

Impact Of HIPAA Privacy Rules From The Consumer Perspective

BY: MONICA B. WILKINSON
COOK, GOETZ, ROGERS & LUKEY, P.C.

I. WHAT THE CONSUMER SHOULD UNDERSTAND ABOUT THE HIPAA PRIVACY REGULATIONS?

A. What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, brought sweeping changes in the area of healthcare transactions, healthcare information, and the portability of health insurance policies. Title II of the Act contains a section known as Administrative Simplification which requires 1) standardized electronic data interchange and 2) protection of confidentiality and security of health data.

B. What Are The Three Main Areas of Administrative Simplification?

1. Transactions, Code Sets, and Identifiers (“TCI”)

Health providers and plans have used a variety of forms, codes, and electronic formats to process claims. The TCI standards will require virtually all health providers and plans to adopt common standards and code sets for processing transactions. In addition, there will be a single unique identifier for providers, employers, health plans, and patients. **Effective Date: October 16, 2002 unless extended to October 16, 2003 by application.**

2. Security of Health Information and Electronic Signature Standards

The security standard will provide a uniform level of protection for all individually identifiable health information that is housed or transmitted electronically. In addition, it will set standards for the use of electronic signatures with HIPAA transactions. **Final regulations are not yet published.**

3. Privacy and Confidentiality

The privacy standards govern who has the right to access protected health information (“PHI”), regardless of whether the information is in hard copy or electronic format. PHI is individually identifiable health information, including demographic information. The privacy

standards permit the non-consensual disclosure of information for treatment, payment, and healthcare operations. *Note: HIPAA law may be preempted by stricter state law so an analysis of both federal and state law is necessary to determine when consent is required and in what form.* Disclosure of health information for other purposes requires the authorization of the patient except in certain limited circumstances. Patients are given new rights to access and amend their medical records and to know who else has accessed their medical records. **Effective Date: April 14, 2003 (April 14, 2004 for small health plans.)**

C. Who is Affected?

All health care providers who transmit health information electronically, health plans, and all health care clearinghouses. There are some very limited exceptions for small health care providers. Covered entities may disclose health information to “business associates” who perform business functions on the covered entities’ behalf as long as the business associates are bound by contractual obligations to protect PHI.

D. What Are The Privacy Regulations?

1. Privacy refers to limiting the availability and use of patient confidential information. The privacy regulations are different from the TCI regulations, which are applicable only to electronics, because they govern privacy protection for PHI whether it is in a paper, electronic, or spoken form. The regulations were first proposed in 1999 and the Final Rule was published in 2000 just as Pres. Clinton was leaving office. There were over 11,000 comments to the Rule and significant changes were made before the Modified Final Rule was published on August 14, 2002.
2. In summary, the privacy regulations address:
 - i. notice of privacy practices;
 - ii. consents and authorizations;
 - iii. patients’ rights of access, amendment, and accounting;
 - iv. business associate agreements;
 - v. policies and procedures re PHI disclosures and patient rights;
 - vi. business procedural changes;
 - vii. education of personnel; and

viii. designating a privacy officer.

E. What Is The Impact of State Law Preemption?

The HIPAA privacy regulations preempt state law whenever they are “contrary to” state law, except for state laws that:

- i. HHS determines are necessary to prevent fraud and abuse, ensure appropriate regulation of insurance and health plans, for state reporting on health care delivery, and other purposes;
- ii. Relate to controlled substances;
- iii. Are “more stringent” than HIPAA;
- iv. Provide for reporting disease, injury, child abuse, birth, death, or for public health initiatives; or
- v. Relate to audits, program monitoring, or licensing and credentialing.

The exception pertaining to “more stringent” state law is the most troublesome because it will require the covered entity to perform a state law preemption analysis.

F. What Is The Minimum Necessary Standard?

Covered entities must make reasonable efforts to limit the use and disclosure of PHI to the minimum amount necessary to accomplish the intended purpose. There are exceptions to this general rule for:

- i. Disclosures to or requests by a health care provider for treatment;
- ii. Permissible uses or disclosures made to the individual;
- iii. Uses and disclosures made pursuant to an individual’s valid authorization;
- iv. Uses or disclosures required for compliance with HIPAA;
- v. Disclosures to HHS for investigation and enforcement of the privacy standards; and

- vi. Uses and disclosures for judicial and administrative proceedings or as required by law.

G. What Are The Enforcement Provisions?

1. Regulatory Enforcement

The Office of Civil Rights (“OCR”) of Health and Human Services (“HHS”) will enforce the HIPAA Privacy Standards. Anyone may file a complaint with OCR when the person has reason to believe there has been a violation. This option is not limited to the patient. OCR may also conduct compliance reviews. There are stringent penalties for covered entities that misuse PHI.

- i. Civil Penalties: \$100 per incident, up to \$25,000 per person per year, for each standard violated; and
- ii. Criminal Penalties:
 - Up to \$50,000 and one year in prison for knowingly and improperly obtaining or disclosing PHI
 - \$100,000 and five years in prison for obtaining PHI under false pretenses
 - Up to \$250,000 and ten years in prison for obtaining and disclosing PHI with the intent to sell it

2. Private Right of Action

The statute does not create a private right of action for individuals, but one may expect courts to look to the standards to determine whether an individual establishes a claim for a common law invasion of privacy, breach of contract, or violation of applicable consumer protection laws.

II. NEW RIGHTS FOR INDIVIDUALS WITH RESPECT TO THEIR HEALTH CARE INFORMATION.

A. Notice of Privacy Practices 45 CFR 164.520

1. An individual has the right to receive a notice of a covered entity's privacy practices which will explain how the covered entity will use and disclose the individual's PHI and state the individual's rights and the covered entity's legal duties with respect to PHI.
2. A group health plan that provides health benefits through an insurance contract with a health insurance issuer or HMO is not required to provide the Notice unless it receives more PHI than summary health information.
3. The Notice must also explain that individuals may file a complaint with the covered entity and with the HHS Secretary and give a brief explanation as to how to do so.
4. A covered entity must document compliance with the Notice requirement by retaining copies of the Notice issued, and if applicable, any written acknowledgement of receipt or documentation of good faith efforts to obtain such written acknowledgment.

B. Inspect and Copy 45 CFR 164.524

1. An individual has a right to inspect and obtain a copy of his/her protected health information in a designated record set, for as long as the protected health information is maintained subject to the exceptions described below.
2. A covered entity may deny an individual access without providing an opportunity for review, in the following circumstances:
 - i. Psychotherapy notes;
 - ii. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative proceeding;
 - iii. PHI maintained by a covered entity that is subject to the Clinical Laboratory Act exemptions;
 - iv. If the covered entity is a correctional institution and release of the PHI would jeopardize health, safety, or security;

- v. Access to information created or obtained in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress;
 - vi. For records that are subject to the Privacy Act, 5 U.S.C. Sec. 552a, access may be denied, if the denial of access would meet the requirements of that Act; and
 - vii. If the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
3. A covered entity may deny an individual access, provided that an individual is given a right to have such denial reviewed, in the following circumstances:
- i. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
 - ii. The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
 - iii. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
4. The review of a reviewable denial must be conducted by a licensed health care professional designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official.
5. If the covered entity denies access, in whole or in part, to PHI, the covered entity must:

- i. Give access to any other PHI requested after excluding the portion to which access is denied;
 - ii. Provide a timely, written denial in plain language that contains the basis for the denial, a statement of the individual's review rights (if applicable), and a description of the covered entity's complaint procedure; and
 - iii. If the covered entity does not maintain the PHI that is the subject of the request, but knows where the requested information is maintained, the covered entity must inform the individual where to direct the request.
6. The covered entity must act on a request generally within 30 days. The covered entity may have a single extension of 30 days.

C. Request Amendment or Correction 45 CFR 164.526

1. An individual has the right to have a covered entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.
2. A covered entity may deny the request to amend if it determines that the PHI:
 - i. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator is no longer available to act on the requested amendment;
 - ii. Is for information that is not part of the designated record set;
 - iii. Would not be available for inspection under the privacy regulations; or
 - iv. Is accurate and complete.
3. The privacy regulations have very technical requirements for accepting an amendment which includes making the amendment, informing the individual, and informing others.
4. The privacy regulations have very technical requirements for denying the amendment which includes a statement of the denial, the individual's right

to a statement of disagreement, and a rebuttal statement. There are also requirements for recordkeeping and future disclosures.

5. The covered entity must act on a request generally within 60 days. The covered entity may have a single extension of 30 days. If the covered entity needs the extension, it must notify the individual of the reason for the delay and the expected time of completion. Only one extension is permitted per request.

D. Request Confidential Communications 45 CFR 164.522(b)

1. Individuals have a right to restrict disclosures of information and related communications made by a covered entity to the individual, by allowing individuals to request that communications be made to the person at an alternative location or by alternate means.
2. A provider must accommodate any reasonable request for confidential communication and may not require an explanation of the reason for the request.
3. The provider may require that the request be put in writing and specify an alternative address or method of contact.
4. In the case of a health plan, the health plan may require that an individual state disclosure of confidential information could endanger the individual.

E. Request Restriction of Disclosures 45 CFR 164.522(a)

1. An individual can request that a covered entity restrict uses or disclosures of PHI to carry out treatment, payment, or healthcare operations and disclosures permitted under Sec. 164. 510(b).
2. A covered entity is **not** required to agree to a restriction.
3. If a covered entity agrees to a restriction, it must document the restriction and may not disclose in violation of the restriction except in case of emergency treatment.
4. Either party may terminate its agreement to a restriction.

F. Accounting for Disclosures 45 CFR 164.528

1. An individual has the right to request an accounting of all disclosures of his/her protected health information if a disclosure was for purposes other than treatment, payment, or health care operations.
2. An individual can request an accounting for a period of up to six years prior to the date of the request. An individual may request an accounting for a shorter period of time, i.e. six months.
3. The covered entity must respond within 60 days. If it cannot do so, it must notify the individual of the reason for the delay and the expected time of completion. Only one extension is permitted per request.
4. Disclosures made as follows are excluded from this tracking requirement:
 - i. Prior to the effective date of the rule;
 - ii. For treatment, payment, or health care operations;
 - iii. To law officials or correctional institutions;
 - iv. Pursuant to an authorization;
 - v. For facility directories;
 - vi. To the individual;
 - vii. For national security or intelligence purposes;
 - viii. To people involved in an individual's care; and
 - ix. For notification purposes related to location, general condition, or death.
5. An individual is allowed to request free of charge one accounting per 12 month time period. A reasonable fee can be charged for more frequent requests.

III. USES AND DISCLOSURES AND THE NEED FOR AUTHORIZATIONS

Use means the sharing, employing, application, utilization, or analysis of information within the organization. Disclosure means release, transfer, provision of access to, or divulging in any manner of information outside the organization. Covered entities must have

authorizations from individuals before using or disclosing PHI for any purpose not otherwise permitted or required by the Privacy Rule. Covered entities also must compare applicable state law with HIPAA to determine whether preemption dictates a different standard than the one set forth in the Privacy Rules.

A. Uses and Disclosures without Authorizations

1. Use and disclosure pertaining to treatment, payment, and healthcare operations. 45 CFR 164.506.

This is a significant change from earlier versions of the regulations which required consent for these purposes. The change though, will be elusive for states, like Michigan, which have laws that require consent in these circumstances because HIPAA is preempted by more stringent state laws.

2. Disclosures to the individual of his/her own PHI. 45 CFR 164.592(a)(1)(i).
3. Required disclosures to the Secretary for enforcement of the Rule.
4. 45 CFR 164.592(a)(2)(ii).
5. Permitted disclosures under 45 CFR 164.512 without authorization or opportunity for the individual to agree or object.

Each of these permitted uses or disclosures has particular elements to be satisfied before a use or disclosure is permitted. Therefore, the standard must be consulted before making a final determination as to whether use or disclosure without authorization or opportunity for the individual to agree or object is permitted;

- i. Uses and disclosures required by law;
- ii. Uses and disclosures for public health activities;
- iii. Uses and disclosures about victims of abuse, neglect, or domestic violence;
- iv. Uses and disclosures for health oversight activities;
- v. Disclosures for judicial and administrative proceedings;

- vi. Disclosures for law enforcement purposes;
 - vii. Uses and disclosures about decedents;
 - viii. Uses and disclosures for cadaveric organ, eye, or tissue donation purposes;
 - ix. Uses and disclosures for research purposes;
 - x. Uses and disclosures to avert a serious threat to health or safety;
 - xi. Uses and disclosures for specialized government functions; and
 - xii. Disclosures for workers' compensation.
6. Permitted disclosures under 45 CFR 164.510 without authorization but requiring an opportunity for the individual to agree or object.

Each of these permitted uses or disclosures has particular elements before a use or disclosure is permitted. Therefore, the standard must be consulted before making a final determination as to whether use or disclosure without authorization but requiring an opportunity for the individual to agree or object is permitted.

- i. Use and disclosure for facility directories; and
- ii. Use and disclosures for involvement in the individual's care and notification purposes;

B. Uses and Disclosures with Authorizations 45 CFR 164.508

- 1. The general rule requires an authorization from individuals before using or disclosing PHI for any purpose not otherwise permitted or required by the Privacy Rule.
- 2. There are even tighter restrictions for psychotherapy notes.
- 3. The following core elements are required in an authorization:
 - i. A description of the information to be used or disclosed;

- ii. The name of the covered entity authorized to use or disclose the PHI;
 - iii. The name of the recipient of the PHI;
 - iv. A description of each purpose of the requested use or disclosure;
 - v. An expiration date, time period, or event;
 - vi. A statement regarding the individual's right to revoke the authorization and describing how to revoke;
 - vii. A statement that the PHI may be subject to redisclosure by the recipient and may no longer be protected by HIPAA;
 - viii. The individual's signature and date of signature; and
 - ix. If signed by a representative, a description of the representative's authority to act for the individual and/or relationship to the individual.
- 4. There may be additional requirements for authorizations for certain kinds of disclosures i.e. authorizations for research (45 CFR 164.512(i)), marketing (45 CFR 164.508(a)(3)), and fundraising (45 CFR 164.514(f)(1)).
 - 5. There are additional requirements for authorizations concerning compound authorizations, prohibition on conditioning of treatment, payment, enrollment, or eligibility of benefits on provision of an authorization, revocation of authorizations, and document retention.

C. Other Requirements Relating to the Use and Disclosure of PHI

1. De-Identification of PHI

De-identified PHI is not subject to the Privacy Rules. 45 CFR 164.514.

2. Minimum Necessary 45 CFR 164.514(d)(1)

When using or disclosing PHI, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. A covered entity may rely, if

reasonable, on a requested disclosure as the minimum necessary for the stated purpose when making disclosures:

- i. For treatment;
 - ii. To the individual;
 - iii. To another covered entity;
 - iv. Pursuant to an authorization;
 - v. Required by law;
 - vi. To the Secretary;
 - vii. Uses or disclosures required for HIPAA compliance;
3. Deceased Individuals 45 CFR 164.502(f)

A covered entity must comply with the Privacy Rules with respect to the PHI of a deceased individual.

4. Personal Representatives 45 CFR 164.502(g)

A covered entity must treat a personal representative as the individual for purposes of the Privacy Rules. There are specific exceptions to this requirement for unemancipated minors and abuse, neglect, and endangerment situations.

IV. MYTHS AND URBAN LEGENDS

There were a number of horror stories circulating throughout the rulemaking process describing how HIPAA regulations would interfere with the delivery of healthcare. Some of these fears have been addressed in the rulemaking process and others in subsequent materials published by the HHS Office of Civil Rights.

A. Picking up Prescriptions.

A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient's best interests in allowing a person, other than the patient, to pick up a prescription. 45 CFR 164.510(b)(3)

Using Fax Machines to Share PHI.

The Privacy Rule permits health care providers to share PHI with other health care providers by fax machines. Health care providers must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. Frequently Asked Questions About the HIPAA Rule, October 2, 2002 ("FAQ").

B. Complete Medical Record.

The Privacy Rule permits a healthcare provider to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted under the Privacy Rule. FAQ.

C. Physician Sign In Sheets.

Physician offices may continue to use sign-in sheets and call out names in the waiting area so long as the information disclosed is appropriately limited. The Privacy Rule explicitly permits certain "incidental disclosures" that occur as a by-product of an otherwise permitted disclosure. Sec. 164.530(c). FAQ.

D. Paying for Copies.

The Privacy Rule permits covered entities to impose a reasonable, cost based fee. The fee may include only the cost of copying (supplies and labor) and postage, if mailed. The fee may not include costs associated with searching for and retrieving the requested information. FAQ.

E. Government Database.

The Privacy Rule does not create a government database with all individual's PHI or require covered entities to send medical information to the federal government for a government database or similar operation. FAQ.

Consumer Privacy Expectations for Protected Health Information Held by Employers and Insurers

BY: MICHAEL FRALEIGH
ASSISTANT ATTORNEY GENERAL
INSURANCE AND BANKING DIVISION

- I. What is Protected Health Information (PHI)?
 1. PHI is defined by 45 CFR 164.501 as Individually Identifiable Health information that is:
 - a. Transmitted in an electronic media;
 - b. Maintained in an electronic media; or
 - c. Maintained or transmitted in any other form or media.
 2. PHI does not include Individually Identifiable Health Information that is contained in:¹
 - a. Education records covered by the Family Education Rights and Privacy Act, that:²
 - i. Contain information directly related to a student; and
 - ii. Are maintained by an educational agency or institution or by a person acting for such agency or institution.
 - b. Records maintained by an educational institution that:³
 - i. Records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;

- ii. Records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement;
 - iii. In the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or
 - iv. Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.
- c. Employment records held by a Covered Entity
 - d. Information that is disclosed to the employer as part of the employment relationship.
3. Health Information is:⁴

“[A]ny information oral or recorded in any form or medium, that:

- (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past present or future payment of for the provision of health care to an individual.”

4. Individually Identifiable Health Information is defined as:⁵

“[I]nformation that is a subset of health information, including demographic information collected from an individual, and

(1) Is created or received by a health care provider, health plan, employer, or health care clearing house; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past present or future payment of for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

5. Individually Identifiable Health Information includes:⁶

a. Names.

b. All geographic subdivisions smaller than a State, including street address, city, county, zip code.

c. All elements of date except the year related to an individual e.g. birth date, admission date, treatment date, discharge date, date of death. If individual is over 89 years old it also includes the year of birth and any information indicative of the year or date of birth.

d. Telephone numbers.

e. Fax numbers.

f. E-mail addresses.

g. Social Security Numbers.

h. Medical record numbers.

i. Health Plan Beneficiary numbers.

- j. Account numbers.
- k. Certificate or license numbers.
- l. Vehicle identifiers and serial numbers, including license plate numbers.
- m. Medical device identifies and serial numbers.
- n. Web Universal Resource Locators (URALs).
- o. Internet Protocol (IP) address numbers.
- p. Biometric identifiers, including voice and fingerprints.
- q. Full-face photographs or comparable images.
- r. Any other unique identifying number, characteristic, or code.

II. Covered Entity

1. “Covered Entity” is a defined term under HIPAA. Covered Entities are limited to:⁷
 - a. Health Plans,
 - b. Health Care Clearing houses, and
 - c. Health care providers who transmits any health information in an electronic form in connection with a transaction covered by this subchapter [45 CFR 160, *et seq.*].”
2. Covered Entity does not include:⁸
 - a. Employers, including Covered Entities in their capacity as employers.
 - b. Insurers that provide coverage for:⁹
 - i. Automobile insurance, including health care benefits

- ii. Causality insurance
- iii. Credit –only insurance.
- iv. Critical illness fixed indemnity insurance.
- v. Disability insurance.
- vi. General liability insurance.
- vii. Life insurance.
- viii. Long term Care fixed indemnity or per diem insurance.
- ix. Medical liability insurance.
- x. Professional liability insurance.
- xi. Property insurance.
- xii. Reinsurance or stop loss insurance.
- xiii. Workers Compensation insurance.
- xiv. Other similar insurance that provides benefits for medical care secondarily or incidentally to other insurance benefits.

III. Disclosure and use of PHI by non-covered entities

- 1. PHI that is obtained by a non-covered entity is not subject to HIPAA’s protections or restrictions on disclosure.
- 2. State law and other federal law protections and restrictions on disclosure will still apply to both covered and non-covered entities.
- 3. A health plan may obtain and use PHI for” underwriting, premium rating, or other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits....” 45 CFR 164.514(g).

IV. Disclosure of PHI to non-covered entities

1. An individual may disclose whatever PHI to a non-covered entity he or she deems prudent.
2. Subject to other legal restrictions, a non-covered entity may require the disclosure of PHI as a condition of obtaining services.
3. A Covered Entity may disclose PHI to a non-covered entity:
 - a. To obtain Professional Liability Insurer (e.g. Medical Malpractice), reinsurance or stop loss insurance as part of the “business management and general administrative activities” allowed under the auspices of Health care operations.¹⁰
 - b. As authorized and to the extent required to comply with workers compensation and other similar programs, established by law, to provide benefits for work-related injuries or illnesses without regard to fault.¹¹
 - c. As allowed by state or federal law.

V. Disclosure of PHI to an Employer

1. A Covered Entity may disclose an in PHI to an employer of an individual, who is part of the employer’s work force, if:¹²
 - a. The Covered Entity is covered health care provider who is a member of the employer’s work force; or provides health care to the individual at the request of the employer to:
 - i. Conduct an evaluation relating to medical surveillance of the work force;
 - ii. Evaluate the individual has a work related illness or injury.
 - b. The PHI that is disclosed consists of findings concerning a work-related illness or injury or workplace-related medical surveillance;

- c. The employer needs such findings in order to comply with its obligations under Occupational Safety and Health Administration (OSHA)¹³ and Mine Safety and Health Administration¹⁴ regulations under state law having a similar purpose, to record such illness or injury, or to carry out responsibility for work place related medical surveillance;
 2. Required Notice the Individual
 - a. The health care provider must provide the individual with written notice that it will disclose PHI related to medical surveillance of the workplace, and work-related injuries and illnesses to the employer.¹⁵ The notice must be given to the individual at the time the health care is provided.
 - b. If the health care is provided at the work site of the employer, by posting the notice in a prominent place where the health care is provided.
 3. Scope of disclosure of PHI to an employer
 - a. The Covered Entity must make a reasonable effort to limit the disclosure of PHI to the minimum amount of information necessary to accomplish the intended use, disclosure or request.¹⁶ Note: The individual may place restrictions on the disclosure and use of PHI. If the entity agrees to the restrictions it cannot, except as provided in 45 CFR 164.522, disclose or use the PHI in violation of the agreed restrictions.
 - b. A Covered Entity cannot release the individual's entire medical record unless:
 - i. "The entire medical record is specifically is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request."¹⁷
 - ii. The disclosure is required by law.
 - iii. The individual authorizes the disclosure.
 4. Nothing in HIPAA prohibits an employer from making an individual's agreement to the disclosure of PHI to the employer a precondition to employment.¹⁸ If the employee agrees to allow the disclosure then the Covered Entity may disclose

PHI to the employer consistent with the terms and conditions of the authorization or release agreed to by the employer and employee.

5. Personal and health related information provided to an employer or obtained by an employer, as part of the employment relationship is not PHI.
6. Prohibitions on use of PHI obtained from a Covered Entity
 - a. Can not use PHI obtained from a Covered Entity for employment decisions such as, promotions or determining employee benefits.
 - b. Must keep the PHI separate from the employment records.

VI. Disclosure of PHI to an Employer that is a Health Plan Sponsor

1. The employer sponsoring the health plan may request the health plan to disclose summary health information in for purposes of:¹⁹
 - a. Obtaining premium bids for group health insurance coverage; or
 - b. Modifying, amending, or terminating the health plan.
2. The health plan, health insurer, or HMO can provide the employer information on whether an individual “is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance insurer or HMO offered by the plan.”²⁰
3. The health plan may disclose any PHI to the employer that the individual has authorized the health plan to disclose to the employer.

DISCLAIMER

The points of view and opinions stated in this article are those of the author and may not represent the official position of Jennifer M. Granholm, Attorney General of the State of Michigan.

Footnotes

1. 45 CFR 164.501.
2. 20 USC 1232g(a)(4)(A).
3. 20 USC 1232g(a)(4)(B).
4. 45 CFR 160.103.
5. 45 CFR 160.103.
6. See, 45 CFR 164.514(b)(2).
7. 45 CFR 160.103.
8. 42 USC 300gg-91(c)(1) and 45 CFR 160.104.
9. An insurer may be a hybrid entity that has both non-covered and Covered Entity functions. If so, the parts of the insurers business that meets the definition of a Covered Entity will be subject to HIPAA's restrictions on the use and disclosure of PHI. 45 CFR 164.504.
10. See, 45 CFR 164.506 and 45 CFR 502(a)(1)(ii).
11. 45 CFR 164.512.
12. 45 CFR 164.512.
13. 29 CFR 1904 – 1928.
14. 30 CFR Part 50 - Part 90.
15. 45 CFR 164.512 (b)(v)(D).
16. 45 CFR 164.502(b)(1).
17. 45 CFR 164.514 (c)(5).
18. Comments to the Final Rule 67 FR 53182, 53193 (August 14, 2002).
19. 45 CFR 164.504(f).

20. 45 CFR 164.504(f)(iii).

The effect of the HIPAA Privacy Rule on Court Proceedings/Civil Discovery in Michigan

By: Monica P. Navarro
Frank, Stefani, Haron & Hall

- I. HIPAA "Satisfactory Assurance" Standard (45 CFR 164.512(d)) (hereinafter all HIPAA citations are to 45 CFR Parts 160 and 165) is a one-size fits all approach
 1. Party-patient medical records
 2. Non-party patient medical records
 3. Mental health records
 4. Judicial and Administrative Proceedings

- II. HIPAA "Satisfactory Assurance" standard outlines HIPAA requirements for the release of PHI through the normal discovery process (discovery requests and subpoenas which are not accompanied by a court order). HIPAA "Satisfactory Assurance" standard can be met in the following three ways:
 1. The party seeking the release of PHI must provide to the custodian of PHI written evidence that he has made a "reasonable effort" to notify the patient.
"Reasonable effort" to notify a patient means:
 - a. The requester has made a "good faith" attempt to provide written notice to the patient.
 - b. The notice (attempted or actually given) included sufficient information about the litigation to enable the patient to appreciate the import of the PHI request.
 - c. The patient did not file timely objections to the PHI request.
 - d. The patient filed timely objections, but the objections were rejected by the court

 2. The party seeking the release of PHI must demonstrate to the custodian of PHI that a "reasonable effort" was made to obtain a qualified protective order (i.e., one which prohibits parties from using or disclosing PHI outside of litigation). To discharge this burden, the requester of PHI must provide a written statement to the custodian stating that:
 - a. The parties to the dispute have agreed to a qualified protective order and
 - b. The qualified protective order has been presented to the court OR
 - c. The requesting party has requested a qualified protective order from the Court.

2. The custodian of PHI makes a "reasonable effort" to provide notice to the patient or to obtain a qualified protective order from the Court in the fashion outlined in II.1 and 2 above.

III. HIPAA "Satisfactory Assurance" Standard does not preempt the majority of discovery procedures set forth by Michigan law.

1. HIPAA provides a "floor" of protections, which are preempted by Amore stringent@ State Law.
 - a. If State law provides more patient access to medical records than does HIPAA, State law applies.
 - b. If State law gives patients more control over the exchange of PHI than does HIPAA, State law applies.
 - c. Where the State law and HIPAA are not contrary to each other, both apply. For example:
 - i. Michigan law provides that chemical breath analysis tests are admissible in court proceedings. MCL 257.625a
 - ii. HIPAA provides that PHI can be disclosed without an authorization where it is required by law for law enforcement purposes. 164.512(a)(2) and 164.512(f).
 - iii. State law and HIPAA are not contrary to each other, so both apply.
2. HIPAA does not apply to all entities simply because they are the custodian of PHI:
 - a. Health plans, clearinghouses, covered providers, and their business associates are HIPAA covered entities.
 - b. Certain entities who are custodians of PHI (such as employers and state Agencies acting in their role of repositories) are not governed by HIPAA.
 - c. Whether or not a custodian of PHI is a covered entity can become relevant for discovery purposes in those situations in which HIPAA preempts state law.

IV. Michigan law and HIPAA generally share the basic principle that, absent applicable waivers and other exceptions carved for law enforcement purposes and other state interests, all PHI obtained by health professionals in connection with providing health related services is confidential.

1. MCL 600.2157: physician/patient privilege
2. MCL 330.1748: mental health records privileged
3. MCL 333.16645: dentist/patient privilege
4. Other state privileges: marriage counselor, physician assistant, social worker, etc.

V. Discovery Rules pertaining to party-patients= PHI not involving mental health records.

1. Michigan law
 - a. MCR 2.310 (D) requires the party-patient whose PHI is being sought to receive actual notice.
 - b. MCR 2.314 requires the party-patient to actually waive privilege over the PHI being sought before it can be discovered.
 - i. A party-patient who has put the PHI in controversy is deemed to have waived privilege over said PHI.
 - ii. A party-patient who has failed to file timely objections after actual notice is deemed to have waived privilege over said PHI.
2. HIPAA is preempted by Michigan law
HIPAA "Satisfactory Assurance" standard is less stringent than Michigan law because it does not require actual notice and waiver by the party-patient. Michigan law will continue to govern party-patient PHI not involving mental health records.

VI. Discovery Rules pertaining to non-party-patient PHI not involving mental health records

1. Michigan law
 - a. Baker v Oakwood Hospital Corp, 608 NW2d 823 (2000) requires non-party patients to waive privilege before their PHI is released. Not enough to de-identify.
2. HIPAA is preempted by Michigan law
 - a. In contrast, HIPAA "Satisfactory Assurance" standard allows the release of PHI without requiring an actual waiver
 - b. HIPAA provides that de-identified PHI is outside the protection of the Privacy Rule. Part 164.514(a)-(c).
 - c. Michigan law will continue to govern non-party patient PHI not involving mental health records.

VII. Discovery Rules pertaining to party-patients= PHI involving mental health records

1. Michigan law
 - a. MCL 330.1750 provides that mental health records are inadmissible in court proceedings without an actual waiver, except a waiver will be implied in the following situations:
 - i. When relevant to the physical or mental condition of the patient which the patient has introduced into a case or proceeding as a claim or defense.
 - ii. When relevant to a matter under consideration in a proceeding provided that the patient was "informed" that any communications made could be used in such proceedings.

- iii. When relevant to determine the legal competence of the patient, provided the patient was "informed" that any communications made could be used in such proceedings.
 - iv. In a civil action by the patient or a criminal action arising from the treatment of the patient against the mental health professional for malpractice.
 - v. If the communication was made during an examination ordered by the court prior to which the patient was "informed" that the communication would not be privileged.
 - vi. If the communication was made during a competency evaluation.
- b. Michigan law, therefore, allows the release of mental health records in situations in which the patient was "informed" of the possibility, even if that patient did not provide an actual waiver of the privilege, because the waiver is deemed implied.¹

2. HIPAA

- a. Under the HIPAA Privacy Rule, "informing" the patient is not sufficient to justify disclosure or to imply a waiver. Instead, the requester of such information has to obtain either an Order from the Court mandating disclosure or has to meet HIPAA "Satisfactory Assurance" standard, which provides more protections than State law in this regard.
- b. The HIPAA Privacy Rule gives psychotherapy notes special treatment from other mental health records.
 - i. They may not be released without patient Authorization in the context of litigation,
 - ii. Unless it is for the purpose of the covered entity defending a legal action brought by the patient. 164.508(2)(C)
- d. HIPAA is more stringent than state law and must be followed.

VIII. Discovery Rules applicable to Arbitration Proceedings

- 1. Michigan law:
 - a. MCL 600.2912g:

¹However, records which are held by the Michigan Department of Community Health must be deidentified before they are disclosed, regardless of whether disclosure is permitted or authorized (See MCL 333.2637).

Med mal actions in which the amount is \$75,000 or less can be submitted to binding arbitration, in which case the statute provides that the parties shall exchange all authorizations necessary to obtain medical records.

- b. State law does not define what constitutes a sufficient "authorization."

2. HIPAA

- a. Does not speak directly to arbitration proceedings
- b. It is not clear whether an arbitration proceeding is a judicial or administrative proceeding which falls under the rubric of 164.512(d).
- c. Even if arbitration proceedings fall under 164.512(d) (the "Satisfactory Assurance" standard), Michigan law is more stringent because it requires the exchange of an Authorization for the release of PHI.
- d. Unlike State law, HIPAA defines the form and substance of what constitutes an "Authorization." 164.508(b).
- e. While the State law will control as to the procedure for releasing PHI in arbitration proceedings, HIPAA will govern the form of the authorization.

SUMMARY

When seeking to discover PHI for civil litigation in Michigan, practitioners will need to adhere to and keep in mind the following:

1. If seeking to obtain mental health records without a court order, practitioners will need to provide the custodian of the PHI with written evidence that the HIPAA "Satisfactory Assurance" standard has been met. To obtain psychotherapy notes, a HIPAA Authorization must be obtained.
2. If seeking to obtain PHI not pertaining to mental health records, practitioners will need to follow current State law procedures.
3. If seeking to obtain PHI in the context of any other dispute resolution procedure, practitioners will need to obtain HIPAA Authorizations for the exchange of PHI.
4. Practitioners should always check the substantive HIPAA and State law affecting the particular type of PHI being sought (such as relating to HIV status, abortion, etc.) to understand any special rules above and beyond the general framework described herein, as well as exceptions to these rules.
5. Understand that not all custodians of PHI are entities covered by HIPAA (i.e., law enforcement agencies, state repositories, etc. are not covered entities even though they hold substantial amounts of PHI). As a practical matter, however, because State law procedures continue to govern the great majority of discovery of PHI in Michigan (with the exception of mental health records), it probably does not pay to engage in a cumbersome analysis of the type of entity in question. Instead, it

would be easier to treat all custodians of PHI as covered entities for the purpose of discovery. However, in some isolated situations, access to PHI may depend on whether or not the custodian is governed by HIPAA, so practitioners should be sensitive to this fact.

STATE OF MICHIGAN
IN THE OAKLAND COUNTY CIRCUIT COURT

JOHN DOE

Plaintiff,

v

JANE DOE

Defendant.

Case No.
Hon.

AUTHORIZATION TO DISCLOSE PATIENT HEALTH INFORMATION

1. I, _____, authorize the use of disclosure of the following individual=s (the APatient@) health information as described below

Patient Name: _____ Health Record Number _____

Date of Birth: _____ Social Security Number _____

2. The following organization, individual or department of the organization (the ACustodian@) is authorized to make the disclosure:

Name _____

Address _____

Telephone No. _____

3. The type and amount of information to be used or disclosed is as follows:

_____ problem list
_____ medication list
_____ list of allergies
_____ immunization record
_____ most recent history and physical
_____ most recent discharge summary
_____ laboratory results from (date) _____ to (date) _____

_____ x-ray and imaging reports from (date)_____ to (date)_____
_____ consultation reports from (doctor=s name)_____
_____ entire record
_____ other_____

4. I understand that the information in the Patient=s health record may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV). It may also include information about behavioral or mental services and treatment for alcohol and drug abuse.

5. This information may be disclosed to the following individual or organization,
_____,
to be used in connection with the instant case for all purposes allowed under the Michigan Court Rules and the Michigan Rules of Evidence.

6. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization I must do so in writing and present my written revocation to the health informational management department of the Custodian listed above. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that this revocation will not apply to the Patient=s insurance company when the law provides the Patient=s insurer with the right to contest a claim under the Patient=s policy. Unless otherwise revoked, this authorization will expire on the following date, event, or condition:

If I fail to specify an expiration date, event, or condition, this authorization will expire in six months.

7. I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this authorization. I understand that I may inspect or copy the information to be used or disclosed, as provided in 45 CFR 164.524. I understand that any disclosure of information carries with the potential for an unauthorized redisclosure and the information may not be protected by federal confidentiality rules. If I have questions about disclosure of my health information, I can contact (insert HIM director, privacy officer, or other office or individual=s name or contact information).

Signature of Patient or Legal Representative

Date

If Signed by Legal Representative, Relationship to Patient

PRIVACY RESOURCES ON THE INTERNET

Privacy Standards: The HHS Office for Civil Rights is responsible for implementing and enforcing the privacy regulations. The following can be located at www.hhs.gov/ocr/hipaa

Frequently Asked Questions About the HIPAA Privacy Rule, (October 8, 2002)

Standards for Privacy of Individually Identifiable Health Information (Unofficial Version) 45 CFR Parts 160 and 164 (August 14, 2002)

Final Modifications to the Privacy Rule, 67 FR No. 157, pp 53181-53273 (August 14, 2002)

Sample Business Associate Contract Provisions, 67 FR No. 157, p 53182, 53264 (August 14, 2002)

Proposed Rule, Standards for Privacy of Individually Identifiable Health Information, 67 FR No. 59, pp14776-14815 (March 27, 2002)

HHS Guidance on Final Privacy Rule, July 6, 2001

Final Rule, Standards for Privacy of Individually Identifiable Health Information, 65 FR No. 250, p 82462-82829 (December 28, 2000)

Delegation of Authority to the Office for Civil Rights, 65 FR No. 250, p 82381 (December 28, 2000)

Proposed Rule, Standards for Privacy of Individually Identifiable Health Information, 64 FR No. 212, p 59918-60065 (November 3, 1999)

Michigan Preemption Analysis

HIPAA Privacy Rule Preemption Analysis Matrix for Michigan Law, Michigan State Bar Health Care Law Section and Michigan Michigan Society of Health Care Attorneys, April 2002 (Revised version expected very soon).

Other Interesting HIPAA Sites

WEDI (Workgroup for Electronic Data Interchange)
SNIP (Strategic National Implementation Process)
Security and Privacy White Papers –
<http://snip.wedi.org/public/articles/index.cfm?Cat=17>

Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University – <http://www.healthprivacy.org>

HIPAAAdvisory, Phoenix Health Systems – <http://www.hipaadvisory.com>

HIPAAcomply, Beacon Partners - <http://www.hipaacomply.com/index.htm>

W:\C\CGR&L\HIPAA Material\Privacy Resources on Internet.doc