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

ADMINISTRATIVE DIRECTIVE

TRANSMITTAL: 06 OMM/ADM-1

TO: Commissioners of Social Services

DIVISION: Office of Medicaid Management

DATE: March 1, 2006

SUBJECT: Instructions for Implementing HIPAA Privacy Protections in LDSS

SUGGESTED DISTRIBUTION: Medicaid Directors
Staff Development Coordinators

CONTACT PERSON: OMM HIPAA Privacy Coordinator
James F. Botta (518) 473-4848
JFB04@health.state.ny.us

ATTACHMENTS:
Attachment 1. LDSS Covered Entity Commissioners letter
Attachment 2. HIPAA Training Package
Attachment 3. Protected Health Information
Attachment 4. Notice of Privacy-English and Spanish
Attachment 5. Enrollee request for Specific Protected Health Information
Attachment 5a Authorization for release of Protected Health Information
Attachment 6 HIPAA Business Associate Appendix
Attachment 7 HIPAA Privacy Rules

FILING REFERENCES

Previous ADMs/INFs	Releases Cancelled	Dept. Regs. see below**	Soc. Serv. Law & Other Legal Ref.	Manual Ref.	Misc. Ref.
03 OMM/ADM-3 97 ADM-15, 91 ADM-36, 90 ADM-21		PHL) Article 27-F 18 NYCRR Parts 357, 360-8,403,428, 441, and 507 and 10 NYCRR Part 63, PHL-Section 2780(7), Section 2782(5) 18 NYCRR Parts 357, 403, 428, 441, and 507	45 C.F.R. §164.502, §164.508, §164.520, §164.522, §164.524, §164.526, §164.528, §164.530, §164.532(B) 42 C.F.R. Part 2		

I. PURPOSE:

The purpose of this Directive is to review actions taken thus far by the Department of Health/Office of Medicaid Management (OMM) to assist Local Departments of Social Services (LDSS) to implement the Health Insurance Portability and Accountability Act (HIPAA) privacy provisions as related to their Medicaid operations- (Medicaid Program, Medicaid Managed Care, Child Health Plus-A and Family Health Plus). In addition, this ADM will describe steps OMM has taken to implement the notice of privacy practices and the privacy right provisions of HIPAA. Since some of these procedures involve referrals to the LDSS for updating information on WMS or other interaction between OMM and the LDSS, this ADM contains information necessary to help the LDSS implement the HIPAA privacy provision. The procedures described herein are intended to remind the LDSS of HIPAA privacy requirements and to inform them of how it was implemented at the state Medicaid Program level.

II. BACKGROUND

HIPAA defines a covered entity as a health plan, a term encompassing health insurance companies, public health programs like Medicaid and Medicare, providers of health care and organizations that help providers bill for their services.

The Local Departments of Social Services (LDSS) Medicaid operation/unit is considered by the state Medicaid program to be functioning as a "Covered Entity'' for the purposes of HIPAA implementation. Local Departments of Social Services (LDSS) are receiving and handling increased amounts of confidential information relating to applicants for recipients of public assistance and Medicaid benefits in order to qualify for assistance. Welfare reform created changes in eligibility requirements that encourage self-disclosure for various exemptions. The implementation of Medicaid mandatory managed care also increased the amount of alcohol and substance abuse related and HIV-related information being handled in LDSS offices. The New York State Department of Health and the New York State Office of Alcoholism and Substance Abuse Services regulations provide that all social service officials, employees and their agents, are responsible for ensuring that no discrimination or abuse occurs against applicants or recipients about whom confidential information is maintained. It is important to remember that HIPAA Privacy procedures do not supercede existing privacy rights incorporated in Title XIX. For Medicaid, HIPAA privacy rights add new procedures to existing privacy requirements that OMM and LDSS have followed for Medicaid recipients since the Medicaid program was established. For your information, relevant citations are provided: Copies of these citations can be obtained from OMM's HIPAA privacy coordinator - James F. Botta, Medicaid Privacy Coordinator - (518) 473-4848; **jfb04@health.state.ny.us**. Mr. Botta is the main contact for questions that the LDSS may have related to all Protected Health Information. See Attachment 7.

There are several existing statutes that establish a framework for Medicaid confidentiality.

A. Medicaid:

1. Section 1902(a)(7) of the Social Security Act requires that state Medicaid plans "provide safeguards that restrict the use and disclosure of information concerning applicants and recipients to purposes directly connected with the

administration of the plan." Therefore, disclosure of information concerning applicants and beneficiaries must be limited to purposes directly connected with the administration of the State Medicaid plan, which includes the delivery of medical services. Purposes related to plan administration include: (1) establishing eligibility; (2) determining the amount of medical assistance; (3) providing services for recipients; and (4) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan (42 CFR 431.302). Therefore, release is permitted of information that is necessary in order to allow a discrete organizational entity or agency to know which services, if any, Medicaid will pay for, and to what extent the organizational entity or agency should bill Medicare or other third parties before billing Medicaid.

B. HIV: State law and regulations limit the general handling of HIV and AIDS data. Regulations and statutes addressing these requirements are contained in Public Health Law (PHL) Article 27-F, 18 NYCRR Parts 357, 403, 428, 441 and 505, and Subpart 360-8, and 10 NYCRR Part 63. The statute and regulations require the development of policies and procedures for accessing, disclosing, and safeguarding the confidentiality of HIV-related information and the communication of such policies and procedures to social services officials, employees and agents. PHL §2783 1 (b) specifically provides for civil penalties not to exceed $5,000.00 for each violation of inappropriate disclosure of HIV-related information.

> **NOTE:** Previously issued requirements pertaining to disclosure and retention of HIV-related information by child welfare staff as described in 18 NYCRR Parts 357, 403, 428, 441, and 507, as well as in 97 ADM-1 5, 91 ADM-36, and 90 ADM-21 remain pertinent and should continue to be followed.

C. Alcohol and Substance Abuse:

1. Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

III. The Department of Health Office of Medicaid Management has taken the following important steps to communicate HIPAA privacy requirements to LDSS

A. Three educational sessions were conducted at the 2003 NYPWA Winter Conference on HIPAA privacy legal requirements, background and regulations. Comprehensive notebooks, "New York State's Privacy Policies and Forms for HIPAA Covered Programs," were distributed to all attendees and mailed to those LDSS that did not obtain a copy personally. If you would like an additional copy of these materials, contact OMM's HIPAA Privacy Coordinator, James F. Botta at (518) 473-4848; jfb04@health.state.ny.us.

B. A letter (Attachment 1) was mailed from Kathryn Kuhmerker, Deputy Commissioner, Office of Medicaid Management, to LDSS Commissioners on March 27, 2003. The letter informed LDSS of the DOH Counsel's opinion that LDSS are covered entities. A letter (Attachment 2) from Kathryn Kuhmerker, Deputy Commissioner, Office of Medicaid Management was mailed to all local districts on April 7, 2003, describing the HIPAA privacy training requirements and included a copy of the Department of Health, Office of Medicaid Management Power Point presentation used to train staff (See Attachment 1).

C. An Administrative Directive (Transmittal 03 OMM/ADM-03) was mailed to all local districts on April 16, 2003 informing them that OMM intended to fulfill the notice requirements (45 C.F.R § 164.520) by mailing a privacy notice to all Medicaid households. This ADM included copies of the notice and required action the LDSS needed to take to meet the continuing notice requirements of HIPAA through distribution of the materials to new enrollees.

D. OMM has created a Medicaid HIPAA website to enhance our ability to share pertinent information in a timely and efficient format. The site may be accessed at: **http://www.health.state.ny.us/nysdoh/medicaid/hipaa/hipaamain.htm**.

IV. HIPAA Citations and Office of Medicaid Management (OMM) Actions

A. Privacy Officer (45 C.F.R. § 164.530(a)(1))

1. Summary: A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

2. Key implementation steps taken by OMM:

   a. OMM has appointed a privacy coordinator, James Botta - (518) 473-4848; jfb04@health.state.ny.us . This individual coordinates all HIPAA Privacy operations for the State Medicaid Operations.
   b. DOH has appointed a privacy officer, Jean Quarrier – (518) 486-1336; joq01@health.state.ny.us . This individual is the HIPAA Privacy Director for the entire Department of Health.

B. Notice of Privacy Practices (45 C.F.R § 164.520)

1. Summary: A recipient has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. The notice must contain a description, including at least one example, of the types of uses and disclosures that the covered entity is permitted to make for each of the following purposes: treatment, payment and health care operations.

2. Key implementation steps taken by OMM:

   a. The Medicaid Privacy Notice has been mailed to all Medicaid heads of household, including Family Health Plus, Medicaid Managed Care and Child Health Plus A enrollees.
   b. A copy of the Notice was mailed (e-mail and regular mail) to LDSS, with appropriate guidelines. See Administrative Directive (Transmittal 03 OMM/ADM-03).
   c. The State will do a mass re-mailing every three years.

C. Recipient Inquiries/Protected Health Information Requests (45 C.F.R § 164.524).

1. Summary: The covered entity must provide the access requested by individuals, including inspection, or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

   a. A recipient has a right of access to inspect and/or obtain a copy of protected health information (PHI) about the individual in a designated record set, or ask about its uses for as long as the protected health information is maintained in the designated record set, except for inquires as designated in this section of the regulation. PHI includes a recipient's Medicaid enrollment, claims and managed care encounter information, etc. Note that the LDSS (or Maximus for LDSS where Maximus is the enrollment broker) may receive consumer requests to access this information. If Maximus cannot answer questions, the recipient should be referred to the Medicaid Helpline. (See #2 below)
   b. If a recipient wishes to obtain a copy of PHI about themselves, this must be done in writing. (See Attachment 5— New York State Department Of Health, Office Of Medicaid Management - Enrollee/Patient Request for Specific Medicaid Protected Health Information.)

3. Key implementation steps taken by OMM:

   a. The Medicaid Help Line in OMM (518-486-9057 or 800-541-2831) was established as the single point of entry for Medicaid, Family Health Plus, Medicaid Managed Care and Child Health Plus A Notice-related inquiries/requests.
   b. If a request for PHI is received by the State OMM, it is referred to the HIPAA Privacy Coordinator.
   c. While OMM has established the procedures to respond to a recipient's privacy rights as described in the HIPAA regulation, LDSS will need to establish a process for ensuring individual requests for PHI or changes to PHI are properly addressed. In the local district offices, these will most likely be changes to Eligibility Data for the recipient.

d. OMM staff use existing procedures that require a written request from the enrollee. Staff verifies that the address on the request matches the address on the Recipient Master File. If the address does not match, OMM staff makes an effort to contact the recipient to resolve the discrepancy. OMM staff will also call the LDSS to verify a possible change of address. A copy of the request annotated with the date of response is kept on file.
e. The OMM Designated Record Set is composed of all enrollments, claims and encounter history on the OMM/AFPP Datamart, which contains all recipients' billing and eligibility records (currently 10/96 forward). It is anticipated that this will generally satisfy a recipient's right to access PHI in MMIS since it is the complete record of PHI that OMM maintains. It is also recognized that the LDSS may have WMS information, local administrative claims data, or medical information used to determine eligibility. Recipients may pursue this information by requesting it through the LDSS.
f. The OMM will search for PHI included in Prior Approval records when requested by a recipient. It is expected that when PA information is automated under eMedNY we will automatically send for this information and return it to the requestor.
g. Requests received by OMM for information about a Fair Hearing will be directed to the Office of Temporary and Disability Assistance.

D. Minimum Necessary (45 C.F.R § 164.502, 164.530)

1. Summary: When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit the disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. Key implementation step taken by OMM:

a. Use and release of Protected Health Information (PHI) must be kept to the minimum necessary to perform functions related to the administration of the program. OMM will discuss with the applicant the specific data required for the intended use.

E. Business Associates (45 C.F.R § 164.502)

1. Summary: A contract between the covered entity and a business associate must establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate HIPAA requirements, if done by the covered entity, except that the contract may permit the business associate to use protected health information for the proper management and administration of the business associate, and the contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

a. Under HIPAA, Business Associate is a person or organization to whom the covered entity discloses protected health information so that the person or organization can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. A Business Associate includes contractors or other persons who receive protected health information from the covered entity (or from another Business Associate of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities.
b. A Business Associate relationship occurs when the right to use or disclose the protected health information belongs to the covered entity, and another person is using or disclosing the protected health information (or creating, obtaining and using the protected health information) to perform a function or activity on behalf of the covered entity. We also clarify that providing specified services to a covered entity creates a business associate relationship if the provision of the service involves the disclosure of protected health information to the service provider.
c. Business Associate excludes a person who is part of the covered entity's workforce.
d. When a health care provider discloses protected health information to health plans for payment purposes, no business associate relationship is established.

2. Key implementation steps taken by OMM

a. OMM identified all contracts, memorandums of understanding and data exchange applications covering the exchange of Medicaid PHI with outside entities. HIPAA compliant contract addendums were sent to all parties with requirements for them to sign and notarize the agreements. (See Attachment 6: **Federal Health Insurance Portability and Accountability Act (HIPAA) Business Associate Appendix.)**
b. OMM is modifying the standard Medicaid confidentiality Data Exchange Application and Agreement to include HIPAA compliant conditions.

F. Authorization for release of Protected Health Information for use or disclosure (45 CFR - 164.508)

1. Summary: Except as otherwise permitted or required by the regulations, a covered entity may not use or disclose protected health information without a valid authorization. When a covered entity obtains or receives a valid authorization for the use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

2. Key implementation steps taken by OMM:

   a. For requests from lawyers or legal guardians, or a recipient's family, the applicant must send a notarized authorization form that is HIPAA compliant (as per 45 CFR 164.508). The authorized request is good only for the specific request.
   b. Valid requests from a court or requests that are received under subpoena will be honored and the data will be released.
   c. (See Attachment 5 A) **AUTHORIZATION FOR RELEASE OF MEDICAID PROTECTED INFORMATION FROM THE NEW YORK STATE DEPARTMENT OF HEALTH, OFFICE OF MEDICAID MANAGEMENT TO A THIRD PARTY OTHER THAN A MEDICAID ENROLLEE/PATIENT.**

G. Recipient's Right to Restrict or Limit Disclosures or Request Alternative Means of Communication (45 C.F.R § 164.522)

1. Summary: A covered program must permit an individual to request that the covered program restrict or limit certain disclosures. The covered program does not have to agree. The Privacy Rule also allows individuals to request that communications by a covered program to the individual be made to the person at an alternative location, or by an alternative means, as long as the request is reasonable with respect to the administrative burden placed on the covered program. Health plans must accommodate all reasonable requests for confidential communications if the individual clearly states that the disclosure of all or part of the Protected Health Information could endanger the individual.

2. Key implementation steps taken by OMM:

   a. In general, current Medicaid procedures at the LDSS and State DOH level already allow for alternative means of communication.
   b. Recipients are routinely given the right to identify on WMS a mail-to address separate from the household address. Recipients will be informed of this option through the OMM Helpline when requested and by the OMM Privacy Coordinator.
   c. Recipients designate in writing when requested for PHI from OMM where they want it sent.
   d. For the Explanation of Medical Benefit system, the mail-to address from WMS (via MMIS) is used.
   e. Recipients will be informed in writing of these facts if they inquire about this right to OMM.
   f. The program will not communicate with the enrollee, unless phone conversation is initiated by the enrollee. Therefore no system to amend or update telephone communications is required if endangerment is alleged.

H. Recipient's Right to Amendment of their PHI (45 C.F.R § 526)

1. Summary: An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record:

   a. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
   b. Is not part of the designated record set;
   c. Would not be available for inspection under 45 CFR §,164.524; or
   d. Is accurate and complete.

2. Key implementation steps taken by OMM:

   a. OMM is not required to, and will not amend claim or encounter data, since the Department, or the LDSS, did not create the data. Other information will be reviewed and amended if deemed appropriate.

I. Accounting of Disclosures of Protected Health Information (45 C.F.R § 164.528)

1. Summary: An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures to carry out treatment, payment and health care operations and except for disclosures made pursuant to enrollee authorization.

2. Key implementation steps taken by OMM:

   a. OMM rarely discloses PHI outside the central administration of the Medicaid program. The only exception would be certain disclosures to courts, which will be maintained, filed and logged.

      1. If the recipient wants to know if his/her PHI was disclosed, OMM will ask the recipient to direct the request in writing to the OMM Privacy Coordinator. Upon receipt of the request, OMM will search its file of court-ordered disclosures of Medicaid claims data, inform the recipient by a form of the policy and the search results. This will be kept on file in OMM.
      2. Oral requests for accounting will not be accepted over the phone. There will be no tracking. The recipient will be sent the proper form to make such a request.

J. Complaint Process (45 C.F.R § 164.530)

1. Summary: A covered entity must provide a process for individuals to make complaints concerning the covered entity's HIPAA policies and procedures or its compliance with such policies and procedures.

   a. A covered entity must document all complaints received, and their disposition, if any.
   b. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart.

2. Key implementation steps taken by OMM:

   a. If the recipient files a complaint verbally or in writing that their privacy rights have been violated, OMM will send a copy of the DOH complaint form to the recipient, acknowledge its receipt, investigate, track with the DOH's Office of Human Rights Administration and inform the recipient of the resolution. The recipient will be informed that they may pursue the matter through the Federal Office of Civil Rights.

   b. OMM has provided training on the entities' policies and procedures to all members of the workforce likely to have access to protected health information. Each entity is required to provide training by the date on which this rule became applicable. After that date, each covered entity would have to provide training to new members of the workforce within a reasonable time after joining the entity.

   c. The OMM Privacy Coordinator must make sure that everyone in the OMM workforce has been trained.

   d. The OMM training materials have been shared with the LDSS who will assure that all workforce members are trained.

V. PROGRAM IMPLICATIONS:

1. It is recognized that no single HIPAA privacy implementation process could be described that would cover all LDSS because of their variations in size and operational processes. It was determined that a description of the procedures developed and implemented by OMM would remind the LDSS of steps that must be taken by them to meet their Medicaid HIPAA obligations. To insure that LDSS managers understand what policies and procedures they must establish to implement HIPAA in their offices, what follows is a description of OMM's HIPAA implementation steps. These are derived directly from the regulation: 45 CFR Parts 160 through 164.

2. These steps are also presented to help LDSS managers understand and ensure the confidentiality of Medicaid Confidential and other Protected Health Information (PHI) and to provide LDSS staff and their consultants with information to implement these policies and procedures. It is vital that LDSS review, update and implement, as needed, all existing policies and procedures, to ensure such information is not disclosed improperly.

VI. REQUIRED ACTION BY LDSS

Below are listed actions that OMM took to implement HIPAA. The Department realizes that variations exist in LDSS operations, but the LDSS must develop policies and procedures, if none exist, and review/revise existing policies and procedures, when appropriate to comply with the HIPAA regulation.

A. Designate a privacy officer

1. Local districts must assign a privacy person or liaison and inform James F. Botta. jfb04@health.state.ny.us (518) 473-4848.
2. The local privacy person will be the Medicaid point of contact for all privacy related issues, including dissemination of forms and training.

B. Notice of Privacy Practice

1. Local districts must print the Notice of Privacy Practices and maintain sufficient copies. Copies can be downloaded from the OMM HIPAA website: **http://www.health.state.ny.us/nysdoh/medicaid/hipaa/hipaamain.htm** .
2. Copies can also be ordered from the OTDA warehouse, LDSS should call (518) 402-0159, (518) 473-3132 or (518) 402-0164. Forms are also housed in the DOH Distribution Center, and can be obtained by calling (518) 486-9054.
3. Copies must be provided to the recipient at eligibility intake, as well as when any temporary card is created. Otherwise, the Notice will be mailed with the acceptance notice.
4. LDSS may develop their own Notice describing uses and disclosures of Medicaid information unique to their districts, OMM must review it for compliance with Title XIX regulations prior to use. Please send the proposed notice to James F. Botta, jfb04@health.state.ny.us or NYS Dept of Health, OMM, Rm. 2038, Corning Tower, Albany. NY, 12237.
5. If the LDSS has its own unique notice, it need not distribute the State's notice. If it distributes the State's notice, it is indicating to enrollees that it conforms in all respects to such notice.
6. Copies of the Notice of Privacy in English and Spanish are attached. (Attachment 4)

C. Recipients' Inquiries/Health Information Requests

1. The LDSS must identify/train staff responsible for county-specific inquiries/requests. Inquiries LDSS receives that concern OMM privacy policies may be referred to the OMM HIPAA Privacy Coordinator, James F. Botta jfb04@health.state.ny.us or NYS Dept. of Health, OMM, Rm. 2038, Corning Tower, Albany, NY, 12237.

2. While the OMM has established the procedures to respond to a recipient's privacy rights as described in the HIPAA regulation, LDSS must establish a process for ensuring individual requests for PHI or changes to PHI are properly addressed. In the local district offices, these will most likely be changes to Eligibility Data for the recipient.

3. LDSS staff must require a written request from the enrollee. Staff should verify that the address on the request matches the address on the Recipient Master File. A copy of the request annotated with the date of response must be kept on file.

4. The OMM Designated Record Set is mainly composed of all enrollment, claims and encounter history on the OMM/AFPP Datamart, which contains all recipients' billing and eligibility records (currently 10/96 forward). It is anticipated that this will generally satisfy a recipient's right to access PHI in MMIS since it is the complete record of PHI that OMM maintains. It is also recognized that the LDSS may have WMS information, local administrative claims data, or medical information used to determine eligibility. Recipients may pursue this information by requesting it through the LDSS. Requests for state held Medicaid information should be forwarded to James F. Botta, OMM Privacy Coordinator jfb04@health.state.ny.us. Mr. Botta will refer requests concerning LDSS held information to the LDSS contact person.

5. The OMM will search for Prior Approval records when requested by a recipient. Recipients may also pursue prior approval information by requesting it through the LDSS.

6. Requests received by OMM for information about a Fair Hearing will promptly be directed to the Office of Temporary Disability Assistance telephone number 518- 474-3265 in order to comply with HIPAA time frames. Recipients may also pursue Fair Hearing information by requesting it through the LDSS. Requests for Fair Hearing information should be directed to:

New York City area for regular Fair Hearing requests	212-417-6550
New York City area for emergency Fair Hearing requests	212-417-3614
New York City area to adjourn an existing Fair Hearing	212-417-3500
Buffalo area for all Fair Hearing transactions	716-852-4868
Rochester area for all Fair Hearing transactions	585-266-4868
Syracuse area for all Fair Hearing transactions	315-422-4868
Long Island area for all Fair Hearing transactions	516-739-4868
Albany area for all Fair Hearing transactions	518-474-8781
TTY access to Fair Hearings for the hearing impaired	877-502-6155

7. Inquiries related to Medicaid Managed Care or Family Health Plus Managed Care should be directed to Jennifer Dean, Acting Director of the Bureau of Inter-governmental Affairs, Office of Managed Care jjd03@health.state.ny.us (518) 486-9015.

D. Minimum Necessary

1. As required by HIPAA, LDSS must complete a functional analysis of staff job functions and need for access to Medicaid PHI. This analysis will serve as the basis for staff authentication and access to PHI. Use and release of Protected Health Information (PHI) must be kept to the minimum necessary to perform functions related to the administration of the program. As an example, a copy of the OMM Minimum Necessary guidelines used in OMM can be obtained from James F. Botta, OMM Privacy Coordinator jfb04@health.state.ny.us

E. Business Associates

1. The LDSS must identify all contracts, memorandums of understanding and data exchange applications covering the exchange of LDSS Medicaid PHI with outside entities. HIPAA compliant contract addendums must be sent to all parties with requirements for them to sign and notarize the agreement. Copies of an example may be obtained from James F. Botta, OMM Privacy Coordinator jfb04@health.state.ny.us

F. Authorization for Release of Protected Health Information for Use or Disclosure

1. Except as otherwise permitted or required by law or regulation, the LDSS may not use or disclose protected health information without a valid authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization. Copies of this form may be requested from James F. Botta, OMM Privacy Coordinator jfb04@health.state.ny.us
2. For requests from lawyers or legal guardians, or a recipient's family, the applicant must send a notarized authorization form that is HIPAA compliant (as per 45 CFR 164.508). The authorized request is good only for the specific request. (Attachment 5)
3. Valid requests from a court or requests that come under subpoena will be honored and the data will be released. Logging of such disclosures when required by HIPAA, must then occur.
4. See Attachment 5a. (Authorization For Release of Medicaid Protected Information)

G. Recipient's Right to Restrict or Limit certain Disclosures or Request Alternative Means of Communication

1. The LDSS must permit an individual to request that the covered program restrict or limit certain disclosures. The covered program does not have to agree. The Privacy Rule also allows individuals to request that communications by a covered program to the individual be made to the person at an alternative location, or by an alternative means, as long as the request is reasonable with respect to the administrative burden placed on the provider. Health plans must accommodate all reasonable requests for confidential communications if the individual clearly states that the disclosure of all or part of the Protected Health Information ("PHI") could endanger the individual. In general, current Medicaid procedures at the LDSS should allow for alternative means of communication on WMS.

H. Recipient's Right to Amendment of their PHI

1. Recipients are routinely given the right to identify on WMS a mail-to address separate from the household address.

2. Recipients designate in their request for PHI from LDSS where they want it sent.

   a. Recipients must be informed in writing by OMM of these facts if they inquire of OMM about this right.
   b. The recipient has the right to amend enrollment or eligibility records. If a recipient requests OMM to mail an amendment to their enrollment information, they will be referred to the LDSS. Amendment requests must be evaluated and appropriate action taken by the LDSS. The recipient will be notified by the LDSS if the request is not honored.

I. Accounting of Disclosures of Protected Health Information

1. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures to carry out treatment, payment and health care operations.

2. LDSS rarely discloses PHI outside the central administration of the Medicaid program. The only exception would be disclosures to courts, which must be maintained, filed and logged.

3. If the recipient wants to know if his/her PHI was disclosed, LDSS will ask the recipient to direct the request in writing to the Privacy Coordinator in LDSS. Upon receipt of the request, LDSS will search its file of court-ordered disclosures of Medicaid claims data, inform the recipient by a form of the policy and the search results. This must be kept on file in LDSS.

4. For oral requests for accounting responses made over the phone. There will be no tracking. The recipient will be sent the proper form to make such a request.

J. Complaint Process

1. The LDSS must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart. Implementation specification: documentation of complaints. A covered entity must document all complaints received, and their disposition, if any. Standard: sanctions: A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart.

2. If the recipient files a complaint verbally or in writing that their privacy rights have been violated, OMM will acknowledge its receipt, investigate and track it with the DOH's Office of Human Rights Administration and inform the recipient of the resolution.

3. The recipient will be informed by LDSS that they may pursue the matter through the Federal Office of Civil Rights.

K. Training

1. The LDSS HIPAA Coordinator is responsible for overseeing training on the entity's policies and procedures to all members of the workforce likely to have access to PHI. Each entity is required to provide initial training by the date on which this rule became applicable. After that date, each covered entity would have to provide training to new members of the workforce within a reasonable time after joining the entity.

2. Each LDSS staff member who has access to PHI and or Medicaid Confidential Data must review the training materials and sign a log sheet indicating they have been trained. The LDSS Personnel or Staff Development Coordinator must make sure that everyone in the workforce who has access to PHI has been trained.

3. The training materials have been shared with the LDSS who will assure that all new workforce members are trained.

4. LDSS are responsible for their own staff training. To support this, OMM mailed a copy of its training materials to LDSS in May 2003 and suggested that they could be supplemented with local HIPAA privacy procedures to assure that training requirements are met.

5. LDSS should follow the same procedures for training all Medicaid staff whether or not they have access to PHI. Other staff that has access to PHI should also be trained.

V. SYSTEMS IMPLICATIONS

The Directive contains no systems implications.

VII. ADDITONAL INFORMATION

The NYS DOH Contact person is

James F. Botta
NYS Dept. of Health/OMM
Corning Tower Bldg. Rm. 2038
Albany, NY 12237-0080
518-473-4848, or e-mail at jfb04@health.state.ny.us,

VIII. DATE OF IMPLEMENTATION – Effective Immediately

_____

Brian J. Wing
Deputy Commissioner
Office of Medicaid Management

ATTACHMENT 1

March 27, 2003

Dear Commissioner:

The Department of Health has determined that local social services districts are "covered entities" within the meaning of the Health Insurance Portability and Accountability Act (HIPAA). Covered entities include health care providers that bill electronically, clearinghouses and health plans. The Medicaid program is specifically named as a health plan in the federal HIPAA regulations.

The Department's determination that local districts are ''covered entities'' does not preclude each district from deciding for itself whether it is a ''covered entity'' under HIPAA. A number of local districts may already have reached that decision. Regardless, both the State and local districts are required to comply with all Medicaid confidentiality policies and procedures, including the HIPAA privacy obligations imposed on Medicaid as a ''health plan''. The Department has statutory responsibility to supervise the joint administration of the Medicaid program, but each entity needs to be accountable for breaches of privacy standards, without regard to "covered entity" status. This means each local district is responsible for enforcing its own privacy standards.

As detailed in the HIPAA sessions presented at the 2003 NYPWA Winter Conference, the Department of Health will work closely with local districts to provide support and guidance as we proceed with our HIPAA privacy compliance efforts. The Department has developed a number of privacy-related model forms that you may use. We distributed a number of these forms at the NYPWA conference including the Notice of Privacy Practices, Authorization for Release of Information, Business Associates Agreement and others. These forms are not intended to be legal advice, but rather, models that may be adopted by the local districts. In addition, the Department is developing Medicaid-specific HIPAA policies, procedures, minimum necessary guidelines, staff training plans, etc. We will provide you with these materials as they become available, along with ADMs detailing the Notice of Privacy Practices processes and descriptions of how the Department is proceeding with implementation of key HIPAA privacy provisions.

If you were unable to attend the NYPWA Conference, we will send you the material distributed at the Conference within the next week or so. If you have any questions related to this letter or any other HIPAA issue, please access the Department's website at www.health.state.ny.us/nysdoh/medicaid/hipaa/privacy.htm; or contact Mr. James Botta at (518) 473-4848, or e-mail at jfb04@health.state.ny.us; or Mr. Mario Tedesco at (518)257-4496, or e-mail at mxt07@health.state.ny.us.

Sincerely,

Kathryn Kuhmerker
Deputy Commissioner
Office of Medicaid Management

ATTACHMENT 2

(April 3, 2003)

Dear Commissioner:

The Privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) must be made operational by April 14, 2003. At the NYPWA Winter Conference, we spoke to you about the provisions that must be implemented by a covered entity, one of which is training. The Office of Medicaid Management (OMM) developed a PowerPoint presentation to train our staff. This training integrates material on existing Medicaid Title XIX confidentiality rules with the new HIPAA requirements.

In the spirit of cooperation, the training package is being made available to the local departments of social services for your information. The presentation is on the attached PowerPoint file, named OMM HIPAA Privacy Training.ppt. Please note that this presentation is only a starting point, since the HIPAA regulation requires that your agency expand upon this to train your staff on how the HIPAA regulation impacts your agency.

If you have any questions related to this training presentation, please contact Mr. James Botta, Office of Medicaid Management Privacy official, at 518-473-4848, or e-mail at jfb04@health.state.ny.us**.**

Sincerely,

Kathryn Kuhmerker
Deputy Commissioner
Office of Medicaid Management

ATTACHMENT 3

Use and Disclosure of Protected Health Information

Use, requests and disclosure of protected health information ("PHI") by the program are covered by this policy. PHI is information created or received by a health care provider, health plan, employer or health care clearinghouse, recorded in any form, e.g., written, oral or electronic. The information is the combination of identifiers and health information, i.e., information relating to the past, present or future physical or mental health of a person or to the condition or treatment of a person or to the payment for care. Other health information is also considered PHI when there is a reasonable basis to believe the information can be used to identify the person.

General Rule:

Only staff whose job functions require them to request, use or disclose PHI should be allowed to handle PHI. Staff whose job functions does not require them to request, use or disclose PHI should not be permitted to view such information. If job responsibilities change, or a special situation occurs requiring access to PHI by staff, supervisory review and approval must be sought to authorize a change for a particular job function.

Minimum Necessary:

Title XIX and HIPAA have virtually identical standards:

(A) A covered program/must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the disclosure or request.

(B) While OMM staffs have brand access to much PHI through the automated databases, it is responsibility of staff and managers to follow the minimum necessary policy.

(C) Federal regulations require the identification of routine and recurring requests and disclosures. General protocols can be used to establish minimum necessary adherence for such routine and recurring activity.

The covered program shall maintain a listing of routine and recurring requests

and disclosure by department or business process. [Covered programs should

select the following applicable initial listing purposes shall be considered routine

and recurring: payment and claims processing, treatment, referrals and

authorizations, case management, quality management, utilization management, program integrity, appeals and re-determinations, enrollment, billing and payment collection, eligibility determination, coordination of benefits, referrals, claims inquiry, quality review, transcription, audit, accreditation, licensing, program/business management, training, and legal services and other health care operations of the organization. PHI disclosed for these purposes will be limited to standard transaction content, or the information needed to enable a complete response for the particular business process.

(D) Federal regulations require covered units to have a policy and criteria for individual review and limitation of non-routine or non-recurring requests and disclosures.

The covered program will maintain a policy for case-by-case review on

appropriate requests and disclosures. Unit staff shall individually review all

requests and disclosures for actions that are not otherwise encompassed in the

implementation of section C above. Staff shall bring such matters to the program

privacy contact, which shall make a determination related to disclosure, in

consultation with the unit supervisor. Consideration shall be given to the

following criteria.

The purpose for which the PHI is needed and the importance of the request or disclosure.

1. Confirmation that the requests or disclosure is either for purposes of treatment, payment, healthcare operations or a regulatory exception.
2. The extent to which the request or disclosure would extend the number of persons with access to the protected health information.
3. The likelihood that further uses or disclosures of the protected health information could occur.
4. The amount of protected health information that would be requested or disclosed.
5. The potential to achieve substantially the same purpose with de-identified information.
6. The technology or methods available to limit the amount of protected health information requested or disclosed.
7. The cost of limiting the request or disclosure.
8. The adequacy of assurances that the PHI will be reasonably safeguarded.
9. Any other factors that the program believes are relevant to the specific determination.

Note: A disclosure may be presumed to be limited to the minimum necessary if the organization seeking disclosure states that (I) the PHI requested is the minimum necessary and (ii) the request is from a public official, a business associate, or a covered entity.

If the request and disclosure is considered to be routine and recurring, it will be added to the routine and recurring listing.

The program will maintain a current listing of routine and recurring requests and disclosures and will update and revise as appropriate to reflect current practices. and add more requests and disclosures as appropriate.]

Attachment 4

Notice of Privacy

Administrative Memorandum
And the Notice

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.
Commissioner
Dennis P. Whalen
Executive Deputy Commissioner

ADMINISTRATIVE DIRECTIVE

TRANSMITTAL: 03 OMM/ADM-3

TO: Commissioners of Social Services

DIVISION: Office of Medicaid Management

DATE: April 16, 2003

SUBJECT: Privacy Notice as required under the Health Insurance Portability & Accountability Act (HIPAA)

SUGGESTED DISTRIBUTION:	Medicaid Directors **Managed Care Coordinators**
CONTACT PERSON:	**Local District Liaison** **Upstate (518) 474 - 8216** **NYC (212) 268 - 6855**
ATTACHMENTS:	**Attachment I Privacy Notice (English)** **Attachment II Privacy Notice (Spanish)**

FILING REFERENCES

Previous ADMs/INFs	Releases Cancelled	Dept. Regs. Soc. Law & Other Legal Ref. .45 C.F.R §164.520…	Serv.Manual	Ref. Misc. Ref.	
Date: April 16, 2003					
Trans. No. 03 OMM/Adm-3					**Page No. 24**

I. PURPOSE

The purpose of this Office of Medicaid Management Administrative Directive (OMM/ADM) is to inform local departments of social services of the Privacy Notice that is required by Federal Regulation to be provided to Medicaid recipients.

II. BACKGROUND

HIPAA, the acronym for the Health Insurance Portability & Accountability Act of 1996 (Public Law 104-191), requires all covered programs to provide adequate notice to enrollees by April 14, 2003, and at least once every three years, of the uses and disclosures of protected health information (PHI) that may be made by the covered program. The privacy rule refers to the standards that protect "individually identifiable health information", which is any information that is generated or received by a health care provider, health plan, or health care clearinghouse; and identifies or may be used to identify an individual.

The Department of Health (DOH) and the local departments of social services (LDSS) which administer Medicaid, a covered program, must provide recipients of regular Medicaid, Medicaid Managed Care, Family Health Plus, and Child Health Plus A with information on how their PHI is used, disclosed and how they may access this information.

To fulfill the HIPAA requirement of adequate notice, DOH has developed a Privacy Notice.

III. PROGRAM IMPLICATIONS

A Privacy Notice has been drafted and will be mailed by DOH to Medicaid Heads of Household, which includes regular Medicaid, Family Health Plus, Medicaid Managed Care and Child Health Plus A in April 2003. Those enrolled in Child Health Plus B or the Family Planning Extension Program (FPEP) will not be sent this Notice, because the Medicaid program does not maintain their health information. These individuals should contact their Child Health Plus B or family planning provider with questions about their protected health information.

LDSS must use a Privacy Notice to provide new recipients of regular Medicaid, Medicaid Managed Care, Family Health Plus, and Child Health Plus A with information on how their PHI is used, disclosed and how they may access this information.

IV. REQUIRED ACTION

Beginning April 14, 2003, LDSS are required to include a Privacy Notice with each Medicaid acceptance notice sent to new and reopened regular Medicaid, Medicaid Managed Care, Family Health Plus, and Child Health Plus A cases. For cases initially granted presumptive eligibility, the HIPAA notice is required to be included with the notice of acceptance when the eligibility determination is made. For new Medicaid cases established by the Office of Mental Health (OMH) and the Office of Mental Retardation & Developmental Disabilities (OMRDD) the Privacy Notice should be sent to the same address/location as the notice of acceptance. A privacy notice is also required to be sent to individuals qualifying under the Qualified Medicare Beneficiary (QMB) Program. A privacy notice must also be sent to

Family Planning Benefit Program (FPBP) recipients. Mailings to FPBP recipients must use the applicant's mailing address in the Associated Name field of WMS (if one is provided) to ensure confidentiality.

Every three years the State will do a mass mailing to Medicaid Heads of Household, including regular Medicaid, Family Health Plus, Medicaid Managed Care and Child Health Plus A. The State is working on the most appropriate way to accomplish that task.

A copy of the Privacy Notice will be e-mailed to all LDSS' to provide district staff the opportunity to download and print copies of the Privacy Notice until an adequate supply is available. When printed, a supply will be sent to each district via regular mail. The notice is available in Spanish as well as in English. A copy of this Privacy Notice as well as routine updates on HIPAA will be posted on the NYS Department of Health web site at:
http://www.health.state.ny.us/nysdoh/medicaid/hipaa/hipaamain.htm

Local districts must use this approved Privacy Notice without modification unless this Department has granted approval for a local equivalent. The Department must review and approve any local equivalent Privacy Notice prior to use by the district to ensure that there are no discrepancies with DOH's approved Privacy Notice. Districts requesting to use a local equivalent Notice should send the Notice to the attention of:

James F. Botta
Medicaid Privacy Officer
Division of Policy & Program Guidance
Office of Medicaid Management
New York State Department of Health
Corning Tower, Room 2038, Empire State Plaza
Albany, New York 12237

The Privacy Notice includes phone numbers that Medicaid recipients or their representatives may call to make a request for privacy information or report a privacy problem or complaint. These numbers, 518-486-9057 or 1-800-541-2831, will be directed to the State Medicaid Help Line. As a single point of entry for Medicaid, Family Health Plus, Medicaid Managed Care and Child Health Plus A Privacy Notice related inquiries and questions, State Medicaid Help Line staff will handle requests for basic information and refer complaints and other requests to the designated State office. The designated State office will triage requests and, redirect questions/inquiries to LDSS offices when appropriate. Normal district procedures should be followed on calls referred to their office.

Medicaid recipients or their representatives may also report a complaint to the federal Department of Health and Human Services' Office for Civil Rights at 212-264-3313 or 1-800-368-1019.

Medicaid enrolled providers will be informed about the provisions of the HIPAA Privacy Notice in upcoming issues of the Medicaid Update. Issues of the Medicaid Update are available on the DOH website at:
http://www.health.state.ny.us/nysdoh/mancare/omm/main.htm

V. SYSTEMS IMPLICATIONS

None

VI. ADDITIONAL INFORMATION

Both English and Spanish versions of the Privacy Notice are attached to this directive. When available, an initial supply of the Privacy Notice will be sent to each district.

Copies of the Privacy Notice may be ordered through any of the following means:

1) by mail, with the request addressed to:

New York State Department of Health
11 Fourth Avenue
Rensselaer, New York 12144

2) by fax, to (518) 465-0432.

3) by e-mail, to b0019w@albnydh2.health.state.ny.us

An Administrative Directive providing additional guidelines relative to HIPAA will be issued.

EFFECTIVE DATE

Use of the Privacy Notice is required for new and reopened regular Medicaid, Medicaid Managed Care, Family Health Plus, and Child Health Plus A cases effective April 14, 2003.

Kathryn Kuhmerker
Deputy Commissioner
Office of Medicaid Management

Notice Of Privacy

1. English Version

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

Privacy Notice

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Effective April 14, 2003, the New York Medicaid program must tell you how the Department uses or shares we use, share, and protect your health information. The New York Medicaid program includes regular Medicaid, Medicaid Managed Care, Family Health Plus, and Child Health Plus A. The program is administered by the

New York State Department of Health and the Local Departments of Social Services.
and the Division of Health Care Access, New York City Department of Health operate the Medicaid, Family Health Plus and Child Health Plus A programs. The New York State Department of Health operates the Child Health Plus B program.

Your Health Information is Private.
We are required to keep your information private, share your information only when we need to, and follow the privacy practices in this notice. We must make special efforts to protect the names of people who get HIV/AIDS or drug and alcohol services.

What Health Information Does the New York Medicaid Program Have?
When you applied for Medicaid, Family Health Plus, or Child Health Plus A, you may have provided us with information about your health. When your doctors, clinics, hospitals, managed care plans and other health care providers send in claims for payment, we also get information about your health, treatments and medications.

If you enrolled in Child Health Plus B, the New York Medicaid program does not have your health information. You should contact your Child Health Plus B plan with questions about your health information.

How Does the New York Medicaid Program, Family Health Plus and Child Health Plus A&B Programs Does the Department of Health Use and Share Your Health Information?

We must share your health information when:

- ***You or your representative requests your health information.***
- ***Government agencies request the information as allowed by law such as audits.*** The Department
- ***The law requires us the Department to share your information.***

In your Medicaid application, you gave the New York Medicaid program the right to use and share your health information to pay for your health care and operate the program. For example, we use and share your information to:

- ***Pay your doctor, hospital, and/or other health care provider bills.*** The Department
- ***Make sure you receive quality health care and that all the rules and laws have been followed.*** We may review your health information to determine whether you received the correct medical procedure or health care equipment.
- The Department ***Contact you about important medical information or changes in your health benefits.***
- ***Make sure you are enrolled in the right health program***. The Department
- ***Collect payment from other insurance companies.***

We may also use and share your health information under limited circumstances to: The Department

- ***Study health care.*** We may look at the health information of many consumers to find ways to provide better health care. The Department
- ***Prevent or respond to serious health or safety problems for you or your community as allowed by federal and state law.***

We must have your written permission to use or share your health information for any purpose not mentioned in this notice.

What Are Your Rights?

You or your representative has the right to:

- Get a paper copy of this notice.
- See or get a copy of your health information. If your request is denied, you have the right to review the denial.
- Ask to change your health information. The Department will look at all requests, but cannot change bills sent by your doctor, clinic, hospital or other health care provider.
- Ask to limit how the Department uses and shares we use and share your information. The Department will look at all requests, but does not have to agree to do what you ask.
- Ask the Department to contact you regarding your health information in different ways (for example, you can ask us to send your mail to a different address).
- Ask for special forms that you sign permitting the Department to share your health information with whomever you choose. You can take back your permission from the Department at any time, as long as the information has not already been shared.
- Get a list of those who received your health information. This list will not include health information requested by you or your representative, information used to operate the New York Medicaid program or information given out for law enforcement purposes.

Child Health Plus A&B or Family Health Plus or Child Health Plus A&B programs.

See the New York State Department of Health Department's w web site for a copy of this notice: www.health.state.ny.us.

1. For more privacy information, to make a request or to report a privacy problem/complaint*, please contact the Medicaid Help Line Office at: (518) 486-9057 or 1-800-541-2831. TTY users should call 1-800-662-1220. The Help Line will direct your calls to the correct state and local department of social services office.

2. You may also report a complaint* to: The Office for Civil Rights, Department of Health and Human Services, Jacob Javits Federal Building, 26 Federal Plaza, Suite 3312, New York, New York 10278; (Telephone) (212) 264-3313 or 1-800-368-1019; (Fax) (212) 264-3039; or (TDD) (212) 264-2355.

******You will not be penalized for filing a complaint*.

The Department If we may change the information in this notice, We will send you a new notice and post a new notice on the New York State Department of Health Department's web site.

2. Spanish Version

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
Commissioner

Dennis P. Whalen
Executive Deputy

Notificación de Privacidad
ESTA CARTA DESCRIBE CÓOMO SE PUEDE USAR Y COMPARTIR DIVULGAR SU INFORMACIONINFORMACIÓN MEDICAMÉDICA CONFIDENCIAL, Y TAMBIENTAMBIÉN CÓOMO PUEDE USTED OBTENER ACCESO A ESA INFORMACIONINFORMACIÓN. . POR FAVOR ANALICE LEA CON CUIDADO ESTA NOTIFICACIÓNINFORMACION, YA QUE NECESITAMOS SU PERMISO POR ESCRITO PARA PODER USAR Y COMPARTIR SU INFORMACION MEDICA.

A partir del 14 de abril de 2003, el progamaprograma de salud de Medicaid de Nueva York tendratendrá que informarle a usted cóomo utiliza, comparte y protege su Informacioninformación Medicamédica. El programa de Medicaid de Nueva York incluye: Medicaid regular, Medicaid Manager Care, Family Health Plus y Child Health Plus A. El programa es administrado por el Departamento de Salud Pública del Estado de Nueva York y por los Departamentos Locales de Servicios Sociales.

Su informacioninformación Medicamédica es siempre Cconfidencial.
Nosotros debemos mantenerla confidencialcuidarla, solamente podemos compartirla sólo cuando seaes absolutamente necesario, y debemos observar todas las reglas de privacidad definidas en esta notificacionnotificación. . Nosotros tambienTambién estamos obligados adebemos proteger los nombres de las personas que reciben servicios medicosrelacionados con eldel VIH/SIDA, o con el abuso de drogas o alcohol.

¿?Queé clase de informacioninformación medicamédica maneja el programa de los diferente servicios del Medicaid de Nueva York?
Cuando usted solicitó cualquiera de los servicios de Medicaid, Family Health Plus, Child Health Plus Aalguno de los differente servicios del Medicaid, usted pudo habernos entregadonos dio informacioninformación acerca de su salud., y tambien nos dio el derecho de usar y compartir su informacion medica. Cuando sus doctores, clínicas, hospitales, planes de salud y Mas tarde losotros proveedores de servicios medicosmédicos nos envianenvían las cuentas para el pago, también recibimos junto con su nueva informacioninformación sobre su salud, tratamientos y medicamentosmedica.

En el programa Medicaid estan incluidos no solamente el Medicaid regular, sino tambien Medicaid Managed Care, Family Health Plus, y Child Health Plus A. Todos estos programas son administrados por el Departamento de Salud Publica de Nueva York, y el Departamento Servicios Sociales en cada ciudad. Nosotros tenemos solament la informacion de servicios Medicaid que usted ha recibido, pero Ssi usted estaá inscrito en el Child Health Plus B, nosotros no tenemos su ninguna informacioninformación médica.acerca de esos servicios, y s Si tiene alguna pregunta sobre su desea informacioninformación médica, por favor comuniquesecomuníquese con su plan Child Health Plus Bellos.

¿Coómo utiliza y comparte su información médica puede el programa Medicaid de Nueva York utilizar y compartir su informacion medica?

Nosotros solamente podemos compartir su informacioninformación medicamédica cuando:

- ***ustedUsted o, su representante solicita su información médica, o.***
- ***Llas agencies del gobierno lo solicitan la información, tal y como lo es permiteido por la ley en casos de auditorias.***
- ***La ley exige que compartamos su información.***

En su solicitud de Medicaid, usted le dio al programa de Medicaid de Nueva York el derecho a usar y compartir su información médica para pagar por su atención médica y la debida operación del programa. Por ejemplo, nosotros usamos y compartimos su información para:

- ***Pagarle a su doctor, hospital, y/o pagar otras cuentas de proveedores de atención médica.***
- *, o para pagar sus servicios medicos, y tambien para* ***aAsegurarnos que usted ha recibido un buen servicio medico de buena calidad, y que todas las regulaciones de la ley hayan sido cumplidas.*** Nosotros podremos revisar su información médica para determinar si recibió los procedimientos médicos correctos o para verificar que el equipo usado en su tratamiento haya sido eles correcto, que todas las regulaciones de la ley hayan sido cumplidas, y tambien para nosotros porder manejar el programa de servicios publicos.
- ***Contactarle a usted para darle información médica importante o informarle acerca de cambios a sus beneficios de salud.***
- ***Asegurarnos que usted está inscrito en el programa de salud adecuado para sus necesidades.***
- ***Cobrar a otras compañías de seguro.***

También podremos

Tambien podemos usarusar y compartir su informacioninformación medicamédica, para:

- darle a usted informacion medica importante, o informarle acerca de cambios de beneficios de salud, para asegurarnos que usted esta inscrito en el programa de salud adecuado para sus necesidades, para nosotros poder cobrar a otras companias de seguro, para ***revisarRevisar la atención médica***. informacionPodremos revisar la información médica de varias personas paray buscar mejores formas de proveer atencionatención medicamédica.
- ***, para pPrevenir o responder a problemas serios de salud o de seguridad, no solamente para usted, sino tambientambién para toda su comunidad, tal yasi como lo es permitenido por las leyes del gobierno Federal y de el Estado.***

Para cualquier otro caso que no haya sido mencionado en esta carta, nosotros debemos obtener de usted un permiso escrito para poder usar y compartir su

información médica., o en cualquier otro caso que no haya sido mencionado en esta carta.

¿Cuáles son sus?e dDerechos?

Usted o su representante tiene siguientedderecho a:

- Derecho de Recibir una copia por escrito de esta notificaciónacerca de los requisitos de **La Informacion Medica** Confidencial.
- Derecho deVer o recibir una copia de su informacioninformación medicamédica, y si esto es negado, tiene el derecho de a revisar y verificar el por queé fue negado.
- Usted puede sSolicitar el cambio de su informacioninformación medicamédica. . Nosotros revisaremos todas las solicitudes de cambios, pero no podemos modificar las cuentas enviadas por su doctor, clínica, hospital o cualquier otro proveedor de sus servicios medicosmédicos.
- Usted puede pPedir que limitemos el modola forma como usamos y compartimos su nformacioninformación medicamédica. . Nosotros revisaremos todas las peticiones, pero no siempre estaremos de acuerdo con cada persona.
- Usted puede sSolicitar que cambiemos el modo en que nos comuniquemoscamos con usted de diferentes maneras, (por ejemplo, usted nos puede pedir que le enviemos su informacioninformación medicamédica a otra direccióndirección).
- Usted puede dDecidir con quién podemos compartir su informacioninformación medicamédica. , y usted tambienTambién podrá puede removeranular estesu permiso en cualquier momento, siempre y cuandoque la informacioninformación no haya sido compartida todaviatodavía.
- Usted puede oObtener una lista de las personas que han recibido su informacioninformación medicamédica. . Esta lista no no debe incluirá informacioninformación médica solicitada por usted o su representaterepresentante, o informacioninformación que haya sidoes utilizada para la operaciónel manejo del progamaprograma de Medicaid de Nueva York, o informacioninformación que haya sido divulgada necesaria para el cumplimento de la ley.

- **Si es posible, vVisite la paginapágina del Internet del Departamento de Salud PublicaPública del Estado de Nueva York para obtener una copias de esta notificaciónlas nuevas regulaciones. : www.health.state.ny.us.**

1. **Para obtener más información sobre asuntos de privacidadSi necesita mas informacion, para hacer una solicitud o si desea reportar un problema o queja* , , por favor comuniquesecomuníquese con el Medicaid Help Line llamando alen: : (518)- 486-9057 o al, 1-800-541-2831. Las personas que usan servicios de teletipo (TTY) pueden llamar al, o 1-800-662-1220 para las personas que usan servicios de teletipo (TTY). . Su llamada seraserá transferida a la correspondiente oficina del estatal y do, o a la oficina local de Sservicios Socialessociales correspondiente. .**

- 2. Usted tambientambién podrá se puede presentar una queja acomunicar con: lLa Oficina de Derechos Civiles, Departamento de Servicios Sociales y Salud Publica, en la siguiente direccion:

Office of Civil Rights, Department of Health and Human Services,
Jacob Javits Federal Building,
26 Federal Plaza, Suite 3312, New York, NY 10278;.

Telefono(Teléfono): (212) 264-3313, oó 1-800-368-1019;, o al (FaxAX numero) (212) 264-3039,; o al (TDD –DispositvoDispositivo de Telecomunicaciones para Sordos) (212) 264-2355.

**** Le aseguramos que uUsted no seraserá penalizado por presentar una queja.***

Si nosotros modificamos esta informacioninformación, le enviaremos una nueva notificación, la cual se lo informaremos en una carta, y tambien lotambién publicaremos en la paginapágina webWeb del Departamento de Salud Pública del Estado de Nueva York.

ATTACHMENT 5

NEW YORK STATE DEPARTMENT OF HEALTH OFFICE OF MEDICAID MANAGEMENT
Enrollee/Patient Request for Specific Medicaid Protected Health Information

Federal regulations permit you to request a specific designated record set. We will try to meet your request. If you wish to request this information, please complete the following:

Name:_____

Client Identification Number (CIN): _____

Date of Birth:_____

Street Address: _____

City: _____

State: _____ Zip Code: _____

Phone Number: _____

Dates of records requested From: _____ To: _____

Reason:
_____
_____

_____ _____
Enrollee/Patient Signature Date

Forward form to:

Claim Detail Unit
Address: NYS Dept of Health/ OMM Corning Tower, Rm 2038 Albany, NY 12237
Phone Number: (518) 473-4848

ATTACHMENT 5 A

AUTHORIZATION FOR RELEASE OF MEDICAID PROTECTED INFORMATION FROM THE NEW YORK STATE DEPARTMENT OF HEALTH, OFFICE OF MEDICAID MANAGEMENT TO A THIRD PARTY OTHER THAN A MEDICAID ENROLLEE/PATIENT

Enrollee/Client Name: _____ Client Identification Number (CIN): _____

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the organization authorized to receive the information is not a health plan, health care provider or clearinghouse, the released information may no longer be protected by federal privacy regulations, except that an enrollee/patient may be prohibited from redisclosing substance abuse information under the federal substance abuse confidentiality requirements. State law governs the release of HIV/AIDS information and you may request a list of persons authorized to re-release HIV/AIDS related information. Authorizations for the release of HIV/AIDS data must comply with the requirements of Article 27-F of the Public Health Law. Authorizations for the release of alcohol and substance abuse records must comply with the requirements of 42 C.F.R. Part2.

Persons/organizations authorized to receive or use the information:

Name _____

Address _____City

_____State_____ Zip_____

Phone Number _____

1. Purpose of the use/disclosure:

   _____

2. Will the person/program requesting the authorization receive financial or in-kind compensation
   in exchange for using or disclosing the health information described above? Yes _____ No _____

3. I understand that my health care and the payments for my health care will not be affected if I do not sign this form except in some situations when information is needed for payment, enrollment, etc.

4. I understand, with few exceptions, that I may see and copy the information described on this form if I ask for it, and that I may get a copy of this form after I sign it.

5. I may revoke this authorization at any time by notifying the Department of Health in writing, but if I do it will not have any affect on any actions they took before they received the revocation.
   This authorization will expire in 30 days of receipt in this office.

Signature of Medicaid Enrollee _____
Date:_____

State of New York }

} ss..

County of ---------- }

On this _____day of _____, 20__, before me personally came and appeared _____, to me known to be the individual described in, and who executed this Medicaid records authorization in my presence and duly acknowledged to me that (s) he executed the same.

_____

Notary Public

ATTACHMENT 6

Federal Health Insurance Portability and Accountability Act (HIPAA)
Business Associate Appendix

I. Definitions:

(a) □.Business Associate□ shall mean the CONTRACTOR.

(b) □.Covered Program□ shall mean the STATE.

(c) Other terms used, but not otherwise defined, in this agreement shall have the same meaning as those terms in the federal Health Insurance Portability and Accountability Act of 1996 (□HIPAA□) and its implementing regulations, including those at 45 CFR Parts 160 and 164.

II. Obligations and Activities of the Business Associate:

(a) The Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by this Agreement or as required by law.

(b) The Business Associate agrees to use the appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(c) The Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of Protected Health Information by the Business Associate in violation of the requirements of this Agreement.

(d) The Business Associate agrees to report to the Covered Program, any use or disclosure of the Protected Health Information not provided for by this Agreement, as soon as reasonably practicable of which it becomes aware.

(e) The Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the Business Associate on behalf of the Covered Program agrees to the same restrictions and conditions that apply through this Agreement to the Business Associate with respect to such information.

(f) The Business Associate agrees to provide access, at the request of the Covered Program, and in the time and manner designated by the Covered Program, to Protected Health Information in a Designated Record Set, to the Covered Program or, as directed by the Covered Program, to an Individual in order to meet the requirements under 45 CFR 164.524, if the business associate has protected health information in a designated record set.

(g) The Business Associate agrees to make amendment(s) to Protected Health Information in a designated record set that the Covered Program directs or agrees to pursuant to 45 CFR 164.526 at the

request of the Covered Program or an Individual, and in the time and manner designated by Covered Program, if the business associate has protected health information in a designated record set.

(h) The Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Program available to the Covered Program, or to the Secretary of Health and Human Services, in a time and manner designated by the Covered Program or the Secretary, for purposes of the Secretary determining the Covered Program's compliance with the Privacy Rule.

(i) The Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Program to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. No such disclosures shall be made without the prior written permission of the New York State Department of Health, Office of Medicaid Management.

(j) The Business Associate agrees to provide to the Covered Program or an Individual, in time and manner designated by Covered Program, information collected in accordance with this Agreement, to permit Covered Program to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

III. Permitted Uses and Disclosures by Business Associate

(a) General Use and Disclosure Provisions

Except as otherwise limited in this Agreement, the Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, the Covered Program as specified in the Agreement to which this is an addendum, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Program.

(b) Specific Use and Disclosure Provisions:

(1) Except as otherwise limited in this Agreement, and only with the prior written permission of the Department the Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(2) The Business Associate may use Protected Health Information to report violations of law to appropriate federal and State authorities, consistent with 45 CFR .164.502(j)(1).

IV. Obligations of Covered Program

Provisions for the Covered Program To Inform the Business Associate of Privacy Practices and Restrictions

(a) The Covered Program shall notify the Business Associate of any limitation(s) in its notice of privacy practices of the Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of Protected Health Information.

(b) The Covered Program shall notify the Business Associate of any changes in, or revocation of, permission by the Individual to use or disclose Protected Health Information, to the extent that such changes may affect the Business Associate's use or disclosure of Protected Health Information.

(c) The Covered Program shall notify the Business Associate of any restriction to the use or disclosure of Protected Health Information that the Covered Program has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of Protected Health Information.

V. Permissible Requests by Covered Program

The Covered Program shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Program. Such Medicaid Protected Health Data may not be in any way permanently combined with other information gained from other sources.

VI. Term and Termination

(a) ***Term.*** Effective April 14, 2003 in the event of termination for any reason, all of the Protected Health Information provided by Covered Program to Business Associate, or created or received by Business Associate on behalf of Covered Program, shall be destroyed or returned to Covered Program, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in The Agreement.

(b) ***Termination for Cause.*** Upon the Covered Program's knowledge of a material breach by Business Associate, Covered Program may provide an opportunity for the Business Associate to cure the breach and end the violation or may terminate this Agreement and the master Agreement if the Business Associate does not cure the breach and end the violation within the time specified by Covered Program, or the Covered Program may immediately terminate this Agreement and the master Agreement if the Business Associate has breached a material term of this Agreement and cure is not possible.

(c) ***Effect of Termination.***

(1) Except as provided in paragraph (c)(2) below, upon termination of this Agreement, for any reason, the Business Associate shall return or destroy all Protected Health Information received from the Covered Program, or created or received by the Business

Associate on behalf of the Covered Program. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that the Business Associate determines that returning or destroying the Protected Health Information is infeasible, the Business Associate shall provide to the Covered Program notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, the Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

VII. Violations

(a) It is further agreed that any violation of this agreement may cause irreparable harm to the State; therefore the State may seek any other remedy, including an injunction or specific performance for such harm, without bond, security or necessity of demonstrating actual damages.

(b) The business associate shall indemnify and hold the State harmless against all claims and costs resulting from acts/omissions of the business associate in connection with the business associate's obligations under this agreement.

Miscellaneous

(a) ***Regulatory References.*** A reference in this Agreement to a section in the HIPAA Privacy Rule means the section as in effect or as amended, and for which compliance is required.
(b) ***Amendment.*** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Program to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.
(c) ***Survival.*** The respective rights and obligations of the Business Associate under Section VI of this Agreement shall survive the termination of this Agreement.
(d) ***Interpretation.*** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Program to comply with the HIPAA Privacy Rule.
(e) If anything in this agreement conflicts with a provision of any other agreement on this matter, this agreement is controlling.
(6) ***HIV/AIDS.*** If HIV/AIDS information is to be disclosed under this agreement, the business associate acknowledges that it has been informed of the confidentiality requirements of Public Health Law Article 27-F.

Name_____

Signature_____

Date_____

Name_____

Signature_____

Date_____

Attachment 7
Health Insurance Portability &Accountability
Act of 1996--HIPAA Privacy Rules

Signed into law on August 21,1996,HIPAA contained provisions for the administrative simplification of the health care industry. HIPAA set a national standard for the electronic transfer of administrative and financial health care data between all payers, all health plans and most health care providers; this standard replaces the many non-standard formats now being used nationwide. HI PAA ’s Privacy Rule gives patients rights to access their health records and to know who else has accessed them, restricts disclosure of their health information to the minimum needed for the intended purpose, establishes new criminal and civil sanctions for improper use or disclosure, and sets new requirements for access to records by researchers and others. Compliance with HI PAA ’s Privacy Rule was generally required by April 14,2003.

HIPAA Programs Within SDOH

Plans: pay for health care (e.g. insurance, managed care)
• Medicaid (includes Medicaid Managed Care, Family Health Plus, Child Health Plus –A, PRI ,FPEB,HI V –SNP) • Child Health Plus • EPIC • HIV-Uninsured Care Programs • Cystic Fibrosis • Indian Health Providers: provide care &bill electronically (physicians, hospitals, etc.) • Helen Hayes (hospital &nursing home) • Veterans Homes (4) • Lead Poisoning/Trace Elements Laboratory Clearinghouses: process health information (e.g., billing agents) • Health Facilities Management • Early Intervention (also a plan)

Health Information Protected under HIPAA (45 CFR § § 160.103,164.501)

Protected Health Information (PHI)= Health Information +Individually Identifying Information PHI is information (e.g. for eligibility, enrollment, care, payment) that: • is created or received by a covered program; • relates to past, present or future health condition, provision of care, and or payment, AND • identifies the individual.

Minimum Necessary Rule (45 CFR §§ 164.530,164.502) • Staff can access only the PHI needed to do their jobs. • All staff, volunteers, students, researchers, consultants, with access to PHI, must be trained in, and comply with, HIV PAA privacy regulations.• LEARN THE LIMITS ON PHI USE FOR YOUR JOB.

Business Associates (45 CFR § 164.502) • HIPAA's privacy requirements apply, by contract, to a program ’s Business Associates. (i.e., entities that perform a function for the program AND have access to PHI). • Programs must enter into agreements with these Business Associates (e.g. consultants). • PHI is limited to what is minimally necessary for them to do their jobs.

Privacy Notice (45 CFR § 164.520)

• Plans must send Notices to all enrollees by 4/14/03.After 4/14/03, to new enrollees; then, once every 3 years. • Providers must make a good faith effort to share Notices with all patients at the first encounter after 4/14/03 &get an acknowledgement of receipt from patients. • Notices must be posted on websites. • GET A COPY OF YOUR PROGRAM ’S NOTICE.

Authorization to Use or Disclose PHI (45 CFR § § 164.508,164.512)

• A person ’s authorization is needed, except when their PHI is used or disclosed: for treatment, payment or health care operations. *However, NYS law requires providers to get consent for external disclosures.* • to the individual; as required by law or judicial order; for public health; for reporting abuse/neglect/violence; for health oversight; etc. Valid authorization must include: description of information disclosed, purpose of disclosure, recipient &disclosing party, expiration date/event and signature +date.

Verify Identity of Person Seeking PHI • Generally, anyone seeking PHI, including the individual, needs to be able to prove who they are. • Staff must verify identity of requestor by following their program ’s verification procedures. • Individual: Ask for some combination of address, SS#, birth

date, maiden name, MA-ID#, etc. Verbal verification is OK if allowed by program ’s process. • Anyone Else: Generally, ask for written authority, e.g. subpoena, government ID, written authorization, contract, MOU, etc.
HIPAA Program Staff • Know SDOH ’s Privacy Official.• Know your program ’s HI PAA Privacy Contact Person. • Know who, in your program, is responsible for receiving & processing PHI -related requests and complaints.• If you have access to PHI ,make sure that you are trained on your program ’s HI PAA-specific policies &procedures.
Links www.hhs.gov.ocr.hipaa (Office of Civil Rights) www.cms.hhs.gov.hipaa (CMS); www.hipaadvisory.com (HIPAA regulations); www.health.state.ny.us.nysdoh.hipaa (Preemption Analysis). The federal HIPAA information & complaint number:
1-800-368-1019

INDIVIDUAL PRIVACY RIGHTS 45 CFR §§ 164.522 to 164.528
HI PAA grants a number of rights to individuals regarding their own PHI .These are: • Right to access their PHI • Right to an accounting of their PHI disclosures • Right to amend their PHI • Right to request confidential communications • Right to request further restrictions on the use & disclosure of their PHI. Generally, these requests need to be submitted in writing to your program ’s Privacy Contact. (NOTE: Standard program communications with enrollees and patients are routine operations, not the exercise of an individual ’s rights, e.g. claim status or coverage inquiries, scheduling appointments or billing inquiries).
Designated Record Set (DRS) (45 CFR § 164.501) • Providers ’ DRS include medical and billing records +PHI used to make decisions about an individual. • Plans ’ DRS include enrollment, payment, claims adjudication and case or medical management record systems +PHI used to make decisions about individuals. • KNOW YOUR PROGRAM ’S DESIGNATED RECORD SET.
Restrict or Limit Disclosures (45 CFR § 164.522) • Individuals have a right to ask a program not to share a part, or all, of their PHI .• Programs are not required to agree to a restriction. • If a restriction is agreed to, the program and its Business Associates must honor it, unless it is terminated or an emergency occurs. **Access PHI (45 CFR § 164.524)** • Individuals have a right to look at, and/or get a copy of, their PHI in a designated record set. HIPAA says fees must be reasonable. In NYS, programs can charge fees up to $.75/page for copies of medical records. • Programs may deny access to PHI in some cases (e.g. psychotherapy notes, legal actions, research, labs).• Programs may limit access to PHI in other cases (e.g., substantial harm to other, life/safety of self and others). • Plans have 30 days to respond to access requests;
providers have 10 days (NYS law).
Confidential Communications
(45 CFR § 164.522)
• Individuals have a right to ask that letters be sent to an alternate address, that another phone number be used, etc. • Providers must grant these requests when reasonable. • Plans must grant these requests when reasonable and when individuals state that not doing so would place them in danger.
Amend PHI (45 CFR § 164.526) • Individuals have a right to request an amendment to their PHI in a designated record set. • Programs must: • inform individuals when changes are approved/denied; • add or notate amendment —or denial —in record;• date/initial any change (do not delete original PHI);• notify Business Associates &others who rely on this information; • respond to a request within 60 days, with one 30-day extension if person is notified in writing.
Account for PHI Disclosures (45 CFR § 164.528)
• Individuals have a right to ask for an accounting of certain disclosures for prior 6 years. NO accounting is necessary for disclosures for payment, treatment, healthcare operations or based upon a signed authorization.

Programs must document: date, description, purpose &copy of disclosures; name &title of person/organization requesting disclosure; • actual materials disclosed. • Programs must provide the accounting within 60 days, with one 30-day extension if person is notified in writing.1st accounting in a 12-month period is free; programs may charge for additional ones.
COMPLAINTS-VIOLATIONS OF PRIVACY RIGHTS (45 CFR § 164.530) • Individuals have the right to complain to the: Office for Civil Rights US Department of Health &Human Services 212-264-3313 Jacob Javitz Federal Building 212-264-3039 (fax) 6 Federal Plaza, Suite 3312 212-264-2355 (TDD) New York, NY 10278 1-800-368-1019 (toll free) • Complaints may also be submitted in writing to your supervisor, your program ’s Privacy Contact or SDOH ’s Privacy Official.
Safeguarding PHI (45 CFR § 164.530) Staff must safeguard —within reason —PHI from any intentional or unintentional use or disclosure. This applies to information shared between programs and Business Associates. • Be careful with whom, where, you discuss PHI . • When discussing PHI on the phone, verify caller ’s identity.• Do not leave PHI on voice mail or on answering machines. • Whenever possible, do not include PHI in emails.• Keep written PHI in a safe place (don ’t leave it in the open, don ’t throw it in the trash, keep it in a locked place, shred it). • Protect your workstation (lock it, protect IDs, secure your passwords &change them frequently. • Never let anyone else use your account. • Minimize storage of PHI on your hard drive.
Violations & Penalties • The most severe penalties are when a person WILLFULLY discloses PHI (e.g., in return for money). • Fines up to $250,000 &10 years in jail, are possible. • Lesser penalties will also apply (e.g., counseling, disciplinary action, reprimand, job loss). • Retaliation against a person reporting a violation, or cooperating in an investigation, is prohibited.,

ATTACHMENT 1

March 27, 2003

Dear Commissioner:

The Department of Health has determined that local social services districts are "covered entities" within the meaning of the Health Insurance Portability and Accountability Act (HIPAA). Covered entities include health care providers that bill electronically, clearinghouses and health plans. The Medicaid program is specifically named as a health plan in the federal HIPAA regulations.

The Department's determination that local districts are ''covered entities'' does not preclude each district from deciding for itself whether it is a ''covered entity'' under HIPAA. A number of local districts may already have reached that decision. Regardless, both the State and local districts are required to comply with all Medicaid confidentiality policies and procedures, including the HIPAA privacy obligations imposed on Medicaid as a ''health plan''. The Department has statutory responsibility to supervise the joint administration of the Medicaid program, but each entity needs to be accountable for breaches of privacy standards, without regard to "covered entity" status. This means each local district is responsible for enforcing its own privacy standards.

As detailed in the HIPAA sessions presented at the 2003 NYPWA Winter Conference, the Department of Health will work closely with local districts to provide support and guidance as we proceed with our HIPAA privacy compliance efforts. The Department has developed a number of privacy-related model forms that you may use. We distributed a number of these forms at the NYPWA conference including the Notice of Privacy Practices, Authorization for Release of Information, Business Associates Agreement and others. These forms are not intended to be legal advice, but rather, models that may be adopted by the local districts. In addition, the Department is developing Medicaid-specific HIPAA policies, procedures, minimum necessary guidelines, staff training plans, etc. We will provide you with these materials as they become available, along with ADMs detailing the Notice of Privacy Practices processes and descriptions of how the Department is proceeding with implementation of key HIPAA privacy provisions.

If you were unable to attend the NYPWA Conference, we will send you the material distributed at the Conference within the next week or so. If you have any questions related to this letter or any other HIPAA issue, please access the Department's website at www.health.state.ny.us/nysdoh/medicaid/hipaa/privacy.htm; or contact Mr. James Botta at (518) 473-4848, or e-mail at jfb04@health.state.ny.us; or Mr. Mario Tedesco at (518)257-4496, or e-mail at mxt07@health.state.ny.us.

Sincerely,

Kathryn Kuhmerker
Deputy Commissioner
Office of Medicaid Management

ATTACHMENT 2

(April 3, 2003)

Dear Commissioner:

The Privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) must be made operational by April 14, 2003. At the NYPWA Winter Conference, we spoke to you about the provisions that must be implemented by a covered entity, one of which is training. The Office of Medicaid Management (OMM) developed a PowerPoint presentation to train our staff. This training integrates material on existing Medicaid Title XIX confidentiality rules with the new HIPAA requirements.

In the spirit of cooperation, the training package is being made available to the local departments of social services for your information. The presentation is on the attached PowerPoint file, named OMM HIPAA Privacy Training.ppt. Please note that this presentation is only a starting point, since the HIPAA regulation requires that your agency expand upon this to train your staff on how the HIPAA regulation impacts your agency.

If you have any questions related to this training presentation, please contact Mr. James Botta, Office of Medicaid Management Privacy official, at 518-473-4848, or e-mail at jfb04@health.state.ny.us.

Sincerely,

Kathryn Kuhmerker
Deputy Commissioner
Office of Medicaid Management

ATTACHMENT 3

Use and Disclosure of Protected Health Information

Use, requests and disclosure of protected health information ("PHI") by the program are covered by this policy. PHI is information created or received by a health care provider, health plan, employer or health care clearinghouse, recorded in any form, e.g., written, oral or electronic. The information is the combination of identifiers and health information, i.e., information relating to the past, present or future physical or mental health of a person or to the condition or treatment of a person or to the payment for care. Other health information is also considered PHI when there is a reasonable basis to believe the information can be used to identify the person.

General Rule:

Only staff whose job functions require them to request, use or disclose PHI should be allowed to handle PHI. Staff whose job functions does not require them to request, use or disclose PHI should not be permitted to view such information. If job responsibilities change, or a special situation occurs requiring access to PHI by staff, supervisory review and approval must be sought to authorize a change for a particular job function.

Minimum Necessary:

Title XIX and HIPAA have virtually identical standards:

(A) A covered program/must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the disclosure or request.

(B) While OMM staffs have brand access to much PHI through the automated databases, it is responsibility of staff and managers to follow the minimum necessary policy.

(C) Federal regulations require the identification of routine and recurring requests and disclosures. General protocols can be used to establish minimum necessary adherence for such routine and recurring activity.

The covered program shall maintain a listing of routine and recurring requests and disclosure by department or business process. [Covered programs should select the following applicable initial listing purposes shall be considered routine and recurring: payment and claims processing, treatment, referrals and authorizations, case management, quality management, utilization management, program integrity, appeals and re-determinations, enrollment, billing and payment collection, eligibility determination, coordination of benefits, referrals, claims inquiry, quality review, transcription, audit, accreditation, licensing, program/business management, training, and legal services and other health care operations of the organization. PHI disclosed for these purposes will be limited to standard transaction content, or the information needed to enable a complete response for the particular business process.

(D) Federal regulations require covered units to have a policy and criteria for individual review and limitation of non-routine or non-recurring requests and disclosures.

The covered program will maintain a policy for case-by-case review on appropriate requests and disclosures. Unit staff shall individually review all requests and disclosures for actions that are not otherwise encompassed in the implementation of section C above. Staff shall bring such matters to the program privacy contact, which shall make a determination related to disclosure, in consultation with the unit supervisor. Consideration shall be given to the following criteria.

The purpose for which the PHI is needed and the importance of the request or disclosure.

1. Confirmation that the requests or disclosure is either for purposes of treatment, payment, healthcare operations or a regulatory exception.
2. The extent to which the request or disclosure would extend the number of persons with access to the protected health information.
3. The likelihood that further uses or disclosures of the protected health information could occur.
4. The amount of protected health information that would be requested or disclosed.
5. The potential to achieve substantially the same purpose with de-identified information.
6. The technology or methods available to limit the amount of protected health information requested or disclosed.
7. The cost of limiting the request or disclosure.
8. The adequacy of assurances that the PHI will be reasonably safeguarded.
9. Any other factors that the program believes are relevant to the specific determination.

Note: A disclosure may be presumed to be limited to the minimum necessary if the organization seeking disclosure states that (I) the PHI requested is the minimum necessary and (ii) the request is from a public official, a business associate, or a covered entity.

If the request and disclosure is considered to be routine and recurring, it will be added to the routine and recurring listing.

The program will maintain a current listing of routine and recurring requests and disclosures and will update and revise as appropriate to reflect current practices. and add more requests and disclosures as appropriate.]

Privacy Notice

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The New York Medicaid program must tell you how we use, share, and protect your health information. The New York Medicaid program includes regular Medicaid, Medicaid Managed Care, Family Health Plus, and Child Health Plus A. The program is administered by the New York State Department of Health and the Local Departments of Social Services.

Your Health Information is Private.
We are required to keep your information private, share your information only when we need to, and follow the privacy practices in this notice. We must make special efforts to protect the names of people who get HIV/AIDS or drug and alcohol services.

What Health Information Does the New York Medicaid Program Have?
When you applied for Medicaid, Family Health Plus, or Child Health Plus A, you may have provided us with information about your health. When your doctors, clinics, hospitals, Medicaid managed care plans and Medicaid Advantage and other health care providers send in claims for payment, we also get information about your health, treatments and medications.

If you enrolled in Child Health Plus B, the New York Medicaid program does not have your health information. You should contact your Child Health Plus B plan with questions about your health information.

How Does the New York Medicaid Program Use and Share Your Health Information?

We must share your health information when:

- ***You or your representative requests your health information.***
- ***Government agencies request the information as allowed by law such as audits.***
- ***The law requires us to share your information.***

In your Medicaid application, you gave the New York Medicaid program the right to use and share your health information to pay for your health care and operate the program. For example, we use and share your information to:

- ***Pay your doctor, hospital, and/or other health care provider bills***.
- ***Make sure you receive quality health care and that all the rules and laws have been followed***.

We may review your health information to determine whether you received the correct medical procedure or health care equipment.

- ***Contact you about important medical information or changes in your health benefits***.
- ***Make sure you are enrolled in the right health program***.
- ***Collect payment from other insurance companies.***

Eligibility in Medicare Part D or other insurance program which might be more economical to you.

We may also use and share your health information under limited circumstances to:

***Study health care*:** We may look at the health information of many consumers to find ways to provide better health care.

- ***Prevent or respond to serious health or safety problems for you or your community as allowed by federal and state law.***

We must have your written permission to use or share your health information for any purpose not mentioned in this notice.

What Are Your Rights?
You or your representative have the right to:

- Get a paper copy of this notice.
- See or get a copy of your health information. If your request is denied, you have the right to review the denial.
- Ask to change your health information. We will look at all requests, but cannot change bills sent by your doctor, clinic, hospital or other health care provider.
- Ask to limit how we use and share your information. We will look at all requests, but do not have to agree to do what you ask.
- Ask us to contact you regarding your health information in different ways (for example, you can ask us to send your mail to a different address).
- Ask for special forms that you sign permitting us to share your health information with whomever you choose. You can take back your permission at any time, as long as the information has not already been shared.
- Get a list of those who received your health information. This list will not include health information requested by you or your representative, information used to operate the New York Medicaid program or information given out for law enforcement purposes.

See the New York State Department of Health web site for a copy of this notice:
www.health.state.ny.us.

1. **For more privacy information, to make a request or to report a privacy problem/complaint * , please contact the Medicaid Help Line Office at: (518) 486-9057 or 1-800-541-2831. TTY users should call 1-800-662-1220. The Help Line will direct your calls to the correct state and local department of social services office.**
2. You may also report a complaint* to: The Office for Civil Rights, Department of Health and Human Services, Jacob Javits Federal Building, 26 Federal Plaza, Suite 3312, New York, New York 10278; (Telephone) (212) 264-3313 or 1-800-368-1019; (Fax) (212) 264-3039; or (TDD) (212) 264-2355.

*** You will not be penalized for filing a complaint.**

If we change the information in this notice, we will send you a new notice and post a new notice on the New York State Department of Health web site.

Disclaimer Privacy Policy Help

Revised: February2006

Notificación de Privacidad

ESTA CARTA DESCRIBE CÓMO SE PUEDE USAR Y DIVULGAR SU INFORMACIÓN MÉDICA CONFIDENCIAL Y CÓMO USTED PUEDE OBTENER ESA MISMA INFORMACIÓN. LÉALA ATENTAMENTE.

El programa de salud Medicaid del Estado de Nueva York debe informarle cómo utiliza, comparte y protege su información médica. Los siguientes seguros médicos forman parte del programa de Medicaid del Estado de Nueva York: Medicaid regular, Programa de Cuidados Administrados de Medicaid, Family Health Plus y Child Health Plus A. El programa es administrado por el Departamento de Salud del Estado de Nueva York y por los departamentos locales de servicios sociales.

Su información médica es confidencial.
Es nuestra obligación el mantener su información enteramente confidencial, compartirla sólo cuando sea absolutamente necesario, y acatar las reglas de privacidad definidas en esta notificación. También, se toman medidas especiales para proteger la identidad de las personas que reciben servicios relacionados con el VIH / SIDA, o con el abuso de drogas o alcohol.

¿Qué clase de información médica maneja el programa de Medicaid de Nueva York?
Cuando usted solicitó los servicios de Medicaid, Family Health Plus o Child Health Plus A, pudo haber entregado información acerca de su salud. Cuando sus médicos, clínicas, hospitales, planes de salud de Cuidados Administrados de Medicaid, Medicaid Advantage, y otros profesionales de servicios médicos envían cobros, también se recibe información sobre su salud, tratamientos y medicamentos recibidos.

Si usted está inscrito en Child Health Plus B, el programa de salud de Medicaid no tiene su información médica. Si tiene preguntas al respecto, comuníquese con el plan de salud Child Health Plus B.

¿Cómo utiliza y comparte su información médica el programa Medicaid de Nueva York?

Debemos compartir información médica en los siguientes casos:

- ***Cuando usted o su representante lo solicitan***
- ***Cuando una agencia gubernamental lo solicita, según lo estipulado por ley, como en el caso de las auditorias***
- ***Cuando lo autoriza la ley.***

En su solicitud de Medicaid, usted le dio al programa de Medicaid de Nueva York el derecho a usar y compartir su información médica con objeto de pagar cuentas por su atención médica y administración del programa. Por ejemplo, se usa y comparte su información con los siguientes propósitos:

- ***Para pagarle a su médico, hospital, y/o pagar otras cuentas a profesionales de atención médica.***
- ***Para asegurarnos de que usted ha recibido un servicio médico de calidad y que todas las reglas y leyes han sido cumplidas.***

Se podrá revisar su información médica para determinar si recibió los procedimientos médicos correctos o para verificar que el equipo usado en su tratamiento haya sido el correcto.

- ***Para comunicarnos con usted y darle información médica importante o informarle acerca de cambios en sus beneficios de salud.***
- ***Para estar seguros de que usted está inscrito en el programa de salud adecuado según sus necesidades.***
- ***Para cobrar a otras compañías de seguro.***

Se podrá revisar su información médica para determinar si reúne los requisitos de Medicare Parte D, o de otro programa de seguro que quizás sea más económico.

Además, se puede usar y compartir su información médica, en ciertas circunstancias tales como:

***Estudios sobre servicios y atención de salud*:** Se examina la información médica de muchos consumidores con miras de implementar mejoras en el sistema de salud.

- ***Prevenir o responder a problemas serios de salud o de su integridad física y la del resto de la población, tal y como lo estipulan las leyes federales y estatales.***

En todo otro caso, no mencionado en esta carta, se deberá obtener su permiso por escrito con objeto de usar y compartir su información médica.

¿Cuáles son sus derechos?
Usted o su representante tiene derecho a:

- Recibir una copia de esta notificación.
- Ver o recibir una copia de su información médica; y si esto es negado, tiene derecho a a saber el porqué de dicha negación.
- Solicitar cambios en su información médica. Examinaremos toda solicitud de cambios, sin embargo, no se pueden modificar las cuentas sometidas por su médico, clínica, hospital o profesional de servicios médicos.
- Solicitar límites en cuanto a cómo se usa y comparte su información médica. Examinaremos su petición, sin embargo, no necesariamente estaremos de acuerdo con lo que usted solicita.
- Solicitar que nos comuniquemos con usted de diferentes maneras (por ejemplo, puede solicitar que enviemos su correspondencia a otra dirección).
- Solicitar un permiso especial, por medio del cual, con su firma, usted nos autoriza a revelar su información médica a la persona que usted elige. Puede anular este permiso en cualquier momento, siempre y cuando la información no haya sido todavía revelada.
- Solicitar una lista de las personas que han recibido su información médica. La lista no incluirá información médica solicitada por usted o su representante, información que haya sido utilizada con propósitos de administrar el programa Medicaid de Nueva York, o información que haya sido divulgada en cumplimento de la ley.

Si desea una copia de esta notificación, obténgala en la página de internet del Departamento de Salud del Estado de Nueva York : www.health.state.ny.us.

1. **Si desea más información sobre asuntos de privacidad, someter una solicitud o reportar un problema o queja*, comuníquese con la Línea de Ayuda de Medicaid al: (518) 486-9057 o al 1-800-541-2831. Usuarios de sistema teletipo (TTY): 1-800-662-1220. Le conectaremos con la oficina correspondiente de servicios sociales a nivel estatal o local.**
2. También, puede presentar una queja* ante la siguiente oficina: *The Office for Civil Rights, Department of Health and Human Services, Jacob Javits Federal Building, 26 Federal Plaza, Suite 3312, New York, NY 10278.* (Teléfono) (212) 264-3313 ó 1-800-368-1019 (Fax) (212) 264-3039; usuarios de TDD llamen al: (212) 264-2355.

*** No se le impondrá una sanción por presentar una queja.**

Si se modifica la información en la presente notificación, se le enviará una nueva notificación. La nueva notificación también se publicará en la página web del Departamento de Salud del Estado de Nueva York.

Actualizado: febrero 2006

NEW YORK STATE DEPARTMENT OF HEALTH OFFICE OF MEDICAID MANAGEMENT
Enrollee/Patient Request for Specific Medicaid Protected Health Information

Federal regulations permit you to request a specific designated record set. We will try to meet your request. If you wish to request this information, please complete the following:

Name:_____

Client Identification Number (CIN): _____

Date of Birth:_____

Street Address: _____

City: _____

State: _____ Zip Code: _____

Phone Number: _____

Dates of records requested From: _____ To: _____

Reason:
_____
_____

_____ _____
Enrollee/Patient Signature Date

Forward form to:

Claim Detail Unit
Address: NYS Dept of Health/ OMM Corning Tower, Rm 2038 Albany, NY 12237
Phone Number: (518) 473-4848

ATTACHMENT 5 A

AUTHORIZATION FOR RELEASE OF MEDICAID PROTECTED INFORMATION FROM THE NEW YORK STATE DEPARTMENT OF HEALTH, OFFICE OF MEDICAID MANAGEMENT TO A THIRD PARTY OTHER THAN A MEDICAID ENROLLEE/PATIENT

Enrollee/Client Name: _____ Client Identification Number (CIN): _____

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the organization authorized to receive the information is not a health plan, health care provider or clearinghouse, the released information may no longer be protected by federal privacy regulations, except that an enrollee/patient may be prohibited from redisclosing substance abuse information under the federal substance abuse confidentiality requirements. State law governs the release of HIV/AIDS information and you may request a list of persons authorized to re-release HIV/AIDS related information. Authorizations for the release of HIV/AIDS data must comply with the requirements of Article 27-F of the Public Health Law. Authorizations for the release of alcohol and substance abuse records must comply with the requirements of 42 C.F.R. Part2.

Persons/organizations authorized to receive or use the information:

Name _____

Address _____City _____State_____

Zip_____

Phone Number _____

1. Purpose of the use/disclosure:
   _____
2. Will the person/program requesting the authorization receive financial or in-kind compensation in exchange for using or disclosing the health information described above? Yes _____ No _____
3. I understand that my health care and the payments for my health care will not be affected if I do not sign this form except in some situations when information is needed for payment, enrollment, etc.
4. I understand, with few exceptions, that I may see and copy the information described on this form if I ask for it, and that I may get a copy of this form after I sign it.
5. I may revoke this authorization at any time by notifying the Department of Health in writing, but if I do it will not have any affect on any actions they took before they received the revocation. This authorization will expire in 30 days of receipt in this office.

Signature of Medicaid Enrollee _____
Date:_____

State of New York }
} ss
County of ---------- }

On this _____day of _____, 20__, before me personally came and appeared _____, to me known to be the individual described in, and who executed this Medicaid records authorization in my presence and duly acknowledged to me that (s) he executed the same.

_____ Notary Public

Federal Health Insurance Portability and Accountability Act (HIPAA) Business Associate Appendix

I. Definitions:

(a) "Business Associate" shall mean the CONTRACTOR.

(b) "Covered Program" shall mean the STATE.

(c) Other terms used, but not otherwise defined, in this agreement shall have the same meaning as those terms in the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, including those at 45 CFR Parts 160 and 164.

II. Obligations and Activities of the Business Associate:

(a) The Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by this Agreement or as required by law.

(b) The Business Associate agrees to use the appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(c) The Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of Protected Health Information by the Business Associate in violation of the requirements of this Agreement.

(d) The Business Associate agrees to report to the Covered Program, any use or disclosure of the Protected Health Information not provided for by this Agreement, as soon as reasonably practicable of which it becomes aware.

(e) The Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the Business Associate on behalf of the Covered Program agrees to the same restrictions and conditions that apply through this Agreement to the Business Associate with respect to such information.

(f) The Business Associate agrees to provide access, at the request of the Covered Program, and in the time and manner designated by the Covered Program, to Protected Health Information in a Designated Record Set, to the Covered Program or, as directed by the Covered Program, to an Individual in order to meet the requirements under 45 CFR 164.524, if the business associate has protected health information in a designated record set.

(g) The Business Associate agrees to make amendment(s) to Protected Health Information in a designated record set that the Covered Program directs or agrees to pursuant to 45 CFR 164.526 at the request of the Covered Program or an Individual, and in the time and manner designated by Covered Program, if the business associate has protected health information in a designated record set.

(h) The Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Program available to the Covered Program, or to the Secretary of Health and Human Services, in a time and manner designated by the Covered Program or the Secretary, for purposes of the Secretary determining the Covered Program's compliance with the Privacy Rule.

(i) The Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Program to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. No such disclosures shall be made without the prior written permission of the New York State Department of Health, Office of Medicaid Management.

(j) The Business Associate agrees to provide to the Covered Program or an Individual, in time and manner designated by Covered Program, information collected in accordance with this Agreement, to permit Covered Program to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

III. Permitted Uses and Disclosures by Business Associate

(a) General Use and Disclosure Provisions

Except as otherwise limited in this Agreement, the Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, the Covered Program as specified in the Agreement to which this is an addendum, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Program.

(b) Specific Use and Disclosure Provisions:

(1) Except as otherwise limited in this Agreement, and only with the prior written permission of the Department the Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(2) The Business Associate may use Protected Health Information to report violations of law to appropriate federal and State authorities, consistent with 45 CFR 164.502(j)(1).

IV. Obligations of Covered Program

Provisions for the Covered Program To Inform the Business Associate of Privacy Practices and Restrictions

(a) The Covered Program shall notify the Business Associate of any limitation(s) in its notice of privacy practices of the Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of Protected Health Information.

(b) The Covered Program shall notify the Business Associate of any changes in, or revocation of, permission by the Individual to use or disclose Protected Health Information, to the extent that such changes may affect the Business Associate's use or disclosure of Protected Health Information.

(c) The Covered Program shall notify the Business Associate of any restriction to the use or disclosure of Protected Health Information that the Covered Program has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of Protected Health Information.

V. Permissible Requests by Covered Program

The Covered Program shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Program. Such Medicaid Protected Health Data may not be in any way permanently combined with other information gained from other sources.

VI. Term and Termination

(a) *Term.* Effective April 14, 2003 in the event of termination for any reason, all of the Protected Health Information provided by Covered Program to Business Associate, or created or received by Business Associate on behalf of Covered Program, shall be destroyed or returned to Covered Program, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in The Agreement.

(b) *Termination for Cause.* Upon the Covered Program's knowledge of a material breach by Business Associate, Covered Program may provide an opportunity for the Business Associate to cure the breach and end the violation or may terminate this Agreement and the master Agreement if the Business Associate does not cure the breach and end the violation within the time specified by Covered Program, or the Covered Program may immediately terminate this Agreement and the master Agreement if the Business Associate has breached a material term of this Agreement and cure is not possible.

(c) *Effect of Termination.*

(1) Except as provided in paragraph (c)(2) below, upon termination of this Agreement, for any reason, the Business Associate shall return or destroy all Protected Health Information received from the Covered Program, or created or received by the Business Associate on behalf of the Covered Program. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that the Business Associate determines that returning or destroying the Protected Health Information is infeasible, the Business Associate shall provide to the Covered Program notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, the Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

VII. Violations

(a) It is further agreed that any violation of this agreement may cause irreparable harm to the State; therefore the State may seek any other remedy, including an injunction or specific performance for such harm, without bond, security or necessity of demonstrating actual damages.

(b) The business associate shall indemnify and hold the State harmless against all claims and costs resulting from acts/omissions of the business associate in connection with the business associate's obligations under this agreement.

Miscellaneous

(a) *Regulatory References*. A reference in this Agreement to a section in the HIPAA Privacy Rule means the section as in effect or as amended, and for which compliance is required.

(b) *Amendment*. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Program to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.

(c) *Survival.* The respective rights and obligations of the Business Associate under Section VI of this Agreement shall survive the termination of this Agreement.

(d) *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Program to comply with the HIPAA Privacy Rule.

(e) If anything in this agreement conflicts with a provision of any other agreement on this matter, this agreement is controlling.

(6) *HIV/AIDS*. If HIV/AIDS information is to be disclosed under this agreement, the business associate acknowledges that it has been informed of the confidentiality requirements of Public Health Law Article 27-F.

Name_____

Signature_____

Date_____

Name_____

Signature_____

Date_____

Health Insurance Portability &Accountability Act of 1996--HIPAA Privacy Rules

Signed into law on August 21,1996,HIPAA contained provisions for the administrative simplification of the health care industry. HIPAA set a national standard for the electronic transfer of administrative and financial health care data between all payers, all health plans and most health care providers; this standard replaces the many non-standard formats now being used nationwide. HI PAA 's Privacy Rule gives patients rights to access their health records and to know who else has accessed them, restricts disclosure of their health information to the minimum needed for the intended purpose, establishes new criminal and civil sanctions for improper use or disclosure, and sets new requirements for access to records by researchers and others. Compliance with HI PAA 's Privacy Rule was generally required by April 14,2003.

HIPAA Programs Within SDOH

Plans: pay for health care (e.g. insurance, managed care)

• Medicaid (includes Medicaid Managed Care, Family Health Plus, Child Health Plus -A, PRI ,FPEB,HI V -SNP) • Child Health Plus • EPIC • HIV-Uninsured Care Programs • Cystic Fibrosis • Indian Health Providers: provide care &bill electronically (physicians, hospitals, etc.) • Helen Hayes (hospital &nursing home) • Veterans Homes (4) • Lead Poisoning/Trace Elements Laboratory Clearinghouses: process health information (e.g., billing agents) • Health Facilities Management • Early Intervention (also a plan)

Health Information Protected under HIPAA (45 CFR § § 160.103,164.501)

Protected Health Information (PHI)= Health Information +Individually Identifying Information PHI is information (e.g. for eligibility, enrollment, care, payment) that: • is created or received by a covered program; • relates to past, present or future health condition, provision of care, and or payment, AND • identifies the individual.

Minimum Necessary Rule (45 CFR §§ 164.530,164.502) • Staff can access only the PHI needed to do their jobs. • All staff, volunteers, students, researchers, consultants, with access to PHI, must be trained in, and comply with, HIV PAA privacy regulations.• LEARN THE LIMITS ON PHI USE FOR YOUR JOB.

Business Associates (45 CFR § 164.502) • HIPAA's privacy requirements apply, by contract, to a program 's Business Associates. (i.e., entities that perform a function for the program AND have access to PHI). • Programs must enter into agreements with these Business Associates (e.g. consultants). • PHI is limited to what is minimally necessary for them to do their jobs.

Privacy Notice (45 CFR § 164.520)

• Plans must send Notices to all enrollees by 4/14/03.After 4/14/03, to new enrollees; then, once every 3 years. • Providers must make a good faith effort to share Notices with all patients at the first encounter after 4/14/03 &get an acknowledgement of receipt from patients. • Notices must be posted on websites. • GET A COPY OF YOUR PROGRAM 'S NOTICE.

Authorization to Use or Disclose PHI (45 CFR § § 164.508,164.512)

• A person 's authorization is needed, except when their PHI is used or disclosed: for treatment, payment or health care operations. *However, NYS law requires providers to get consent for external disclosures.* • to the individual; as required by law or judicial order; for public health; for reporting abuse/neglect/violence; for health oversight; etc. Valid authorization must include: description of information disclosed, purpose of disclosure, recipient &disclosing party, expiration date/event and signature +date.

Verify Identity of Person Seeking PHI • Generally, anyone seeking PHI, including the individual, needs to be able to prove who they are. • Staff must verify identity of requestor by following their program 's verification procedures. • Individual: Ask for some combination of address, SS#, birth date, maiden name, MA-ID#, etc. Verbal verification is OK if allowed by program 's process. • Anyone Else: Generally, ask for written authority, e.g. subpoena, government ID, written authorization, contract, MOU, etc.

HIPAA Program Staff • Know SDOH 's Privacy Official.• Know your program 's HI PAA Privacy Contact Person. • Know who, in your program, is responsible for receiving & processing PHI -related requests and complaints.• If you have access to PHI ,make sure that you are trained on your program 's HI PAA-specific policies & procedures.

Links www.hhs.gov.ocr.hipaa (Office of Civil Rights) www.cms.hhs.gov.hipaa (CMS); www.hipaadvisory.com (HIPAA regulations); www.health.state.ny.us.nysdoh.hipaa (Preemption Analysis). The federal HIPAA information & complaint number: 1-800-368-1019

INDIVIDUAL PRIVACY RIGHTS 45 CFR §§ 164.522 to 164.528

HI PAA grants a number of rights to individuals regarding their own PHI .These are: • Right to access their PHI • Right to an accounting of their PHI disclosures • Right to amend their PHI • Right to request confidential communications • Right to request further restrictions on the use & disclosure of their PHI. Generally, these requests need to be submitted in writing to your program 's Privacy Contact. (NOTE: Standard program communications with enrollees and patients are routine operations, not the exercise of an individual 's rights, e.g. claim status or coverage inquiries, scheduling appointments or billing inquiries).

Designated Record Set (DRS) (45 CFR § 164.501) • Providers ' DRS include medical and billing records +PHI used to make decisions about an individual. • Plans ' DRS include enrollment, payment, claims adjudication and case or medical management record systems +PHI used to make decisions about individuals. • KNOW YOUR PROGRAM 'S DESIGNATED RECORD SET.

Restrict or Limit Disclosures (45 CFR § 164.522) • Individuals have a right to ask a program not to share a part, or all, of their PHI .• Programs are not required to agree to a restriction. • If a restriction is agreed to, the program and its Business Associates must honor it, unless it is terminated or an emergency occurs. **Access PHI (45 CFR § 164.524)** • Individuals have a right to look at, and/or get a copy of, their PHI in a designated record set. HIPAA says fees must be reasonable. In NYS, programs can charge fees up to $.75/page for copies of medical records. • Programs may deny access to PHI in some cases (e.g. psychotherapy notes, legal actions, research, labs).• Programs may limit access to PHI in other cases (e.g., substantial harm to other, life/safety of self and others). • Plans have 30 days to respond to access requests; providers have 10 days (NYS law).

Confidential Communications (45 CFR § 164.522)

• Individuals have a right to ask that letters be sent to an alternate address, that another phone number be used, etc. • Providers must grant these requests when reasonable. • Plans must grant these requests when reasonable and when individuals state that not doing so would place them in danger.

Amend PHI (45 CFR § 164.526) • Individuals have a right to request an amendment to their PHI in a designated record set. • Programs must: • inform individuals when changes are approved/denied; • add or notate amendment —or denial —in record;• date/initial any change (do not delete original PHI);• notify Business Associates &others who rely on this information; • respond to a request within 60 days, with one 30-day extension if person is notified in writing.

Account for PHI Disclosures (45 CFR § 164.528)

• Individuals have a right to ask for an accounting of certain disclosures for prior 6 years. NO accounting is necessary for disclosures for payment, treatment, healthcare operations or based upon a signed authorization. Programs must document: date, description, purpose &copy of disclosures; name &title of person/organization requesting disclosure; • actual materials disclosed. • Programs must provide the accounting within 60 days, with one 30-day extension if person is notified in writing.1st accounting in a 12-month period is free; programs may charge for additional ones.

COMPLAINTS-VIOLATIONS OF PRIVACY RIGHTS (45 CFR § 164.530) • Individuals have the right to complain to the: Office for Civil Rights US Department of Health &Human Services 212-264-3313 Jacob Javitz Federal Building 212-264-3039 (fax) 6 Federal Plaza, Suite 3312 212-264-2355 (TDD) New York, NY 10278 1-800-368-1019 (toll free) • Complaints may also be submitted in writing to your supervisor, your program 's Privacy Contact or SDOH 's Privacy Official.

Safeguarding PHI (45 CFR § 164.530) Staff must safeguard —within reason —PHI from any intentional or unintentional use or disclosure. This applies to information shared between programs and Business Associates. • Be careful with whom, where, you discuss PHI . • When discussing PHI on the phone, verify caller ’s identity.• Do not leave PHI on voice mail or on answering machines. • Whenever possible, do not include PHI in emails.• Keep written PHI in a safe place (don ’t leave it in the open, don ’t throw it in the trash, keep it in a locked place, shred it). • Protect your workstation (lock it, protect IDs, secure your passwords &change them frequently. • Never let anyone else use your account. • Minimize storage of PHI on your hard drive. **Violations & Penalties** • The most severe penalties are when a person WILLFULLY discloses PHI (e.g., in return for money). • Fines up to $250,000 &10 years in jail, are possible. • Lesser penalties will also apply (e.g., counseling, disciplinary action, reprimand, job loss). • Retaliation against a person reporting a violation, or cooperating in an investigation, is prohibited.