THE LEGAL AID SOCIETY

Health Law Unit
199 Water Street
New York, NY 10038
T (212) 577-3300
www.legal-aid.org

THE HIPAA PRIVACY RULE[1]

What is the HIPAA Privacy Rule?

The HIPAA[2] Privacy Rule is found in federal regulations that detail the rights of patients and the obligations of health care providers and health insurance plans to safeguard the privacy of **Protected Health Information (PHI)**. The regulations describe how to get copies of medical records and a patient's right to limit access to PHI by third parties. The Privacy Rule is intended to both protect patients' health information and ensure the flow of medical information.

The American Recovery and Reinvestment Act of 2009 ("ARRA," commonly known as "the stimulus package"), enacted on February 17, 2009, also includes some provisions that affect HIPAA. These changes have not yet been interpreted by courts or implementing agencies, but they will be briefly discussed throughout this memo as well.

What is Protected Health Information?

Protected Health Information (PHI) is all, "individually identifiable health information." This includes information related to:

- the patient's physical or mental health status
- the provision of health care to the patient, or
- the payment for health care

AND information that can be used to identify a patient, like her name, address, birth date, Social Security Number and so on. 45 C.F.R. §160.103.

---

[1] Legal Aid Society Health Law Unit, May 2004; Updated August 2009

[2] HIPAA stands for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191. In addition to safeguarding patients' privacy rights, HIPAA provides rights and protections for participants and beneficiaries in group health plans who change employment or otherwise seek a change in coverage. Such protections limit exclusions for preexisting conditions, prohibit discrimination against employees and dependents based on their health status, and allow a special opportunity to enroll in a new plan to individuals in certain circumstances. HIPAA may also give you the right to purchase individual coverage if you have no group health plan coverage available and have exhausted COBRA or other continuation coverage.

PHI is not limited to information regarding doctors' treatments. It can also include information collected by non-medical personnel such as social workers. *See Gratton v. United Parcel Service, Inc.*, 2008 WL 4934056 (E.D.N.Y. 2008).

PHI does NOT include information that has been "de-identified" such as a statistical report or general, non-specific information. 45 C.F.R. § 164.502(d)(2) and 45 C.F.R. § 164.514.

Who is required to safeguard protected health information?

The Privacy Rule applies to all **covered entities**. 45 C.F.R. §160.102. Covered entities are **health plans, health care clearinghouses,** and any **health care provider** who transmits health information in electronic form for certain transactions. 45 C.F.R. §160.103.

> **Health Plans** include health, vision, dental, HMO, Medicaid, Medicare, and Long-Term Disability Insurers. A group health plan with less than 50 participants, administered only by the employer who established and maintains the program, is NOT covered by the HIPAA Privacy Rule. 45 C.F.R. §160.103.
>
> **Health Care Providers** include every health care provider who electronically transmits health information in certain transactions (like inquiries, referrals, and other requests). The provider is covered even if a third party such as a billing service transmits the information on the provider's behalf. 45 C.F.R. §160.103.
>
> **Health Care Clearinghouses** include entities that process information that is received from another entity, or vice versa. Examples of health care clearinghouses are billing services, repricing companies, and community health management information systems. 45 C.F.R. §160.103.

The HIPAA privacy Rule does not apply to government-funded programs whose principal purpose or activity is unrelated to the provision of health care. 45 C.F.R. §160.103.

Often a covered entity will contract another entity to perform certain functions involving the use or disclosure of PHI (like claims processing, billing, or utilization review). The HIPAA Privacy Rule refers to these entities as **business associates**. 45 C.F.R. §160.103. Under the original HIPAA Privacy Rule, a covered entity could share PHI with a business associate, however, the covered entity was responsible for making sure that the business associate also safeguarded PHI as provided in the contract between the two entities. 45 C.F.R. § 164.502(e).

The ARRA changes this framework in some respects. The definition of business associates is now expanded to include other services that handle PHI. ARRA § 13408. Business associates are also directly responsible for compliance with certain elements of HIPAA, including the implementation of physical, technical, and administrative safeguards for PHI, and can be directly investigated and penalized for violations. ARRA §§ 13401, 13404.

HIPAA only applies to the entities discussed above. Other entities which may hold health information, such as law firms, courts, or community organizations, are not covered by HIPAA's privacy rule, though other privilege or confidentiality laws may apply. *See, e.g., Coy v. Washington County Hosp. Dist.,* 866 N.E.2d. 651, 655-56 (Ill. App. Ct 2007) (health information not protected by HIPAA once in court record).

Who can access a patient's PHI?

A covered entity **must** provide PHI to a patient (or her **personal representatives**) upon request. A patient also has the right to know to whom her PHI has been disclosed. The HIPAA Privacy Rule guarantees a patient's right to inspect, obtain a copy and amend her own medical records. Under the regulations, a patient is entitled to receive copies of her medical records within 30 days of her request. In New York State, a provider must permit access within 10 days of the request. N.Y. Pub. Health L. § 18(2)(a)(d)(e), N.Y. Mental Hyg. Law § 33.16(b)(1). Providers are allowed to charge up to 75 cents per page for copies of medical records, however, the release of records cannot be denied for inability to pay. N.Y. Pub. Health L. § 18(2)(e); N.Y. Mental Hyg. Law § 33.16(b)(6).

A covered entity must treat a patient's personal representative in the same manner as the patient with regard to uses and disclosures of the patient's PHI. A personal representative is a person legally authorized to make health care decisions on behalf of the patient. 45 C.F.R. § 164.502(g). The covered entity does not have to disclose information if it determines that the personal representative may be abusing or endangering the patient. 45 C.F.R. § 164.502(g)(5); *see also In re Berg*, 886 A.2d. 980 (N.H. 2005).

The Privacy Rule also applies to the PHI of a deceased individual. 45 C.F.R. § 164.502(f). The covered entity must treat an executor, administrator, or another person with the authority to act on the behalf of the deceased individual or the deceased's estate as a personal representative. 45 C.F.R. § 164.502(g)(4).

In most cases, a patient's guardian has the right to access the patient's medical records. Pub. Health L. § 18. Health care agents are also entitled to access most health information. Pub. Health L. §2980; *see also Mougiannis v. North Shore-Long Island Jewish Health System*, 806 N.Y.S.2d. 623 (N.Y. App. Div. 2005). In New York State, however, a provider may, after considering the circumstances, deny a parent's request for medical records if the child is over 12

years of age and the child objects to the disclosure.[3] N.Y Pub. Health L. § 18(3)(c); N.Y. Mental Hyg. Law § 33.16(c)(2). In New York State, a child under 21 years of age has the right to obtain certain services without the consent of a parent (like treatment and screening for sexually transmitted disease). Under New York State Law, medical records of treatment for venereal disease or for abortion are not to be released or disclosed to the parent of a minor who has obtained these services. N.Y. Pub. Health L. § 17.

THE HIPAA Privacy Rule requires a **health care provider** to allow a patient to request that the covered entity communicate with her by alternate means or at alternate locations. 45 C.F.R. § 164.522(b)(1)(i). For example: an adolescent wants to receive pregnancy test results at an alternate phone number or by mail at an alternate address. A **health plan** must also allow a patient to request alternate communication if the patient indicates that the information could endanger her. 45 C.F.R. § 164.522(b)(1)(ii). The covered entities must accommodate reasonable requests.

The ARRA also requires covered entities that maintain electronic health records to provide them to patients in electronic format if requested, for a fee no greater than the entities' labor costs in producing the copy. ARRA § 13405(e).

Can a covered entity deny a patient her own medical records?

Under certain circumstances, a covered entity can deny a patient access to her PHI (like psychotherapy notes, legal documents, and some research information). 45 C.F.R. § 164.524(a)(1). New York State law also allows a medical provider to deny access to certain records when reviewing them would be likely to cause serious harm. N.Y. Pub. Health Law § 18(3); N.Y. Mental Hyg. Law § 33.16(c). If access is denied for this reason, then the person requesting the information must be informed why it is being denied, and the patient has a right for this decision to be reviewed by the appropriate medical records access review committee free of charge.[4] Within ten days of a request for such a review, the provider who wishes to restrict access must forward the relevant records to the chairman of the committee, who must make a written determination after allowing

---

[3] The Privacy Rule does not alter state laws that provide individuals with greater rights to control their PHI. 45 C.F.R. § 160.202. New York State Department of Health describes situations when state law preempts the Privacy Rule. *See* NYSDOH HIPAA Preemption Charts, at www.health.state.ny.us/nysdoh/hipaa/hipaa_preemption_charts.htm (last updated Oct. 2002). Courts have ruled, though, that HIPAA's standards always apply to *de*-identified information even where state rules would have been more restrictive. *See Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923, 926 (7th Cir. 2004); *In re Zypexra Products Liability Litigation*, 254 F.R.D. 50 (E.D.N.Y. 2008).

[4] These committees are appointed by the New York State Commissioner of Health from candidate lists submitted by provider associations. N.Y. Pub. Health Law 18(4). For more information on this procedure, and for forms to request such a review, see http://www.health.state.ny.us/professionals/patients/patient_rights/docs/you_and_your_health_records.htm and http://www.health.state.ny.us/forms/doh-1989.pdf

both parties reasonable opportunity to be heard. If the committee decides that access to the records should still be denied, it must inform the requesting party that the decision may be reviewed in court. N.Y. Pub. Health Law § 18(3)(e)-(f); N.Y. Mental Hyg. Law § 33.16(c)(4)-(5); *see also Davis v. Henderson*, 549 N.Y.S.2d 241 (N.Y. App. Div. 1989) (finding denial of access case not yet ripe for judicial review before internal review procedures carried out).

When can a covered entity release PHI without a patient's authorization?

A covered entity can use and disclose PHI without a patient's authorization in the following situations:

- When the disclosure is to the patient
- For treatment, payment, or other health care operations
- When a patient has given informal permission for protected health information to be disclosed through an opportunity to agree or object
- When an incidental disclosure is made as a result of a permitted disclosure
- Certain identified "national priority purposes," including public health activities, law enforcement activities, research, and "essential government functions"
- When the information is a "limited data set" from which certain identifiers of the patient have been removed
- When required by court order under certain limited circumstances (see below)
- In "whistleblower" cases, where a disclosure to an attorney or law enforcement official uncovers unlawful activity. 45 C.F.R. § 164.502(j).

The Privacy Rules require covered entities to try to limit the use and disclosure of PHI. 45 C.F.R. § 164.502(b). This "minimum necessary" standard does not apply in all cases; for example, a covered entity should not limit disclosure to a provider for treatment purposes, to the patient, or pursuant to a written authorization. 45 C.F.R. § 164.502(b)(2). The ARRA requires the Secretary of Health and Human Services to issue guidance on this "minimum necessary" standard within eighteen months of the Act's passage (i.e. before August 18, 2010). ARRA § 13405(b).

A patient can ask to further restrict the use of her PHI. 45 C.F.R. §164.522. For example, a patient can ask that her PHI not be disclosed to a certain doctor. The covered entity can, but is not required to, honor such requests. If the covered entity agrees to the restriction, it must comply with the restriction. 45 C.F.R. § 164.502. Under the ARRA, the covered entity must honor a patient's request not to release information to a health plan for payment purposes if the patient pays out of pocket for the relevant services. ARRA § 13405(a).

The ARRA requires covered entities and business associates to notify patients, and in some cases the public, in case of certain breaches where unauthorized persons gained access to PHI. ARRA § 13407.

What is a HIPAA release or authorization?

This is a form which allows the patient to control access to her PHI. The HIPAA Privacy Rule says that a covered entity cannot use or disclose PHI except as defined in the Privacy Rule **or** as the patient authorizes in writing. Because the law is designed to protect the privacy of health information, the regulations are very specific about the format of the authorization for a third party to receive PHI. 45 C.F.R. §164.508. If a patient wishes to allow psychotherapy notes to be disclosed to a third party, a separate authorization should be completed, although courts have sometimes interpreted general releases to also cover psychotherapy notes if the patient's intent is clear. 45 C.F.R. §164.508(b)(3); *see also Kalinoski v. Evans*, 377 F.Supp.2d. 136 (D.D.C. 2005).

A HIPAA compliant authorization must contain the following elements:

- A specific description of the information to be used or disclosed For example, any records related to a particular treatment period or provider
- The name of the person(s) or organization who will be authorized to release the information
- The name of the person(s) or organization to whom the information is authorized to be released
- A description of the purpose of the use or disclosure **OR** the statement, "at the request of the individual"
- A date or event of expiration
- The signature of the individual/ patient and date (If signed by a personal representative, the authorization should include a description of the person's relationship to the patient)

The authorization must also give notice to the patient of the following:

- A patient's right to revoke authorization
- The potential for redisclosure by the person who receives the information

A patient can revoke such an authorization in writing at any time, however, authorization cannot be revoked for information that has already been released in compliance with the law. 45 C.F.R. §164.508(b)(5); *see also Koch v. Cox*, 489 F.3d 376 (D.C. Cir. 2007).

Does a patient have to sign a HIPAA release?

In most cases, a covered entity cannot deny treatment, payment, enrollment, or eligibility if a patient refuses to authorize the disclosure of her PHI beyond the disclosures permitted by the HIPAA Privacy Rule. 45 C.F.R. § 164.508(b)(4). A covered entity can not retaliate against a patient for exercising rights provided by the Privacy Rule.

Can friends or relatives access a patient's information without written authorization?

If a patient is incapacitated or in an emergency, covered entities can generally disclose PHI if the disclosure, in their professional opinion, is in the best interests of the patient. 45 C.F.R. § 164.510. Friends or relatives may be able to obtain information about a patient's whereabouts or health status from a hospital directory. The Privacy Rule, however allows a patient to opt-out of such a directory or to limit the hospital from sharing PHI with friends or relatives. 45 C.F.R. § 164.510.

A covered entity may rely on a patient's informal permission (not in writing) to disclose to relatives, friends, or other persons, PHI that is directly relevant to that person's involvement in care or payment for care. For example, a pharmacist could dispense a patient's medications to a relative of the patient with informal permission.

Are authorizations required to obtain medical records in judicial and/or administrative proceedings?

Although PHI can be obtained without authorization in certain circumstances under HIPAA[5], New York's civil practice rules, which would apply for state law claims, are more restrictive. Medical providers are only required to comply with subpoenas for medical records if they are accompanied by a written authorization from the patient. In addition the subpoena must state in conspicuous bold-faced type that the records shall not be provided unless the subpoena is accompanied by a written authorization from the patient. If an authorization does not accompany

[5] Under HIPAA, covered entities are allowed to disclose PHI if they are ordered to do so by a court or administrative tribunal. 45 C.F.R. § 164.512(e)(1)(i). PHI can also be released pursuant to subpoena or other discovery request not accompanied by court or tribunal order if the party seeking the PHI provides proof that it has made reasonable efforts to ensure that notice was given to the individual who is the subject of the PHI sought, that the notice contained sufficient information about the litigation or proceeding so that the individual could object to the court or tribunal, that the time to object has elapsed, and that no objections were filed. 45 C.F.R. § 164.512(e)(1)(ii - iii). For lawsuits under federal law, such as federal employment discrimination, ERISA, Medicare and Medicaid fraud, or social security disability cases, New York's more stringent rules may be trumped by the less stringent rules of HIPAA and the Federal Rules of Evidence. *See Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923, 925 (7th Cir. 2004).

the subpoena the provider is not required to respond. CPLR § 3122. Once health information is entered into a judicial record, it is no longer protected by HIPAA because courts are not covered entities, though other confidentiality or privilege rules may apply. *See, e.g., Coy v. Washington County Hosp. Dist.,* 866 N.E.2d. 651, 655-56 (Ill. App. Ct 2007).

Does a covered entity have to give notice of their privacy practices?

Yes. A covered entity must provide a patient with notice of its privacy policies including the right to complain to Health and Human Services' Office of Civil Rights if the patient believes her privacy rights were violated. Such notice does not apply in emergency situations until the emergency is over. 45 C.F.R § 164.520

The covered entity is also supposed to get written acknowledgment that the consumer has received a privacy policy notice. 45 C.F.R § 164.520(c)(2)(ii). Many providers are asking that patients sign a letter acknowledging that they have received notice of the provider's privacy policy.

What can a patient do if she feels that her PHI was disclosed improperly?

A patient can file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). In most cases, a patient must file an OCR complaint in writing within 180 days of when she knew of or should have known of the inappropriate use or disclosure. 45 C.F.R. § 160.306(b)(3). Covered entities who violate the HIPAA Privacy Rule may face civil money penalties. A patient cannot sue for damages under the HIPAA Privacy Rule. Complaints about violations in New York State should be addressed to the following regional office.

Region II - NJ, NY, PR, VI
Office for Civil Rights
U.S. Department of Health & Human Services
26 Federal Plaza - Suite 3312
New York, NY 10278
(212) 264-3313; (212) 264-2355 (TDD)
(212) 264-3039 FAX

The standard OCR complaint form can be found at:
- http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintpackage.pdf

A covered entity may not retaliate in any way against any individual exercising their rights created by HIPAA, including filing a complaint. 45 C.F.R. §§ 160.316, 164.530(g).

A patient may also try to resolve the problem with the health plan or health care provider's designated privacy officer.

If OCR pursues the case, the original HIPAA Enforcement Rule allowed it to impose fines of up to $100 per violation, limited to $25,000 per calendar year for the same type of violation. 45 C.F.R. § 160.404. This penalty is not exclusive, so it does not replace other penalties or damage awards that may be required by other laws. 45 C.F.R. § 160.404. The entity accused of a violation may challenge any fine and has the right to appear before an Administrative Law Judge for an impartial hearing at which it may present evidence, conduct discovery, call witnesses, etc. 45 C.F.R. §§ 160.504, 160.506.

The ARRA now includes a tiered penalty structure, where uncorrected violations due to willful negligence can be penalized at up to $50,000 per violation, not to exceed $1,500,000. ARRA § 13410. The ARRA also makes it clear that HIPAA criminal penalty provisions apply to individual employees, as opposed to just entities. ARRA § 13409, *see also* 42 U.S.C. § 1320d-6(a) (2006). The ARRA also now allows state attorneys general to police and enforce HIPAA. ARRA § 13410(e).

How has the HIPAA Privacy Rule been enforced so far?

Since the establishment of the Privacy Rule in 2003, OCR has received almost 45,000 complaints. It has completed full investigations in about 13,000 of those cases, finding violations in almost 9,000 of them. Of the 32,000 cases where investigations have not been completed, about 25,000 of them were closed as being ineligible for enforcement because the complaint was not timely or did not describe any potential violation.

The OCR HIPAA enforcement website reports on types of enforcement activity. For example, the site tells of a case where a patient complained when a hospital left a detailed answering machine message about her condition and treatment which her daughter eventually listened to. In response, OCR required the hospital to develop and implement new policies on leaving "minimally necessary" information in these types of messages, and to train all staff on these procedures. Another patient's provider refused to release his records to him until OCR contacted them, then tried to charge him $100 for the copies. OCR required the provider to refund this money.
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case14.

How can an advocate get a health plan or a provider to disclose PHI even without a HIPAA release?

There are several approaches that an advocate can try:

- The advocate can set up a three way call with the patient and the covered entity (i.e. Medicaid, the client's doctor, etc.). The client can give oral permission to have the plan or provider give you the PHI you need. The patient can also request the PHI on her own and give it to the advocate.
- The advocate can talk to a health plan or provider about non-specific information. For example: How can I help a patient get a managed care exemption; What can I do if a patient's application was processed incorrectly.
- The advocate may negotiate with a plan or a provider for the patient without asking for any further disclosure of PHI.

Web Resources

U.S. Department of Health and Human Services, Office for Civil Rights
http://www.hhs.gov/ocr/hipaa/

New York State Department of Health
http://www.health.state.ny.us/nysdoh/hipaa/hipaa.htm

http://www.health.state.ny.us/professionals/patients/patient_rights/docs/you_and_your_health_records.htm

Health Privacy Project
http://www.healthprivacy.org/

Health Assistance Partnership
http://www.hapnetwork.org/medicare/HIPAA_Resource_Center.html