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.