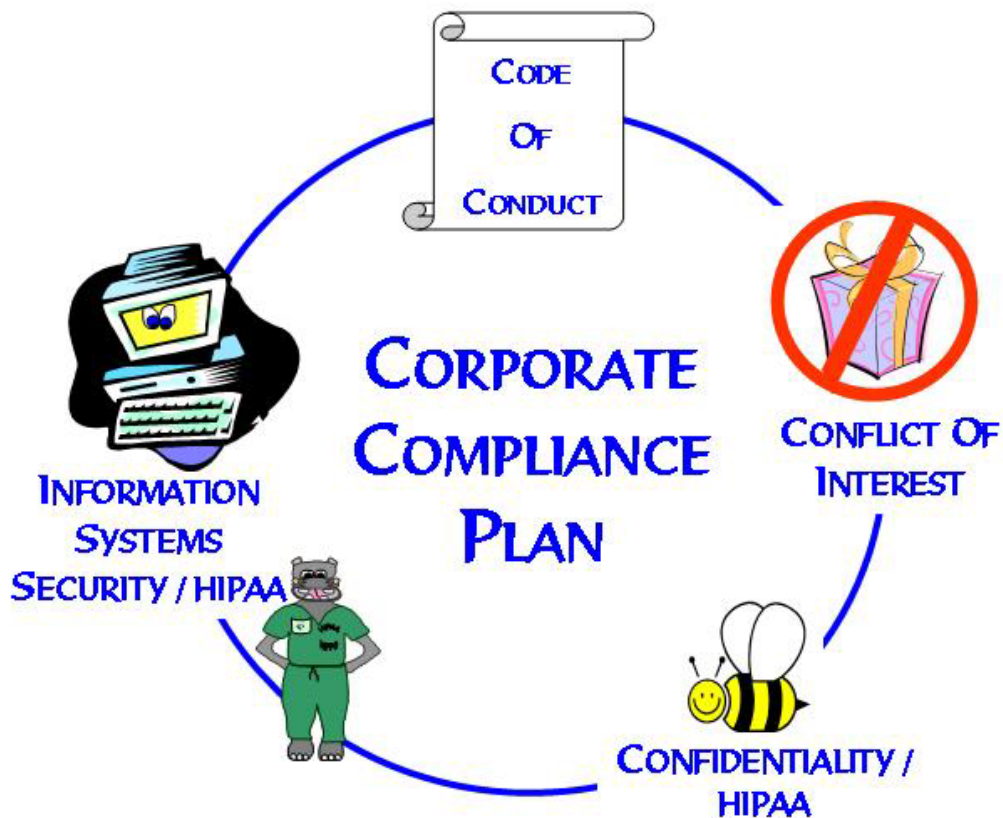


METHODIST HEALTH SYSTEM

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) GUIDE




METHODIST
HEALTH SYSTEM

7/2006

CONTENT OUTLINE

	PAGE
Resources	1
I. Patient Rights and HIPAA	2
II. Health Care Operations.....	3
A. Health Care Operations Includes	
III. Use and Disclosure of PHI Permitted without an Authorization.....	4
A. General Use and Disclosure	
IV. Use or Disclosure for Payment Purposes.....	4-5
A. HIPAA Payment Regulations Apply	
B. Payment Activities Include	
V. Privacy Notice and Acknowledgement	5-7
A. Purpose of the Notice	D. Questions about the Notice
B. Content of the Notice	E. Providing the Notice to Patients
C. Providing the Notice to Patients	F. OHCAs
VI. Patient Requests.....	8-9
A. Requests for Alternative Communications	C. Terminating Agreements to Restrict
B. Requests for Additional Restrictions	D. Limitations to Requests for Restriction
VII. Authorizations to Disclose PHI.....	9-10
A. Instances Where Authorizations are Generally Required	B. Authorizations Used as a Condition of Service
	C. Authorization Requirements
	D. Revocation of Authorization
VIII. Directory Information	11
IX. Direct versus Indirect Treatment under HIPAA	11
A. Direct Treatment Relationships	B. Indirect Treatment Relationships
X. Minimum Necessary.....	12
XI. Access to Medical Records	12-14
A. Exclusions to the Right of Access	D. Denying Access to PHI with an Opportunity to Appeal
B. Psychotherapy Notes	E. Denial Process
C. Denying Access to PHI without Opportunity to Appeal	F. PHI not Maintained Onsite
XII. Amendment of Records	15-16
A. Exemptions to the Right of Amendment	C. When an Amendment to the Record is Denied
B. When an Amendment to the Record is Accepted	D. How to Respond to Statements of Disagreement

CONTENT OUTLINE

XIII. Personal Representatives 16-17

XIV. Requests for Information by Family Members..... 17-18

XV. Verification of Requestor’s Authority and Identity.....18

XVI. Accounting for Disclosures..... 18-20

 A. What to Include in an Accounting

 B. Exclusions to the Need to Account for Disclosures

 C. General Accounting for Disclosures Requirements

 D. Temporary Suspension of Accounting for Disclosures

 E. Accounting for Disclosures Requirement and Research

XVII. Disclosures Made to an Employer.....20

XVIII. Judicial and Administrative Proceedings.....21

 A. Disclosures for Judicial and Administrative Proceedings

 B. Satisfactory Assurance

 C. Disclosure without Satisfactory Assurance

XIX. Public Health under HIPAA22

 A. Public Health Authorities

 B. Food and Drug Administration

 C. Communicable Disease

XX. Incidental Disclosures and Office Practices23

XXI. Disposal and Retention of Records23

XXII. Marketing and HIPAA 24-25

 A. Definitions of Marketing

 B. Exceptions to the Marketing Definition

 C. Other Laws

 D. Authorization to Disclose PHI for Marketing Purposes

XXIII. Fundraising 25-27

 A. Use of PHI for Fundraising

 B. Fundraising Communication Requirements

 C. Opt-out versus Opt-in

XXIV. Complaints27

XXV. Consequences of Noncompliance.....27

XXII. Where to Go For Questions27

RESOURCES

SARA JUSTER

MHS CORPORATE COMPLIANCE OFFICER..... 354-2174

KIM LAMMERS

JENNIE EDMUNDSON COMPLIANCE OFFICER..... 396-6084

MARY MEYSENBURG

MH PRIVACY OFFICER..... 354-4667

MARY THOMAS

PCI PRIVACY OFFICER 354-5616

HIPAA REGULATIONS

I. PATIENT RIGHTS AND HIPAA:

HIPAA provides all patients with certain rights with respect to their protected health information (PHI). These include the right:

- To inspect and obtain a copy of their health records.
- To correct and amend any errors in those records or put a statement of exception in the record for information with which the patient disagrees.
- To receive an accounting of any disclosures of the records.
- To request additional protections for particularly sensitive information in the records.

In addition, the patient must:

- Be given a Notice of MHS privacy practices.
- Sign a written acknowledgement of receipt of that Notice.
- Sign an Authorization before any "extra" uses and disclosures, such as research.
- Be given an opportunity to agree or object to other types of use or disclosure.
- Be provided with the names, offices, and procedure to file a complaint about the privacy practices of an MHS affiliate.

Health care institutions covered by HIPAA (covered entities) must train their entire work force about HIPAA. They must also establish policies and procedures to protect patients' rights. Covered entities are organizations that routinely handle protected health information (PHI) in any capacity. Each member of the workforce of a covered entity is also covered by HIPAA.

PHI includes any information created or received by an MHS affiliate that relates to the:

- Past, present, or future physical / mental health / condition of an individual.
- Provision of health care to an individual.
- Past, present, or future payment for an individual's health care.

II. HEALTH CARE OPERATIONS:

HIPAA permits us to use or disclose a patient's PHI for **health care operations** without obtaining that patient's permission. Health care operations include many functions under HIPAA.

A. HEALTH CARE OPERATIONS INCLUDE:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines or protocols.
- Population-based activities relating to improving public health or reducing health care costs.
- Evaluating health plan performance.
- Underwriting, premium rating and other activities relating to health insurance contracting.
- Conducting or arranging for medical review, legal services, auditing functions, or other compliance programs.
- Business planning and development, cost-management, and planning-related analyses.
- Development or improvement of methods of payment or coverage policies.
- Business management and general administrative activities of the entity.
- Business activities relating to compliance with HIPAA.
- Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers (provided protected health information is not disclosed).
- Resolution of internal grievances.

III. USE AND DISCLOSURE PERMITTED WITHOUT AN AUTHORIZATION:

A. GENERAL USE AND DISCLOSURE OF PHI:

In general, HIPAA permits us to use or disclose PHI without an authorization to / for:

- A patient or his / her authorized representative.
- Treatment, payment, or other health care operations.
- IRB or Privacy Board approved research.
- Other entities in compliance with permitted uses and disclosures for law enforcement, judicial, or administrative proceedings, etc.
- Avert a serious, imminent threat to public health or safety.
- The Secretary of Department of Health and Human Services (DHHS) for investigations of complaints or general compliance reviews.
- Fundraising or marketing.
- When all patient-identifying information has been removed.

With some exceptions (e.g., related to information exchanged between / among providers for treatment), such uses and disclosures must be limited to the minimum necessary.

IV. USE OR DISCLOSURE FOR PAYMENT PURPOSES:

HIPAA permits us to use or disclose a patient's PHI for **payment** without obtaining the patient's permission. Payment is broadly defined under HIPAA. The term includes almost any activity involved in our attempt to obtain payment for the health care services we provide.

A. HIPAA PAYMENT REGULATIONS APPLY TO:

- Health care providers who obtain reimbursement for health care services.
- Health plans who provide reimbursement to providers of health care services.

IV. USE OR DISCLOSURE FOR PAYMENT PURPOSES (CONT'D):

B. PAYMENT ACTIVITIES INCLUDE:

- Determinations of eligibility or coverage.
- Adjudication or subrogation of health benefit claims.
- Risk adjustment activities based on enrollee health status and demographic characteristics.
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance.
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.
- Utilization review activities, including precertification and pre-Authorization of services, concurrent and retrospective review of services.
- Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
 - Name and address
 - Date of birth
 - Social Security Number
 - Payment history
 - Account number(s)
 - Name(s) and address(s) of health care provider(s) and / or health plan(s)

V. PRIVACY NOTICE AND ACKNOWLEDGEMENT:

HIPAA imposes several new requirements on health care providers, including the requirement that direct treatment providers give all patients a Privacy Notice and post the Notice in public areas. We must also provide the Notice to any person who requests a copy. We are not, however, required to give inmates a Privacy Notice.

V. PRIVACY NOTICE AND ACKNOWLEDGEMENT (CONT'D):

Direct providers must also make a good faith effort to obtain a written acknowledgement of receipt from each patient. The acknowledgment simply states that the patient has received our Privacy Notice, not that they have read, understood, or agreed with it.

A. PURPOSE OF THE NOTICE:

The notice-and-acknowledgment process is intended to create an "initial moment" during which patients can:

- Discuss their particular privacy questions and concerns.
- Request additional protections for information they consider particularly sensitive.
- Ask for more confidential communication methods.

B. CONTENT OF THE NOTICE:

The HIPAA privacy regulation specifies the content of the Notice. The regulation also requires the Notice be written in "plain language." The Privacy Notice outlines patients' legal rights and our legal duties with respect to protected health information (PHI).

C. QUESTIONS ABOUT THE NOTICE:

If patients have specific or complex questions, refer them to your Privacy Officer. However, you should be familiar enough with our Notice, the HIPAA regulation, and state privacy protections to answer basic patient questions.

D. PROVIDING THE NOTICE TO PATIENTS:

The notice must be given to patients no later than the first date of service delivery, including service delivered electronically or over the telephone. If service is not delivered in person, the Notice may be sent to the patient by e-mail, or standard mail. We can delay providing the Privacy Notice and obtaining an acknowledgment in emergency treatment situations until it is reasonably practical.

V. PRIVACY NOTICE AND ACKNOWLEDGEMENT (CONT'D):

D. PROVIDING THE NOTICE TO PATIENTS (CONT'D):

The Notice must be provided, and Acknowledgment obtained:

- When the patient arrives for a scheduled appointment or procedure.
- Via standard mail no later than the day of service if the first treatment is over the telephone.
- As soon as it is reasonable to do so when the patient is treated for an emergency condition.
- After pre-admission contact with the patient, the provision of the Notice and acknowledgement of receipt can be accomplished on the day of admission.

E. OHCAs:

MHS affiliate hospitals and their Medical Staffs participate in an organized health care arrangement (OHCA). HIPAA allows OHCA participants to comply with the Privacy Notice requirements by providing a joint Notice. Our joint Notice complies with HIPAA and:

- Describes with "reasonable specificity" all the entities, service delivery sites, and classes of service, and any PHI sharing that may occur.
- Specifies all participating entities agree to abide by identical information practices.
- Does NOT eliminate the need for physicians to provide a Privacy Notice to patients treated outside the hospital (i.e., in the office). However, a patient who has already received a Privacy Notice from an MHS hospital does not need to receive another copy of the Notice because all MHS affiliates are considered a single entity under HIPAA.

VI. PATIENT REQUESTS:

A. REQUESTS FOR ALTERNATIVE COMMUNICATIONS:

Patients can also request certain kinds of PHI be communicated by alternative means or to alternative locations. HIPAA requires us to accommodate "**reasonable requests**" of this kind and prohibits us requesting, as a condition of providing confidential communications, an explanation from the patient as to why they are requesting a restriction.

B. RIGHT TO REQUEST ADDITIONAL RESTRICTIONS:

HIPAA gives patients the right to request additional restrictions on uses and disclosures of their PHI. Although patients have the right to make the request, we are not required to agree to any requested restriction. If we accept the restriction, we must abide by it except in emergencies where a use or disclosure is necessary to provide treatment. Pursuant to MHS policy, all requests for additional restrictions must be forwarded to the affiliate Privacy Officer for review and approval. Only the Privacy Officer may approve a requested restriction.

C. TERMINATING AGREEMENTS TO RESTRICT:

We may cancel our agreement to a restriction if the:

- Patient agrees to, or requests the termination in writing.
- Patient requests a termination orally (oral declaration must be documented).
- Patient is informed we are canceling our agreement to a restriction. In this case, the termination is only effective for the protected health information created or received after the patient has been informed.

VI. PATIENT REQUESTS (CONT'D):

D. LIMITATIONS TO REQUESTS FOR RESTRICTION:

HIPAA does not permit patients to restrict the uses and disclosures for the following purposes:

- Public health
- Abuse, neglect, or domestic violence reporting
- Health oversight
- Judicial or administrative proceedings
- Law enforcement
- Research under Privacy Board or IRB waiver
- Immediate threats to public safety
- Government functions
- Uses and disclosures otherwise required by law

VII. AUTHORIZATIONS TO DISCLOSE PHI:

We are permitted a broad range of uses and disclosures of PHI for treatment, payment, and other health care operations (TPO), without any permission from the patient. For some additional activities, the patient must provide an authorization.

A. INSTANCES WHERE AUTHORIZATIONS ARE GENERALLY REQUIRED:

1. **Psychotherapy Notes**, except for treatment uses by the originator of the notes (i.e., the therapist), supervised training of other mental health practitioners within the covered entity, or defense against a legal action brought by the subject of the notes.
2. **Research**, except where waived by an IRB or Privacy Board determination.
3. **Marketing**, unless activity fails to meet certain criteria for exception.
4. **Requests for release of PHI that does not fall within TPO**, such as information required as part of an insurance coverage application.

VII. AUTHORIZATIONS TO DISCLOSE PHI (CONT'D):

B. AUTHORIZATIONS USED AS A CONDITION FOR SERVICES:

We cannot condition treatment and payment for health services on an authorization except for:

- Research-related treatment, conditioned on provision of an authorization for research uses and disclosures.
- Enrollment in the health plan or eligibility for benefits on conditioned on provision of a pre-enrollment authorization for risk-rating or underwriting.
- A claim under plan coverage, if necessary to determine the level or validity of the payment.
- Provision of health care solely for creating PHI for disclosure to a third party can be conditioned on an authorization for disclosure to that third party (e.g., a life insurance physical exam).

C. AUTHORIZATION REQUIREMENTS:

A standard MHS Authorization form, as well as a checklist to evaluate non-standard authorizations, is available. The checklist will help you confirm authorizations you receive contain the required elements.

If we receive multiple conflicting authorizations, we are bound by the more restrictive authorization unless / until the conflict is resolved. The minimum necessary standard does not apply to authorizations of any kind

D. REVOCATION OF AUTHORIZATION

A patient may revoke an authorization at any time, provided the revocation is in writing, *except* to the extent we have taken actions relying on it. As with other HIPAA documentation retention requirements, we must keep a signed authorization for six years from the date of its creation or the date when it last was in effect, whichever is later

VIII. DIRECTORY INFORMATION:

HIPAA allows hospitals to continue to maintain "directories" of current patients that contain:

- Patient name.
- Location in the facility.
- Condition described in general terms, not communicating specific medical information.
- Religious affiliation.

The patient's name, location, and general condition may be disclosed to anyone who asks for the patient by name. Religious affiliation information may be disclosed to members of the clergy. No authorization is required for disclosure of such limited information. However, patients must be informed in advance this information will be included in a directory and given an opportunity to opt-out.

In emergency circumstances when it is not possible to give a patient an opportunity to object, directory information disclosures can be made if:

- The provider feels it would be in the best interests of the patient.
- No prior expressed preference of the patient to the contrary is known.
- An opportunity to object must be provided as soon as is practical.

IX. DIRECT VERSUS INDIRECT TREATMENT UNDER HIPAA:

A. DIRECT TREATMENT RELATIONSHIPS:

Providing, coordinating, or managing health care and related services by one or more health care providers is a direct treatment relationship.

B. INDIRECT TREATMENT RELATIONSHIPS:

Indirect treatment relationships are those where care is provided based on the orders of another health care provider. In such cases, while the services or products (such as a lab test or a diagnostic screening) may involve a relationship with the patient, the diagnostic or other results go to the direct health care provider. **Indirect treatment providers DO NOT need to give patients a separate Privacy Notice.**

X. MINIMUM NECESSARY:

HIPAA REGULATIONS

When using, disclosing, or requesting PHI, we must make reasonable efforts to limit ourselves to the minimum necessary to accomplish the job. The minimum necessary standard does not apply if we are providing the PHI to a patient or in response to an Authorization by the patient.

We may not use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount necessary to do the job. The Department of Health and Human Services (DHSS) has made it clear that the minimum necessary standard is to be implemented reasonably, so a provider's functions are not excessively restricted.

XI. ACCESS TO MEDICAL RECORDS:

HIPAA regulations grant every patient a right of access to inspect and obtain a copy of all protected health information within their medical records maintained by us.

- Our Privacy Notice informs patients all requests to access PHI must be writing.
- We must respond to requests within 30 days of receipt (10 days in Nebraska) by providing access or writing a response stating the reason(s) for denial.

A. PATIENTS' RIGHTS TO ACCESS EXCLUDES:

- Psychotherapy notes.
- Information compiled for use in civil, criminal or administrative proceedings.
- Information protected by the Clinical Laboratory Improvements Amendments of 1988 (CLIA).

XI. ACCESS TO MEDICAL RECORDS (CONT'D):

B. PSYCHOTHERAPY NOTES:

Psychotherapy notes receive special protection under HIPAA. Although PHI may generally be accessed for treatment, payment, or other healthcare operations without explicit permission from the patient, the use or disclosure of psychotherapy notes generally requires an authorization. The only exceptions are:

- For the originator of the notes to treat the patient.
- For students, trainees, or practitioners in supervised training programs.
- To defend a legal action or other proceeding brought by the patient against the covered entity.
- For lawful health oversight activities or as otherwise required by law.
- For coroners or medical examiners (where the patient is deceased).
- Where, consistent with applicable law and the standards to ethical conduct, there is a good faith belief the use or disclosure is necessary to prevent or lessen a serious threat to health or safety.

C. DENYING ACCESS TO PHI WITHOUT OPPORTUNITY TO APPEAL:

We can deny a patient's request for access to their PHI without opportunity to appeal in the following circumstances:

- The information falls into one of the excluded categories (see page 5).
- The request comes from an inmate in a correctional institution, and access would endanger the health or safety of that person or anyone else in the facility.
- The information is generated in the course of ongoing research, and disclosure would jeopardize the research (provided the patient must have agreed to such a restriction previously, and access rights are restored at the conclusion of the protocol).
- Records containing the information are subject to federal Privacy Act protections.
- The information was obtained from someone under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source.

XI. ACCESS TO MEDICAL RECORDS (CONT'D):

D. DENYING ACCESS TO PHI WITH AN OPPORTUNITY TO APPEAL:

We can deny a patient access to their PHI with an opportunity to appeal when a licensed health care professional determines that access is:

- Reasonably likely to endanger the life or physical safety of a patient or another person.
- Reasonably likely to cause substantial harm to the patient or another person.
 - Requests by a personal representative of a patient may be denied for the same reasons.

E. DENIAL PROCESS:

- We must make a good faith effort **only** to deny access to parts of the record that meet denial grounds on page 6, and provide the rest.
- If we do not possess the information, but know where it is maintained, we must inform the patient where to request access.
- We must have all denials reviewed by a licensed health care professional designated by us to act as a reviewing official. He / she must not participate in the original decision to deny.
- Patients may appeal our determination by complaining to DHHS.

F. PHI REQUESTED NOT MAINTAINED ONSITE:

If a patient requests access to information not maintained onsite or otherwise readily accessible, we have up to 60 days to provide access if we do not deny the request. (An additional 30-day extension is allowed, but a written explanation of the reasons for delay must be provided).

We can provide access at a convenient time and place, (i.e. normal business hours) or we can mail the requested information to the patient. The scope, format, and other aspects of the request may be negotiated with the patient, as necessary to achieve timely access. Individuals can agree to a summary or explanation of information instead of the actual information.

We may charge reasonable, "cost-based" fees for preparations of summaries and explanations, copying and postage, etc.

XII. AMENDMENT OF RECORDS:

HIPAA provides patients with "rights to amend" (to take exception to information in their records with which they disagree) and request corrections. We may choose to make requested changes; or the information can be left unchanged if it is believed to be correct. If left unchanged, we must document in the record the patient's disagreement.

Individuals have a right to amend any element of protected health information in the designated record set, for as long as we maintain that information. We are not obligated to amend the record if we determine another institution was the creator of the information at issue. This is true unless the patient provides a reasonable basis to believe the originator is no longer available to act on the request.

We have established policies and forms to process requests for amendments. We must act on requests no later than 60 days after receiving a request. (An additional 30 days is permitted, provided the patient is informed in writing of the reasons for the delay and given a date for completion). Acting on such a request means either correcting the record or providing the patient with a written denial.

A. EXEMPTIONS TO THE RIGHT OF AMENDMENT:

Protected health information exempt from HIPAA's right of access is also exempt from the right of amendment. Our Privacy Notice specifies amendment requests must be in writing and include supporting reason(s).

B. WHEN AN AMENDMENT TO THE RECORD IS ACCEPTED:

We must make reasonable efforts to inform and provide the amendment within a reasonable time to:

- Persons identified by the patient as having received health information about the patient and need the amendment.
- Persons, including business associates, we know have the information subject to the amendment and may have relied, or could foreseeably rely on it to the detriment of the patient.

XII. AMENDMENT OF RECORDS (CONT'D):

C. WHEN AN AMENDMENT TO THE RECORD IS DENIED:

If we refuse to amend the record, we must send a written rejection notice to the patient. It must include:

- The reasons for the denial.
- The patient's right to and the process to submit a "statement of disagreement."
- A statement that, even if a statement of disagreement is not submitted, he / she may still request us to include his / her request for amendment and our denial with any future disclosures of the information.
- The patient's right to and the process to submit a complaint to us and / or DHHS.

D. HOW TO RESPOND TO "STATEMENTS OF DISAGREEMENT":

We may respond to a patient's "statement of disagreement" with a "rebuttal statement". If we do so, it must be included in the health record and a copy provided to the patient. Future disclosures of PHI to which the disagreement relates must include at least a summary of the patient's objection(s) and our response(s). If we are informed of a correction by another covered entity, we must amend our own records. A privacy officer will handle these requests, and document that designation in the records.

XIII. PERSONAL REPRESENTATIVES:

For adults and emancipated minors (i.e., married minors or those serving in the Armed Forces), HIPAA's rules are straightforward:

- If a legal personal representative has the right to make decisions about the patient's health care, that legal representative may make decisions regarding the PHI associated with that health care.

XIII. PERSONAL REPRESENTATIVES (CONT'D):

For "unemancipated minors" (i.e., children), the parent or legal guardian generally has the right to make decisions regarding their child's PHI. There are, however, certain exceptions:

- If parental consent is not required for the care provided (i.e., STD's or substance abuse).
- When the parent has agreed to a confidential relationship between the child and the provider.
- When the provider has a reasonable belief the child may be subject to abuse or neglect.
- When the provider believes it is not in the best interest of the patient.

Currently, neither Nebraska nor Iowa restrict the ability of a non-custodial parent to access their child's PHI, absent a court order to the contrary.

An executor, administrator, or other person that has the right to act on behalf of a deceased person (or that patient's estate) is considered a personal representative under HIPAA.

Remember that state laws may provide greater restrictions than HIPAA regarding disclosure of information. In such cases, state law preempts HIPAA and we will continue to follow state law.

XIV. REQUESTS FOR INFORMATION BY FAMILY MEMBERS:

Sometimes a patient's family member may request and should be given PHI. For example, a pharmacist may use professional judgment and experience to make reasonable inferences of the patient's best interest in allowing a person, other than the patient, to pick up a prescription. If a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual, the pharmacist may safely assume that he / she is involved in the individual's care. The patient does not need to provide the pharmacist with the names of such persons in advance.

XIV. REQUESTS FOR INFORMATION BY FAMILY MEMBERS (CONT'D):

However, we must reasonably limit the amount of information disclosed for such purposes to the minimum necessary. In addition, we must abide by any reasonable requests for confidential communications and any agreed-to restrictions on the use or disclosure of PHI.

XV. VERIFICATION OF REQUESTOR'S AUTHORITY AND IDENTITY:

When a patient, legal representative, guarantor or other family member requests information over the telephone, we must make a good-faith effort to establish that person's authority and identity. In order to establish their authority, you may request they fax the legal document granting them authority to act on the patient's behalf. To establish their identity, you should ask for two or more data elements only they should know (e.g., Social Security number, birth date, ZIP code, physician's name, date(s) of service, account number, mother's maiden name, etc). Ask for as much of this information as you feel is necessary to establish identity. When in doubt about the caller's identity, do not give out PHI over the telephone.

XVI. ACCOUNTING FOR DISCLOSURES:

HIPAA gives patients the right to request an accounting of disclosures. An accounting is a listing of disclosures of a patient's PHI made by us or our business associates for up to six years preceding the request on or after April 14, 2003. Each MHS affiliate's HIM department will track the disclosures that must be accounted for. We have 60 days to provide the accounting. Therefore, if you should receive a request for an accounting, you should immediately forward the request to the appropriate affiliate Privacy Officer.

XVI. ACCOUNTING FOR DISCLOSURES (CONT'D):

A. IN GENERAL THE FOLLOWING DISCLOSURES MUST BE INCLUDED IN AN ACCOUNTING –

Disclosures for / about:

- Public health activities.
- Victims of abuse, neglect, or domestic violence.
- Health oversight activities.
- Judicial and administrative proceedings.
- Law enforcement purposes.
- Decedents.
- Organ Donation.
- Research.
- Averting serious threat to public health or safety.
- Specialized government functions
- Workers' Compensation
- Inadvertent or unauthorized disclosures.

B. EXCLUSIONS TO THE NEED TO ACCOUNT FOR DISCLOSURES:

1. Accountings do not include disclosures made to carry out treatment, payment, and health care operations.
2. Accountings may also exclude disclosures:
 - To the patient, of his or her own protected health information.
 - Made pursuant to a patient's Authorization.
 - Incidental to an otherwise permissible disclosure.
 - Disclosures that occurred before the HIPAA compliance date of April 14, 2003.

C. GENERAL ACCOUNTING FOR DISCLOSURES REQUIREMENTS:

Written accountings must include:

- Date of the disclosure (if multiple, start and stop date and the frequency,).
- Name and address of the entity or person who received the PHI
- Brief description of the PHI disclosed.
- Brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure.

XVI. ACCOUNTING FOR DISCLOSURES (CONT'D):

D. TEMPORARY SUSPENSION OF ACCOUNTING FOR DISCLOSURES:

Temporary suspension of an accounting may occur for national security, intelligence, health oversight, or law enforcement purposes.

Suspensions require an agency or official to provide a written statement that such an accounting would be reasonably likely to impede their activities.

The statement must specify the time for which such a suspension is required (oral requests of this kind are permitted, but can be in effect for no longer than 30 days without a written request as a follow-up).

E. ACCOUNTING FOR DISCLOSURES REQUIREMENT AND RESEARCH:

Disclosures for research operating under a waiver of authorization are not exempt from the accounting requirement. Disclosures made following an authorization for research are exempt. The requirement can be met by:

- Providing patients with a list of all practices for which their PHI may have been disclosed following a waiver.
- Researcher's name and contact information.

XVII. DISCLOSURES MADE TO AN EMPLOYER:

We may disclose PHI about an employee to an employer, workers' compensation insurer, State administrator, or other persons or entities involved in workers' compensation systems, without the individual's authorization under the following conditions:

- As authorized by and to the extent necessary to comply with workers' compensation or similar laws that provide benefits for work-related injuries or illness without regard to fault.
- To the extent the disclosure is required by State or other law. The disclosure must comply with and be limited to what the law requires.
- For purposes of obtaining payment for any health care provided to the injured or ill worker.

XVIII. JUDICIAL AND ADMINISTRATIVE PROCEEDINGS:

A. DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS:

We may disclose PHI in the course of any judicial or administrative proceeding:

- In response to a court order, as long as it discloses only PHI expressly authorized by such order.
- In response to a subpoena, discovery request, or other lawful process, not accompanied by a court order if:
 - We receive satisfactory assurance from the requestor that reasonable efforts have been made to ensure the patient has been given notice of the request.
 - We receive satisfactory assurance from the requestor reasonable efforts have been made to secure a qualified protective order.
- As long as we follow MHS guidelines to ensure compliance with state and federal law prior to releasing any information pursuant to a subpoena.

B. SATISFACTORY ASSURANCE:

Occurs when written statements or accompanying documentation demonstrates:

- Requestor made a good faith attempt to provide written notice to the patient or mailed a notice to the patient's last known address.
- The notice included sufficient information about the litigation or proceeding to permit the patient to raise an objection to the court.
- The time for the patient to raise objections to the court has elapsed, and:
 - No objections were filed or the court resolved all objections filed.
- The disputing parties have agreed to a qualified protective order and have presented it to the court.
- The requestor has asked for a qualified protective order from a court that:
 - Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding.
 - Requires the return of the PHI (including all copies made) at the end of the litigation or proceeding to us.

C. DISCLOSURE WITHOUT SATISFACTORY ASSURANCE:

We may disclose PHI without receiving satisfactory assurance if we make reasonable efforts to provide notice to the patient or seek a qualified protective order.

XIX. PUBLIC HEALTH UNDER HIPAA:

A. PUBLIC HEALTH AUTHORITIES:

Disclosure of PHI to public health authorities or other agencies authorized by law to collect or receive such data is allowed. Such disclosures may relate to:

- The reporting of diseases or injuries.
- "Vital events" such as birth or death.
- Reporting of child abuse or neglect.
- The conduct of public health surveillance, investigations, and interventions.

B. FOOD AND DRUG ADMINISTRATION (FDA):

Disclosures are permitted for purposes related to the quality, safety, or effectiveness of FDA-regulated product or activities. These include:

- Collecting or reporting adverse events, product defects or problems, or biological product deviations.
- Tracking FDA-regulated products.
- Enabling product recalls, repairs, or replacement, or for look-back.
- Conducting post-marketing surveillance.

C. COMMUNICABLE DISEASES:

Disclosures are permitted to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease / condition, as long as we or a public health authority is authorized by law to make such notifications.

XX. INCIDENTAL DISCLOSURES AND OFFICE PRACTICES:

Incidental uses and disclosures of PHI are inevitable. HIPAA requires you take reasonable steps to keep such incidental disclosures to a minimum. The following office practices can help minimize incidental disclosures:

- Discuss patient cases in areas where you cannot be overheard.
- Restrict what is on waiting room sign-in sheets (and how patients are called in from the waiting room).
- Move daily appointment logs and related documents away from patient traffic areas.
- Obscure names and other information visible on the charts left hanging on door and hallway racks.
- Move "white boards" and similar devices used to display patient information to less visible areas.

XXI. DISPOSAL AND RETENTION OF RECORDS:

HIPAA privacy and security standards require appropriate destruction of obsolete records containing PHI. We must assure secure disposal for any PHI it holds. Our business associates, on termination of a contract with us, must return or destroy all PHI in their possession. Where not possible, the business associate must extend the privacy / security protections of the contract for as long as the information is retained.

HIPAA privacy standards also address records retention. We must keep any documentation related to patient requests for access, amendment, or accountings of PHI disclosures for six years. The six year requirement extends to any policy or procedural documentation, including our Privacy Notice, consents (if any), authorizations, and the like (measured from the time of its creation, or when it was last in effect).

If state laws require longer retention of these or any other records held by us, the state requirements control.

XXII. MARKETING AND HIPAA:

A. DEFINITION OF MARKETING:

The Health Insurance Portability and Accountability Act defines marketing as: "Making a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service."

Marketing communications that use PHI require prior written authorization.

If on its face, the communication encourages the recipient of the communication to purchase or use the product or service, the communication is marketing.

Marketing is also defined as an arrangement between us and another covered entity where one discloses PHI in exchange for direct or indirect payment. The entity that receives the disclosed information uses it to communicate about its own product or service and encourage recipients to purchase or use that product or service.

B. EXCEPTIONS TO THE MARKETING DEFINITION:

- Information regarding a health-related product or service provided by MHS or an MHS affiliate.
- Information regarding a patient's treatment.
- Information regarding care coordination of a patient.
- Information regarding participants in a provider network or health plan:
 - Services offered by providers.
 - Benefits covered by a health plan.
 - Health-related information about benefits, products or services optionally available to a health plan enrollees.
 - Advice to health plan members about available health plan options that could enhance or substitute for existing coverage.
- Face-to-face communications made by us to a patient.
- Promotional gifts of a nominal value.
- General health or wellness information that does not promote a specific product or service.
- Communications about government or government-sponsored programs.

XXII. MARKETING AND HIPAA (CONT'D):

C. OTHER LAWS MAY APPLY:

If MHS receives payment related to communications that fall within one of the exceptions to the HIPAA definition of marketing, the communication is not magically transformed into “marketing.” However, anti-kickback, fraud, abuse, and self-referral statutes and regulations may restrict such communications.

D. AUTHORIZATION TO DISCLOSE PHI FOR MARKETING PURPOSES:

We must obtain a prior authorization for any use or disclosure of PHI that constitutes marketing under HIPAA.

- If marketing involves direct or indirect payment to a covered entity from a third party, the authorization must state such payment is involved.
- Authorizations must be specific about the kind(s) of marketing contemplated; a blanket authorization for such purposes is not valid.

Selling lists of patients with particular conditions to another entity requires an authorization, regardless of whether that third party has no relationship with the covered entity or enters a business associate agreement with the covered entity.

XXIII. FUNDRAISING:

HIPAA regulations offer no explicit definition of fundraising. The Department of Health and Human Services (DHHS) offers the following definition:

“Activity for the specific purposes of raising funds for the institution, rather than a general charitable purpose.”

If we wish to engage in fundraising activities of any kind we must inform patients that fundraising is planned and what patient information will / will not be used. Patients are informed of this by our Privacy Notice.

XXIII. FUNDRAISING (CONT'D):

A. USE OF PROTECTED HEALTH INFORMATION FOR FUNDRAISING:

For fundraising purposes, HIPAA permits us to use, or disclose to a business associate or institution-related foundation, only two types of protected health information (PHI) **without specific written permission from the patient:**

1. Basic demographic information relating to an patient excluding “any information about the illness or treatment, diagnosis, or nature of services.”

This information includes:

- Name
- Address
- Age
- Gender
- Insurance status

2. Dates of health care provided to an individual.

Use of any other kind of PHI for fundraising requires an individual “opt-in” via a specific authorization. These limitations apply to internal uses (solely within the covered entity) as well as external disclosures to business associates or institutionally related foundations.

Broad access to PHI is unnecessary for fundraising and unnecessarily intrudes on the privacy of the patient.

B. FUNDRAISING COMMUNICATION REQUIREMENTS:

All fundraising communications must include a description of how an individual may opt-out of receiving additional messages or materials.

- We must make reasonable efforts to ensure such opt-out requests are promptly honored.

XXIII. FUNDRAISING (CONT'D):

C. OPT-OUT VERSUS OPT-IN:

- An opt-in requires an action or affirmation by an individual to be included; the default is exclusion.
- An opt-out requires an action or affirmation to be excluded; the default is inclusion.

A standard authorization form for opting in and out will be available to Health System affiliates.

XXIV. COMPLAINTS:

All HIPAA violation complaints should be directed to the Privacy Officer. Individuals who believe we are not complying with HIPAA may also file a complaint with the Secretary of the United States Department of Health and Human Services (DHHS).

We may not require a patient to waive their rights to file a complaint as a condition of the provision of treatment, payment, and enrollment in a health plan or eligibility for benefits, nor may we intimidate or retaliate against complainants, be they patients / customers or members of our workforce.

XXV. CONSEQUENCES OF NONCOMPLIANCE:

In addition to our established discipline policy, HIPAA includes substantial civil and criminal penalties, ranging from \$100 per violation to \$250,000 and 10 years in prison.

XXVI. WHERE TO GO FOR QUESTIONS:

See all relevant policies, ask your supervisor for guidance, or contact your Privacy Officer.