



STATE OF NEW YORK DEPARTMENT OF HEALTH

Corning Tower

The Governor Nelson A. Rockefeller Empire State Plaza

Albany, New York 12237

Antonia C. Novello, M.D., M.P.H., Dr.P.H.
Commissioner

Dennis P. Whalen
Executive Deputy Commissioner

October 15, 2002

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") gave the federal Department of Health and Human Services ("HHS") the authority to promulgate regulations containing standards with respect to the privacy of individually identifiable health information. HIPAA provided that such standards shall not supersede State law that imposes more stringent standards (P.L. 104-191, § 264(c)). HHS promulgated the federal standards, and they are now in Parts 160 and 164 of Title 45 of the Code of Federal Regulations (the "Privacy Rule").

Under the Supremacy Clause of the U.S. Constitution, federal law preempts State law when preemption is the clear and manifest purpose of Congress. In instances where the purpose of Congress is not clear, only the judicial branch of government can determine whether a federal law preempts a State law under the Supremacy Clause.

In enacting HIPAA, Congress clearly did not supersede State laws that impose more stringent standards with respect to the privacy of individually identifiable health information. Thus, the Department will continue to enforce such State laws that are within the Department's purview to enforce. The Department will enforce other State laws to the extent that the Privacy Rule does not preempt them. Under the provisions of the Privacy Rule, the Privacy Rule does not alter State laws that permit individuals greater rights of access to or amendment of their own individually identifiable health information (45 CFR § 160.202(More stringent)).

April 14, 2003, is the compliance date for most covered entities under the Privacy Rule. Unless the relevant federal or State laws or regulations are amended, the Department intends to enforce specified provisions of State law as outlined in the following charts.

PHL § 17

HIPAA Privacy Rule	PHL § 17	Law That Will Prevail
<p>A "covered entity" may generally disclose "protected health information" (PHI) to another covered entity for treatment, payment or health care operations without consent (164.506(a), 164.506(c)). A covered entity may use or disclose PHI without an authorization or opportunity to agree or object to the extent that such use or disclosure is "required by law" (164.512(a), 164.501(Required by law)).</p>	<p>"Upon the written request . . . [of a patient, a provider] . . . must release and deliver . . . copies of all . . . medical records . . . regarding that patient to any other designated physician or hospital. . ." (PHL § 17).</p>	<p>PHL § 17 prevails, because disclosures under PHL § 17 are "required by law."</p>
<p>"If, and to the extent, prohibited by an applicable provision of State . . . law, . . . a covered entity may not disclose, or provide access . . . to, protected health information about an unemancipated minor to a parent, guardian, or other person acting <i>in loco parentis</i>" (164.502(g)(3)(ii)(B)).</p>	<p>". . . [R]ecords concerning the treatment of an infant patient for venereal disease or the performance of an abortion operation upon such infant patient shall not be released or in any manner be made available to the parent or guardian of such infant. . ." (PHL § 17).</p>	<p>PHL § 17 prevails, because it is a provision of State law that prohibits a disclosure about an unemancipated minor to a parent, guardian, or other person acting <i>in loco parentis</i>. Also, PHL § 17 prevails, because HIPAA does not preempt State law that imposes privacy standards that are "more stringent than" the standards imposed under HIPAA (P.L. 104-191, § 264(c)(2)).</p>

PHL § 18

HIPAA Privacy Rule	PHL § 18	Law That Will Prevail
General rule		
Applies to any "covered entity": health care provider, health plan or health care clearinghouse (unless the entity transmits no health information in electronic form in connection with a transaction covered by the HIPAA Regulations) (160.102)	Applies to any "health care provider" as defined in New York law (18(2), 18(1)(b), 18(1)(c), 18(1)(d))	HIPAA prevails for health plans, health care clearinghouses and individuals who are health care providers under HIPAA but are not health care practitioners under State law. <u>The remainder of this chart is confined to the law for "health care providers" under State law.</u>
Applies to all medical records and billing records and any other records used to make decisions about individuals (164.524(a), 164.501(Designated record set))	Applies to information concerning or relating to the examination, health assessment or treatment of an individual (18(2), 18(1)(e))	HIPAA prevails for billing records. <u>The remainder of this chart is confined to "patient information" under State law.</u>
Exceptions to the general rule (when access can be denied)		
No exception	Does not apply to clinical records (maintained or possessed by an OMH, OMRDD or OASAS facility) access to which is governed under Mental Hygiene Law §§ 22.03 and 33.16 (18(1)(e)(i))	The law for clinical records maintained or possessed by an OMH, OMRDD or OASAS facility is beyond the scope of this chart.
Does not apply to psychotherapy notes (164.524(a)(1)(i), 164.501(Psychotherapy notes)).	No exception	For psychotherapy notes as defined by HIPAA, PHL § 18 prevails.
No exception	Does not apply to <u>practitioner's personal notes and observations</u> (18(1)(e)(ii))	For personal notes and observations other than psychotherapy notes as defined by HIPAA, HIPAA prevails
No exception	Does not apply to information maintained by a practitioner, concerning or relating to the prior examination or treatment of a subject received from another practitioner (18(1)(e)(iii))	HIPAA prevails
No exception	Does not apply to diagnostic services performed by a practitioner at the request of another practitioner (18(1)(e)(last sentence))	HIPAA prevails

<p>Does not apply to PHI 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 (164.524(a)(2)(v))</p>	<p>Does not include data disclosed to a practitioner in confidence by other persons on the basis of an express condition that such data would never be disclosed (18(1)(e)(iv))</p>	<p>HIPAA prevails</p>
<p><u>PHI does not make reference to another person</u>, and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to <u>endanger the life or physical safety</u> of the individual or another person (164.524(a)(3)(i)), e.g., when an individual exhibits suicidal or homicidal tendencies. This exception is intended to apply where disclosure is reasonably likely to result in the individual committing suicide, murder, or other physical violence. Under this reason for denial, covered entities may not deny access on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm (65 Fed. Reg. 82,555).</p>	<p>Provider may deny access to all or part of the information and may grant access to a prepared summary of the information if, after consideration of all the attendant facts and circumstances, the <u>provider determines that the request to review all or a part of the patient information can reasonably be expected to cause substantial and identifiable harm to the subject or others</u> which would outweigh the qualified person's right of access to the information (18(3)(d)(i)).</p>	<p>HIPAA prevails</p>
<p><u>PHI makes reference to another person</u>, and a licensed health care professional has determined, in the exercise of professional judgment, that disclosure is reasonably likely to cause <u>substantial harm to such other person</u> (164.524(a)(3)(ii)). Substantial harm means serious harm (65 Fed. Reg. 82,555) and may be substantial physical, emotional, or psychological harm (65 Fed. Reg. 82,556).</p>	<p>Provider may deny access to all or part of the information and may grant access to a prepared summary of the information if, after consideration of all the attendant facts and circumstances, the provider determines that the request to review all or a part of the patient information can reasonably be expected to cause <u>substantial and identifiable harm to the subject or others</u> which would outweigh the <u>qualified person's right of access</u> to the information (18(3)(d)(i)).</p>	<p>HIPAA prevails if disclosure would cause substantial harm to the subject but not to the other person. PHL § 18 prevails if disclosure would cause substantial harm to the other person.</p>

<p><u>The request is made by the individual's personal representative,</u> and a licensed health care professional has determined, in the exercise of professional judgment, that disclosure is reasonably likely to cause <u>substantial harm to the individual or another person</u> (164.524(a)(3)(iii)).</p>	<p>Provider may deny access to all or part of the information and may grant access to a prepared summary of the information if, after consideration of all the attendant facts and circumstances, the provider determines that the request to review all or a part of the patient information can reasonably be expected to cause <u>substantial and identifiable harm to the subject or others which would outweigh the qualified person's right of access</u> to the information (18(3)(d)(i)).</p>	<p>PHL § 18 prevails</p>
<p>Parental access to child's health information</p>		
<p>General rule is that parent has access (164.502(g)(1)).</p>	<p>General rule is that parent has access (18(2), 18(1)(g)).</p>	<p>No conflict</p>
<p>Parents have no right of access if minor can lawfully obtain health care service without the consent of a parent (164.502(g)(3)(i)). "If, and <u>to the extent</u>, permitted or required by an applicable provision of State . . . law, . . . a covered entity may disclose, or provide access . . . to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis (164.502(g)(3)(ii)(A)).</p>	<p>If a parent requests information concerning a child over 12 years old, the practitioner may notify the child and if the child objects to disclosure, may deny the request (18(3)(c)).</p>	<p>PHL § 18 prevails, because a covered entity may only disclose PHI to a parent to the extent permitted by State law. Also, HIPAA does not preempt State law that imposes privacy standards that are "more stringent than" the standards imposed under HIPAA (P.L. 104-191, § 264(c)(2)).</p>
<p>Parent has no right to access if the covered entity has a reasonable belief that the child has been or may be subjected to domestic violence, abuse or neglect by the parent or disclosure could endanger the child and the covered entity, in the exercise of professional judgment, decides that disclosure is not in the best interest of the child (164.502(g)(5)).</p>	<p>Provider may deny access to all or part of the information and may grant access to a prepared summary of the information if, after consideration of all the attendant facts and circumstances, the provider determines that disclosure would have a detrimental effect on the provider's professional relationship with an infant, or on the care and treatment of the infant, or on the infant's relationship with his or her parents (18(3)(d)(i), 18(2)(c)).</p>	<p>PHL § 18 prevails</p>

Fees		
Covered entity may impose a reasonable, cost-based fee (164.524(c)(4)).	The provider may impose a reasonable charge, not to exceed costs and not to exceed 75¢ per page, but the release of records cannot be denied solely because of inability to pay (18(2)(e)).	PHL § 18 prevails
Procedure		
Covered entity must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format, in a timely manner (30 or 60 days, with a possible 30 day extension) (164.524(c)(2), 164.524(b)(2)).	Provider must permit visual inspection within 10 days and furnish a copy within a reasonable time if the provider has space available to permit visual inspection, or must provide a copy within 10 days if the provider does not have space available to permit visual inspection (18(2)(a), (d), (g)).	PHL § 18 prevails
A licensed health care professional must be designated by the provider as a reviewing official to make a final determination (164.524(d)(4)).	A medical record access review committee appointed by the commissioner of the Department of Health (DOH) reviews appeals of denials of access (18(4)).	No conflict, because it is possible to comply with both the State and federal requirements. The reviewing official reviews HIPAA issues, and the medical record access review committee reviews PHL § 18 issues.
Individuals have a right to have a covered entity amend inaccurate or incomplete PHI about themselves created by a health care provider. Where a request to amend is denied, individuals may submit into the medical record a written statement of disagreement and the provider may submit a written rebuttal to such statement (164.526).	Individual may challenge the accuracy of information and may require that a brief written statement prepared by the individual concerning the challenged information be inserted into the medical record (18(8)).	HIPAA prevails

PHL § 206(1)(j)

HIPAA Privacy Rule	PHL § 206(1)(j)	Law That Will Prevail
<p>Generally, a covered entity may not disclose PHI for research purposes without an authorization (164.508). A covered entity may disclose PHI without authorization to the extent that such use or disclosure is to a public health authority for public health activities (164.512(b)), to a health oversight authority for health oversight activities (164.512(d)) or if an IRB has waived the requirement to get an authorization, applying the specific criteria in 164.512(i). A covered entity must provide an accounting of a § 206(1)(j) disclosure if the subject did not authorize the disclosure and requests an accounting (164.528). PHI may only be disclosed in a manner consistent with a covered entity's Notice of Privacy Practices (164.502(i)). If disclosure is not pursuant to an authorization, covered entities must limit PHI disclosed for research to that which is reasonably considered to be the "minimum necessary" to accomplish the research (164.514(d)(3)(ii)). However, the covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for section 206(1)(j) research if DOH represents that the information DOH is requesting is the minimum necessary to do the research (164.514(d)(3)(iii)). PHI that is de-identified under HIPAA is no longer PHI and is no longer subject to HIPAA (164.514(a), (b), (c)). A covered entity may disclose a "limited data set" to DOH for research purposes if DOH executes a "data use agreement" (164.514(e)).</p>	<p>The Commissioner of DOH shall cause to be made scientific studies and research, and in conducting such studies and research, the commissioner is authorized to collect information, and such information shall be kept confidential and shall be used solely for the purposes of medical or scientific research or the improvement of the quality of medical care through the conduction of medical audits (PHL § 206(1)(j)).</p>	<p>Covered entities may disclose PHI to DOH under PHL § 206(1)(j):</p> <ol style="list-style-type: none"> (1) if the subject authorizes the disclosure under HIPAA; or (2) if an IRB has waived the requirement to get authorization, applying the specific criteria in HIPAA. <p>(A covered entity may disclose PHI to DOH without authorization for public health or health oversight activities, but such activities would not generally be considered PHL § 206(1)(j) research.)</p> <p>In addition, the disclosure must be:</p> <ol style="list-style-type: none"> (1) accounted for by the provider if not authorized by the subject; (2) consistent with the provider's Notice of Privacy Practices; and (3) the minimum necessary to accomplish the research if not authorized by the subject. DOH could be asked to represent that the requested disclosure is the minimum necessary. <p>Also, covered entities may disclose information that has been de-identified under HIPAA. Alternatively, a covered entity may disclose a "limited data set" to DOH for research purposes if DOH executes a "data use agreement."</p>

PHL § 2782

HIPAA Privacy Rule	PHL § 2782	Law That Will Prevail
<p>"If, and to the extent, permitted or required by an applicable provision of State . . . law, . . . a covered entity may disclose, or provide access . . . to, protected health information about an unemancipated minor to a parent, guardian, or other person acting <i>in loco parentis</i>" (164.502(g)(3)(ii)(A)).</p>	<p>"No person who obtains confidential HIV related information in the course of providing any health or social service or pursuant to a release of confidential HIV related information may disclose or be compelled to disclose such information, except to . . . an authorized agency in connection with foster care or adoption of a child" (PHL § 2782(1)(h)).</p>	<p>HIPAA does not preempt PHL § 2782(1)(h), but HIPAA may require an authorization to disclose confidential HIV related information to an authorized agency in connection with foster care or adoption of a child, if the agency is not a "person acting <i>in loco parentis</i>."</p>
<p>A covered entity may use or disclose PHI without an authorization or opportunity to agree or object to the extent that such use or disclosure is "required by law" (164.512(a), 164.501(Required by law)) or if the disclosure is "for a law enforcement purpose to a law enforcement official . . . [i]n compliance with and as limited by the relevant requirements of . . . [a]n administrative request. . . ." (164.512(f)(1)(ii)).</p>	<p>"No person who obtains confidential HIV related information in the course of providing any health or social service or pursuant to a release of confidential HIV related information may disclose or be compelled to disclose such information, except to . . . an employee or agent of the division of parole . . . [or] an employee or agent of the division of probation and correctional alternatives or any local probation department . . . [or] an employee or agent of the commission of correction" (PHL § 2782(1)(l), (m), (o)).</p>	<p>HIPAA does not preempt PHL § 2782(1)(l), (m) or (o). Nor would HIPAA require an authorization to disclose confidential HIV related information under these provisions, because such disclosures may be required by law or are for law enforcement purposes to law enforcement officials in compliance with and as limited by the relevant requirements of an administrative request.</p>

<p>Generally, a covered entity must treat a "personal representative" of a person who is the subject of PHI as though the personal representative were the person (164.502(g)).</p>	<p>Generally, a parent, legally appointed guardian or committee exercises rights on behalf of a child, ward or incapacitated person (<u>e.g.</u>, PHL § 18(2)(b), (c)).</p>	<p>Preemption of Mental Hygiene Law Article 81 and Surrogate's Court Procedure Act Articles 17 and 17-A is beyond the scope of this chart. This row of this chart is merely intended to preface the analysis of preemption of PHL § 2782(4) below.</p>
<p>If under applicable law a person has authority to act on behalf of an individual who is <u>an adult or an emancipated minor</u> in making decisions related to health care, a covered entity must treat such person as a personal representative with respect to PHI relevant to such personal representation (164.502(g)(2)).</p> <p>A covered entity may not disclose PHI about an <u>unemancipated minor</u> to a parent, guardian, or other person acting <i>in loco parentis</i> to the extent that an applicable provision of State or other law, including applicable case law, prohibits such disclosure (164.502(g)(3)(ii)(B)).</p> <p>A covered entity may elect not to treat a person as the personal representative of an individual if:</p> <p>(i) The covered entity has a reasonable belief that: (A) The individual has been or may be subjected to domestic violence, <u>abuse</u>, or <u>neglect</u> by such person; or (B) Treating such person as the personal representative could <u>endanger</u> the individual; <u>and</u></p> <p>(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative (164.502(g)(5)).</p>	<p>"A physician may disclose <u>confidential HIV related information</u> pertaining to a protected individual to a <u>person</u> (known to the physician) <u>authorized pursuant to law to consent to health care</u> for a protected individual when the physician reasonably believes that: (1) disclosure is medically necessary in order to provide timely care and treatment for the protected individual; and (2) after appropriate counseling as to the need for such disclosure, the protected individual will not inform a person authorized by law to consent to health care; <u>provided, however, that the physician shall not make such disclosure if</u>, in the judgment of the physician: (A) the <u>disclosure would not be in the best interest of the protected individual</u>; or (B) the protected individual is authorized pursuant to law to consent to such care and treatment" (PHL § 2782(4)(e) [emphasis supplied]).</p>	<p>PHL § 2782(4)(e) prevails. A physician shall not disclose confidential HIV related information to a parent or guardian of a protected individual, if in the judgment of the physician, the disclosure would not be in the best interest of the protected individual, because HIPAA does not preempt State law that imposes privacy standards that are "more stringent than" the standards imposed under HIPAA (P.L. 104-191, § 264(c)(2)). Also, a physician shall not disclose confidential HIV related information to a parent or guardian of a minor who is a protected individual, if in the judgment of the physician, the disclosure would not be in the best interest of the protected individual, because State law prohibits such disclosure. There is no conflict between HIPAA and State law with respect to a disclosure of confidential HIV related information to a personal representative of a protected individual in abuse, neglect or endangerment situations, where, in the judgment of the physician, the disclosure would not be in the best interest of the protected individual.</p>

PHL § 2805-m

HIPAA Privacy Rule	PHL § 2805-m	Law That Will Prevail
<p>The HIPAA right of access to PHI applies to all medical records and billing records and any other records <u>used to make decisions about individuals</u> (164.524(a), 164.501 (Designated record set)). Individual means the person who is the subject of PHI (164.501 (Individual)).</p>	<p>Information required to be collected and maintained under PHL §§ 2805-j, 2805-k and reports required to be submitted under PHL § 2805-l and any incident reporting requirements imposed upon diagnostic and treatment centers shall be kept confidential and shall not be released except to DOH or under PHL § 2805-k(4).</p>	<p>PHL § 2805-m prevails. None of the information that must be kept confidential under PHL § 2805-m is part of an individual's designated record set under HIPAA, because such information is not used to make decisions about the subject of the PHI.</p>

PHL § 4410

HIPAA Privacy Rule	PHL § 4410(2)	Law That Will Prevail
<p>A covered entity may use and disclose PHI for treatment, payment, or health care operations without consent (164.502(a)(1)(ii), 164.506). A covered entity may obtain consent of the individual to use or disclose PHI to carry out treatment, payment, or health care operations (164.506(b)(1)). Except in an emergency treatment situation, a provider must make a good faith effort to obtain a written acknowledgment of receipt of the provider's Notice of Privacy Practices, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained (164.520(c)(2)(ii)).</p>	<p>"Unless the patient waives the right of confidentiality, a health maintenance organization or its comprehensive health services plan shall not be allowed to disclose any information which was acquired by such organization or plan in the course of the rendering to a patient of professional services by a person authorized to practice medicine, registered professional nursing, licensed practical nursing, or dentistry, and which was necessary to acquire to enable such person to act in that capacity, except as may be otherwise required by law. A non-participating provider shall provide an enrollee's organization with such patient information as is reasonably required by the organization to administer its plan. In making such disclosure a provider shall comply with the provisions of subdivision six of section eighteen of this chapter concerning the disclosure of patient information to third parties provided, however, that with respect to a protected individual as defined in subdivision six of section twenty-seven hundred eighty of this chapter, disclosure shall be made only pursuant to an enrollee's written authorization and shall otherwise be consistent with the requirements of such section and rules and regulations promulgated pursuant thereto" (PHL § 4410(2)).</p>	<p>Health maintenance organizations must comply with both HIPAA and State law.</p>

Civil Rights Law § 79-1

HIPAA Privacy Rule	Civil Rights Law § 79-1	Law That Will Prevail
<p>A "covered entity" may generally disclose PHI to another covered entity for treatment, payment or health care operations without consent (164.502(a)(1)(ii), 164.506(a), 164.506(c)). A covered entity generally must have authorization to disclose PHI for other purposes (164.508). To be valid, an authorization must contain specified elements and comply with specified requirements (164.508(c)).</p>	<p>No person shall perform a genetic test on a biological sample taken from an individual without the prior written informed consent of such individual consisting of eight specific elements (Civil Rights Law § 79-1(2)).</p>	<p>Disclosures of genetic test information for treatment, payment or health care operations need only be in compliance with Civil Rights Law § 79-1. If not for treatment, payment or health care operations, a HIPAA-compliant authorization is also required.</p>

Education Law § 6530(23)

HIPAA Privacy Rule	Education Law § 6530(23)	Law That Will Prevail
<p>A covered entity may use and disclose PHI for treatment, payment, or health care operations without consent (164.502(a)(1)(ii), 164.506). A covered entity may obtain consent of the individual to use or disclose PHI to carry out treatment, payment, or health care operations (164.506(b)(1)). Except in an emergency treatment situation, a provider must make a good faith effort to obtain a written acknowledgment of receipt of the provider's Notice of Privacy Practices, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained (164.520(c)(2)(ii)).</p>	<p>The following is professional misconduct for a physician, physician's assistant or a specialist's assistant: "Revealing of personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient, except as authorized or required by law."</p>	<p>Physicians, physician's assistants and specialist's assistants must comply with both HIPAA and State law.</p>