

HIPAA BACKGROUND INFORMATION

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act, a federal law passed in 1996 to improve the efficiency and effectiveness of the nation's health care system. The act includes a series of administrative simplification provisions requiring the use of industry-wide standard data sets and calls for new safeguards on the privacy and security of the personal health information.

What do the HIPAA privacy regulations address?

The HIPAA privacy regulations, entitled "The Standards for Privacy of Individually Identifiable Health Information" were issued by the U.S. Department of Health and Human Services pursuant to the federal HIPAA statute. The HIPAA Privacy Regulations, which take effect on April 14, 2003, provide the first comprehensive federal protection for the privacy of individuals' medical records and other personal health information. In general, the HIPAA Privacy Regulations:

- Give individuals the right to access their medical records;
- Limit the use and disclosure of individually identifiable health information;
- Restrict most disclosures of information to the minimum needed for the intended purpose; and
- Provide civil and criminal penalties if these privacy rights are violated.

What types of organizations and individuals are required to comply with HIPAA?

HIPAA privacy standards apply to:

- Health care providers who transmit any health information electronically in connection with certain transactions;
- Health plans; and
- Health care data clearinghouses.

What is covered by HIPAA?

HIPAA covers Protected Health Information (PHI) which is individually identifiable health information relating to:

- Past, present or future physical or mental health or condition of an individual;
- Provision of health care to an individual; or
- The past present or future payment for health care provided to an individual.

This broad definition includes medical records and history, enrollment data, health plan choice and health insurance premium information.

HIPAA: NYSHIP and NYS Participating Employers

Please note that the following information relates to your agency as a Participating Employer in the New York State Health Insurance Program (NYSHIP) only. It applies to all NYSHIP programs in which your agency has elected to participate which may include the Health Insurance Program (the Empire Plan and NYSHIP HMO coverage), the Dental Program and/or the Vision Program. If your agency offers other health insurance plans to employees you should consult with your legal counsel regarding how the provisions of HIPAA affect you in relation to those plans. Also, this information pertains only to the HIPAA privacy regulations. Other HIPAA regulations may be issued in the future and result in additional requirements and/or obligations.

What is NYSHIP's status under HIPAA?

As a group health plan NYSHIP is a covered entity under HIPAA and as such must fully comply with the requirements of HIPAA. The NYSHIP's plan sponsor is the Health Insurance Council, as established in NYS Civil Service Law. The Council consists of the President of the Civil Service Commission, the Director of the Budget and the Director of the Governor's Office of Employee Relations.

As a Participating Employer in NYSHIP, how is your agency affected by HIPAA privacy regulations?

As the result of our review of the HIPAA privacy regulations we have determined that, within the context of NYSHIP participation, a Participating Employer is subject to some HIPAA privacy requirements. HIPAA has the effect of restricting the flow of certain types of information related to the health care of the employer's employees and restricts the circumstances under which those types of information can be disclosed to the employer by the plan and the plan's insurers.

Pursuant to 45 CFR 164.504(f), the NYSHIP and its program insurers and/or administrators may disclose to a Participating Employer information on whether an employee is enrolled in, or has disenrolled from, the program(s). Additionally, the NYSHIP and its program insurers and/or administrators may disclose summary health information to a Participating Employer if the Participating Employer requests the summary health information for one of the following purposes:

- To obtain premium bids from other plans;
- To provide health insurance coverage under the Participating Employer's group health plan; or
- To modify, amend, or terminate the Participating Employer's group health plan.

In the past, the NYSHIP has provided Participating Employers with enrollment information and summary health information upon request, and will continue to do so as long as the information is for the purposes described above, consistent with HIPAA privacy requirements. The NYSHIP has not disclosed individual-specific health information to Participating Employers in the absence of a signed authorization by the individual, and will continue to follow that practice, consistent with HIPAA privacy requirements. Therefore, if an employee requests assistance from agency staff in resolving a NYSHIP claim problem that involves the disclosure of protected health information, such authorization will be required.

What steps does your agency need to take to ensure compliance with HIPAA?

Because a NYSHIP Participating Employer may receive and use only enrollment information and summary health information, being a NYSHIP Participating Employer does not make your agency subject to most HIPAA privacy implementation requirements. For example, as a **NYSHIP Participating Employer** your agency is:

- **Not** required to amend any documents it has produced describing the terms of its local group health plans [45 CFR 164.504(f)];
- **Not** required to maintain or provide a Notice of Privacy Practices [45 CFR 164.520(a)];
- **Not** required to designate a privacy official or a complaint official; and
- **Not** required to implement policies and procedures regarding other HIPAA requirements such as training, organizational safeguards, a complaint process, sanctions for noncompliance by employees that violate HIPAA standards, mitigation procedures to address violations of HIPAA standards, or to otherwise implement other standards that the NYSHIP has been required to implement.

However, as a NYSHIP Participating Employer, your agency is subject to the following HIPAA privacy requirements [45 CFR 164.530]:

- A Participating Employer may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual as a consequence of the individual having exercised any right he or she may have pursuant to HIPAA, or as a consequence of an individual having participated in any process established by the HIPAA regulations, such as filing a complaint with the NYSHIP or with the Secretary of Health and Human Services concerning the NYSHIP's privacy practices. Also, no such action may be taken against any individual(s) who testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act, or for opposing any act or practice that the person believes violates HIPAA privacy requirements as long as the individual acts in good faith, the manner of opposition is reasonable, and the manner of opposition does not involve a disclosure of another person's protected health information.
- A Participating Employer may not require any individual to waive their right under 45 CFR 160.306 to file a complaint with the Secretary of Health and Human Services concerning a potential violation of HIPAA privacy requirements as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

What steps is NYSHIP taking to be HIPAA compliant by April 14, 2003?

NYSHIP will be fully compliant with HIPAA by the effective date. NYSHIP has or is in the process of taking the following steps in accordance with HIPAA requirements:

- Amending its Plan documents;
- Amending its contracts with program insurers and/or administrators;
- Maintaining a Notice of Privacy Practice;
- Designating a privacy official and a complaint official;
- Providing HIPAA training to staff;
- Implementing security safeguards;
- Establishing a complaint process;
- Establishing sanctions for noncompliance by employees that violate HIPAA standards; and
- Establishing mitigation procedures to address violations of HIPAA standards.

Additionally, enrollees in NYSHIP will be receiving Notices of Privacy Practices from the insurers and/or administrator of each program in which they are enrolled. Enrollees may request a copy of NYSHIP's Notice of Privacy Practice by contacting the Employee Benefits Division; it will also be available on the Department's website at www.dcs.state.ny.us, and click on Employee Benefits.