PRIVACY POLICY MANUAL

TABLE OF CONTENTS

PRIVACY POLICY

April 2003

Revision Dates: June 2010
April 2013
September 2013

1. INTRODUCTION:

1.1 Background.

In 1996, the federal Health Insurance Portability and Accountability Act (HIPAA) was signed into law as PL 104-191. Its primary purpose was to protect health insurance coverage for workers and their families when they change or lose their jobs. However, in recognition of the fact that this new protection would impose additional administrative burdens on health care providers, plans, and clearinghouses, a section entitled "Administrative Simplification" was included in the law that is specifically designed to reduce the administrative burden associated with the transfer of health information between enterprises, and, more generally, to increase the efficiency and cost-effectiveness of the health care system in the United States. This approach is intended to accelerate the move from paper-based exchanges to electronic transactions through the establishment of uniform standards.

However, in enacting this legislation, Congress also acknowledged that electronic transmission of health care data in order to achieve these efficiencies could result in a loss of confidentiality of that data. Accordingly, it directed the federal Department of Health and Human Services (HHS) to develop standards and regulations to enhance the protection of confidentiality, hereafter referred to as the "HIPAA Privacy Regulations"[1].

In April of 2001, regulations were promulgated by HHS. which generally prohibit a "Covered Entity" from using or disclosing and individual's protected health information except as otherwise permitted or required by the rules[2]. Amendments to these regulations were finalized and adopted in August, 2002. A "Covered Entity" was required to be in compliance with the HIPAA Privacy Regulations by April, 2003.

Subsequently, in 2009, the American Recovery and Reinvestment Act of 2009 was enacted as an economic stimulus vehicle. Title XIII of this Act includes the Health Information Technology for Economic and Clinical Health Act (HITECH), primarily to provide funding for electronic health records and related activities. Subtitle D of the HITECH Act reinforces HIPAA and provides additional legal protections, in anticipation of increased use of electronic systems for healthcare purposes. In January of 2013, the Department of Health and Human Services issued a "final ruling" on HIPAA and HITECH that clarified a number of provisions in the laws. Effective March 26, 2013, this "Omnibus Rule" requires "covered entities" and their Business Associates to be in compliance with the revisions by September 23, 2013.

The New York State Office of Mental Health has determined that it is a "Covered Entity" for purposes of the HIPAA Privacy Regulations[3]. As such, it is required to establish and implement this policy as part of its compliance strategy.

---

[1]It should be noted that the HIPAA Privacy Regulations are part of a broader series of standards issued by HHS under the Administrative Simplification provisions of the HIPAA statute. Others include final Standards for Electronic Transactions, as well as for data security, electronic signatures, and health plan and provider identifiers.

[2]45 CFR Parts 160 and 164: Standards for Privacy of Individually Identifiable Health Information.

[3]See Appendix 1 for official designation of OMH as a "Covered Entity."

The HIPAA Privacy Regulations establish a foundation of federal protections for the privacy of protected health information. However, it is important to note that these regulations do not replace federal, state, or other law that grants individuals even greater privacy protections.

The concept of confidentiality of medical information, and particularly mental health information, is not new to the New York State Office of Mental Health. In fact, it has long been recognized that the very fact of one's mental illness, and receiving professional help for such illness, can, if generally revealed, cause a person to be subjected to prejudice and stigma in one's professional and personal life. It has also been recognized that effective and lasting psychiatric therapy can take place only in an environment of privacy and trust in which the patient knows that his/her statements will be held in confidence.

Notwithstanding the critical importance of confidentiality to the therapeutic relationship, it is not absolute. Under certain circumstances, the law may allow or even require that the patient's right to privacy yield to the legitimate and overriding interest of certain parties in obtaining necessary patient information.

This policy directive sets forth the New York State Office of Mental Health's privacy policy. By setting forth certain rules, requirements, and strategies intended to protect the confidentiality of individually identifiable health information, the Office will be able to ensure that patient privacy is appropriately safeguarded.

1.2 Impact of OMH Privacy Policy on Existing OMH Policies and Procedures.

This policy governs the use and disclosure of individually identifiable health information. A number of existing Office of Mental Health policy directives already have provisions related to the use and disclosure of such information, which might be impacted by this privacy policy. The following table identifies the impact of this policy on the use and disclosure provisions of current policy directives of the Office of Mental Health, as set forth in the OMH Official Policy Manual:

Current OMH Policy Directive	Subject Matter	Affected by OMH Privacy Policy?	Explanation	Relevant Privacy Policy Provisions
A-250	Personal Privacy Protection Law	YES Fully Partially	The OMH Privacy Policy supersedes any provisions of A-250 as they apply to the use or disclosure of clinical records, including, e.g., D)4)b); D)5)	Section 6 Section 10
PC-310	Access of Psychiatric History Information	NO	The information use and disclosure provisions found in PC-310 remain in effect.	Section 6, particularly Paragraph 6.2
PC-400	Discharge and Conditional Release of Patients to the Community from State Operated Psychiatric Facilities	NO	PC-400 is consistent with the OMH Privacy Policy, as recent amendments to the directive contain appropriate references to HIPAA.	Section 6

Current OMH Policy Directive	Subject Matter	Affected by OMH Privacy Policy?	Explanation	Relevant Privacy Policy Provisions
PC-450	Procedures Following Death of Patient	NO	PC-450 is consistent with the OMH Privacy Policy, as recent amendments to the directive contain appropriate references to HIPAA.	Section 6, particularly subparagraphs 6.3.10, 6.3.11
PC-615	Referrals	NO	The information use and disclosure provisions of PC-615 remain in effect.	Section 6
PC-801	Social Security Benefits	NO	The information use/ disclosure provisions in PC-801 remain intact.	Section 6, particularly Paragraph 6.2
PC-1411	Acquired Immune Deficiency System (AIDS)	YES Fully Partially	The information use/ disclosure terms of PC-1411 remain in effect, due to stricter language of AIDS statute (PHL Article 27-F). Language in section D)l)ii) provides that release of information normally considered non-confidential (e.g. age, sex, residence) must be evaluated in the context of whether or not it may lead to identification of the patient. This, however, is PHI in accordance with HIPAA and the OMH Privacy Policy and must be treated as confidential.	With regard to the language of PC-1411 which is superseded by the OMH Privacy Policy, see Paragraph 5.3.
QA-400	Uniform Clinical record (UCR)	NO	QA-400 remains in effect. Information contained in the UCR is considered part of the "designated record set" for purposes of the HIPAA Privacy Regulations. * But note: QA-400 requires each facility director to develop procedures to (1) ensure the confidentiality/ security of the UCR and (2) ensure information that is in the UCR is released only as allowed by MHL Section 33.13. These procedures must be reviewed and revised if necessary to ensure consistency with the OMH Privacy Policy, which shall supplement any individual facility procedures previously developed.	Section 3 (h)

Current OMH Policy Directive	Subject Matter	Affected by OMH Privacy Policy?	Explanation	Relevant Privacy Policy Provisions
QA-410	Access of DCJS Records	NO	The information use and disclosure provisions of QA-410 remain in effect.	Paragraph 6.3, particularly subparagraphs 6.3.3, 6.3.6, and 6.3.8
QA-500	Patient Complaint Resolution Process	YES Fully Partially	The provisions of QA-500 remain in effect for the filing of all complaints except complaints based on a potential violation of a misuse or improper disclosure of protected health information. The procedure for filing and addressing those complaints is governed by the OMH Privacy Policy. If a complaint filed pursuant to QA-500 appears to involve a misuse or improper disclosure of PHI, appropriate steps must be taken to assist a patient in filing the complaint in accordance with the OMH Privacy policy.	Section 4, particularly paragraph 4.6
QA-510	Clinical Risk Management and Incident Management Plans	NO	The information use and disclosure provisions within QA-510 remain in effect. OMH Counsel's Office has made a determination that incident reports are excluded from the definition of "health information" for purposes of HIPAA Privacy Regulations.	Section 3(e) Section 6
QA-515	Reporting Requirements for Alleged Child Abuse and Neglect	NO	The information use and disclosure provisions within QA-515 remain in effect.	Section 6, particularly subparagraph 6.3.2
QA-520	Missing Persons	NO	The information use and disclosure provisions of QA-520 remain in effect.	Section 6, particularly subparagraphs 6.3.3, 6.3.6, and 6.3.7

Current OMH Policy Directive	Subject Matter	Affected by OMH Privacy Policy?	Explanation	Relevant Privacy Policy
QA-530	Reporting Requirements for Events Which May be Crimes	NO	The reporting provisions of QA-530, relative to reporting crimes that occur at the facility, remain in effect. *Note: Sample agreement accompanying this policy directive has been revised; see Appendix 4.	Section 6, particularly 6.3.6
QA-535	Sentinel Events	NO	The reporting and information use/disclosure provisions of QA-535 remain in effect.	Section 3(e) Section 6
QA-615	Access to Clinical Records by Qualified Persons	YES Fully Partially	The OMH Privacy Policy supersedes QA-615 in its entirety.	Section 10, particularly paragraph 10.1, 10.2
QA-620	Access to Information by the Media	YES Fully Partially	The OMH Privacy Policy supersedes QA-620 in its entirety.	Section 8, particularly paragraph 8.7

1.3. Relevant Statutes and Standards

45 C.F.R. Parts 160, 164
Mental Hygiene Law Section 33.13
Mental Hygiene Law Section 33.16
Public Health Law Article 27-F
Public Officers Law Section 74
OMH Official Policy Directive QA-602: Use of Personal Cell Phones and Recording Devices in Facilities
OMH HIPAA Preemption Analysis

2. APPLICABILITY:

The OMH Privacy Policy applies to all New York State Office of Mental Health centers, bureaus, facilities, and programs and, as applicable, to all New York State Office of Mental Health workforce members.

3. DEFINITIONS:

(a) ***Access*** means the opportunity to inspect or review the contents of a Designated Record Set and/or obtain a copy of it.

(b) ***Authorization*** means an expression of permission by a patient or his/her personal representative that allows the use or disclosure of PHI for purposes other than treatment, payment, or health care operations purposes.

(c) ***Breach*** means the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

(d) ***Business Associate*** means a person or entity who, for or on behalf of the Office of Mental Health, (but not as a member of its workforce), performs, or assists in the performance of, a function or activity for which the use or disclosure of PHI is necessary, including organizations that provide data transmission of PHI and require access to such information on a routine basis. Examples include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation (e.g. The Joint Commission), financial services involving use or disclosure of PHI, Health Information Exchange Organizations, Regional Health Information Networks, E-Prescribing Gateways, vendors that contract with covered health care providers to offer personal health records to their patients, or a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a Business Associate.

(e) ***Capacity*** means a patient's ability to understand and appreciate the nature and consequences of a decision related to the use or disclosure of his/her PHI (e.g., being photographed); to make a decision regarding such use or disclosure, and to understand that the decision regarding such use or disclosure will involve no penalty or loss of benefits to which the patient is otherwise entitled.

(f) ***Clinical record*** means the collection of information concerning a patient and his or her health and/or behavioral health care (including admission, legal status, assessment, treatment planning, treatment, and discharge) that is created and maintained in the regular course of OMH facility business in accordance with OMH policies, made by a person who has knowledge of the acts, events, opinions or diagnoses relating to the patient, and made at or around the time indicated in the documentation The clinical record does not include Incident Reports nor any of the incident report's supporting documents, (e.g., internal investigation materials or reports or quality assurance materials or reports).

(g) ***Clinical Records Access Review Committee*** *(formerly Medical Records Access Review Committee)* means a regional committee which is responsible for reviewing appeals filed by qualified persons who have been denied access to a Designated Record Set by a State operated or State licensed mental health facility.

(h) ***Correctional Institution*** means any place operated by or under contract with a government entity (federal, state, or local government or Indian tribe) for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. This includes Office of Mental Health forensic facilities that provide services to persons committed to mental institutions through the criminal justice system (i.e., via Criminal Procedure Law Section 330.20 or Article 730), or others awaiting charges or trial.

(i) ***Covered Entity*** means a health plan, health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction[4], which is required to comply with the HIPAA Privacy Regulations.

(j) ***Designated Record Set*** means the clinical record and the billing records contained in the Patient Resource Case File, and any other supplemental, additional, or modified forms which may be utilized by a facility to record information that is used to make decisions about a particular patient's care. It does not include the Incident Report (nor any of the Incident Report's supporting documents e.g., internal investigation materials or reports, or quality assurance materials or reports) or the Education Record.

[4]The "covered transactions" refer to a list of electronic transmissions of information to carry out financial or administrative activities related to health care. A few examples are health care claims (billing), benefit coordination, enrollment/disenrollment in a health plan, health plan eligibility, and health plan premium payments. The complete list can be found at 45 C.F.R. §160.103.

(k) ***Designated Staff Member*** means a physician, psychologist, nurse or certified social worker who is currently licensed to practice his/her profession by the New York State Education Department or any other person not prohibited by law from providing mental health services.

(l) ***Disclose*** means to release, transfer, provide access to, divulge in any manner, or otherwise share protected health information with a person, organization, or entity that is not part of the Office of Mental Health.

(m) ***Forensic Patient*** means and includes:

(1) an inmate of a state correctional institution that is receiving mental health services from the Office of Mental Health in accordance with Section 402 of the Corrections Law;

(2) a person committed to an Office of Mental Health facility by a court order issued pursuant to Article 730 of the Criminal Procedure Law, or who is subject to subsequent retention orders following an initial commitment made under this statute; or

(3) a person committed to the custody of the Commissioner of the Office of Mental Health, in a forensic or civil facility by a court order issued pursuant to Section 330.20 of the Criminal Procedure Law or who is subject to subsequent retention orders following an initial commitment made under this statute, including persons who have been found to suffer from a dangerous mental disorder or who have been found to be mentally ill (as both terms are defined in Section 330.20 of the Criminal Procedure Law[5]); or

(4) any person in a local correctional facility, who is either awaiting sentence or who has been sentenced, who is receiving services from the Office of Mental Health in accordance with Section 508 of the Corrections Law.

(n) ***Facility Serving Forensic Patients*** means a facility operated by the Office of Mental Health, whether secure or non-secure, which provides services to forensic patients.

(o) ***Health Care Operations*** means and includes functions such as quality assessment and improvement activities; reviewing competence and qualifications of health care professionals; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice/improve their skills as health care providers; conducting or arranging for medical review; legal services and auditing functions; planning and development; and general business and administrative activities.

(p) ***HHS*** means the federal Department of Health and Human Services.

(q) ***Health Oversight Agency*** means a governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is authorized by law to oversee the public or private health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights for which health information is relevant.

(r) ***Individua***l means a patient, as defined in this section, or a research participant, as the context applies.

(s) ***Informed Consent*** means the legally effective knowing agreement of a patient, or his or her personal representative, with sufficient capacity to agree and so situated as to be able to

[5]This category includes persons commonly referred to in the OMH system as “Track 1's and Track 2's”, but does not include “Track 3's.” Persons who are on “Track 3" are not considered “inmates” for purposes of this policy directive.

exercise free power of choice without undue inducement or any element of force, fraud, deceit, duress, or any other form of constraint or coercion.

(t) ***Inmate*** means a person incarcerated or otherwise confined to a correctional institution.

(u) ***Law Enforcement Official*** means a public employee from any branch of government who is empowered by law to investigate a potential violation of the law or to prosecute, or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

(v) ***Minor*** means an individual less than 18 years of age.

(w) ***Notice of Privacy Practices*** means a written notification relating to a Covered Entity's use and disclosure of protected health information (PHI) that is mandated under HIPAA Privacy Regulations for distribution to all individuals whose information will be collected by or on behalf of the entity.

(x) ***Patient*** means and includes:

(1) for adults, each individual for whom a clinical record is maintained or possessed by a facility or program and, if applicable, his or her personal representative; and

(2) for minors, each individual for whom a clinical record is maintained or possessed by a facility or program and his or her parent, unless clinically contraindicated, or personal representative.

(y) ***Payment*** means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.

(z) ***Personal Representative*** means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in loco parentis (i.e., acting as a temporary guardian of a child), who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting in loco parentis has assented to an agreement of confidentiality between the provider and the minor.

(aa) ***Protected Health Information (PHI)*** means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

(ab) ***Qualified person*** means a person who may request access to a designated record set. For purposes of this policy directive, qualified persons are limited to the following:

(1) the patient who is receiving or has received services from an inpatient or outpatient program operated by a State psychiatric facility and about whom a designated record set is maintained or possessed by the facility;

(2) the committee of an incompetent patient appointed by the court pursuant to Article 78 of the Mental Hygiene Law; or guardian of the person appointed by the court pursuant to Article 81 of the Mental Hygiene Law;

(3) the guardian of a minor patient appointed pursuant to Article 17-A of the Surrogate's Court Procedure Act or other legally appointed guardian if that guardian has consented to the minor's treatment;

(4) the parent of a minor patient if that parent has consented to the minor's treatment; and

(5) any other personal representative, as defined in this section.

(ac) ***Research*** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

(ad) ***Treatment*** means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.

(ae) ***Use*** means the sharing, application, utilization, examination, or analysis of protected health information within the Office of Mental Health.

(af) ***Workforce Members*** means employees, volunteers, trainees, clinicians serving under contracts with facilities, and other persons whose conduct, in the performance of work for the Office, including its programs or facilities, is under the direct control of the Office of Mental Health, regardless of whether or not they are paid by the Office.

4. ADMINISTRATIVE REQUIREMENTS:

4.1. Personnel Designations. The Office of Mental Health must designate and document designations of the following:

4.1.1. Privacy Official.

The Commissioner shall designate an individual to be the Office of Mental Health Privacy Official, who shall be responsible for the development and implementation of Office-wide policies and procedures relating to the safeguarding of PHI.

Each Facility Director shall designate a Privacy Official Liaison to act in support of the Privacy Official, and to ensure that the activities required by the OMH Privacy Policy are carried out in each State operated psychiatric hospital and State operated program.

4.1.2. Contact Person or Office.

Each Facility Director shall designate an individual, position, title, or office that will be responsible for receiving complaints relating to PHI and for providing information about the Office of Mental Health's privacy practices.

The respective contact person or office shall be identified on the Notice of Privacy Practices utilized by each State operated psychiatric hospital and State operated program, in accordance with Section 9 of this policy directive.

4.2. Policy Control. The Office must document the following actions relating to its policies and procedures:

4.2.1. Required Policies and Procedures.

The Office of Mental Health shall design and implement policies and procedures to assure appropriate safeguarding of PHI in its operations. The OMH Privacy Policy is intended to fulfill

this responsibility as well as to assure compliance with the HIPAA Privacy Regulations and New York State law. State operated psychiatric centers and programs may supplement this policy directive with their own policies and procedures to facilitate these assurances.

4.2.2. Changes to Policies and Procedures.

The Office of Mental Health must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. The Office may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, the Office shall make correlative changes in its Notice of Privacy Practices, in accordance with Section 9 of this policy directive. The Office shall not implement a change in policy or procedure prior to the effective date of the revised Notice.

4.3. Documentation Requirements.

The Office of Mental Health must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations that are required to be documented under the HIPAA Privacy regulations[6], for a period of six (6) years from the later of the date of creation or the last effective date.

4.4. Training Requirements.

The Office must facilitate and document the following training actions:

4.4.1. When Required.

On and after April 1, 2003, All Office of Mental Health workforce members must receive training on applicable policies and procedures relating to PHI as necessary and appropriate for such persons to carry out their functions within the Office.

4.4.2. Training New Workforce Members.

Each new workforce member shall receive the training as described in subparagraph 4.4.1 within a reasonable time after joining the workforce.

4.4.3. Changes in Policies/Procedures.

Each workforce member whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a change in position or job description, must receive the training as described in subparagraph 4.4.1 within a reasonable time after the change becomes effective.

---

[6]The general documentation requirements in the HIPAA privacy regulations can be found at 45 CFR Section 164.530(j)1(ii) and (iii). Elements required to be documented (i.e., in writing) include, e.g.,: Business Associate contracts, authorizations and authorization revocations, IRB waiver of an individual's authorization, denials of requests for access to PHI, denials of requests to amend PHI, Notice of Privacy Practices, information to be included in an accounting, privacy official designation, contact person/office to receive complaints, that workforce training has been provided, all complaints received from individuals and their dispositions, sanctions for violating this policy, and changes to policies/procedures. A complete list of documentation requirements can be obtained from Counsel's Office.

4.5. Safeguards.

Each center, bureau, facility, or program of the Office must have in place appropriate administrative, technical, and physical safeguards to reasonably safeguard PHI from intentional or unintentional unauthorized use or disclosure.

4.5.1. Administrative Safeguards.

Administrative safeguards shall include, at a minimum, the establishment of a clearly identified structure within which HIPAA compliance issues can be addressed.

(a) Each workforce member must be informed, by Central Office if he/she primarily works in a Central Office location, or by the respective facility if he/she primarily works in a facility or facility program location, as to the steps to take if encountering what reasonably appears to be noncompliance with the OMH Privacy policy, the HIPAA Privacy Regulations, or New York State law.

(b) Such steps shall include reporting any apparent noncompliance to his or her supervisor, who shall then, in turn, ensure that the matter is appropriately referred within the identified HIPAA compliance structure.

4.6. Complaint Process.

Each facility shall have in place a process for its patients to make complaints about the Office of Mental Health's HIPAA policies and procedures and/or the Office's compliance with those policies and procedures, and must document all complaints received and the disposition of each complaint. At a minimum, such process shall include the following provisions:

4.6.1. Notification procedures.

(a) The process shall assure that each patient receives written information about the complaint process upon his or her admission to a program and again upon his or her request. With the patient's consent, such information shall also be provided to the patient's family member or significant other.

(b) Such information shall clearly identify who a patient should contact if he or she wishes to file a complaint[8]. Information regarding access to the Office of Mental Health Customer Service line (1-800-597-8481) and to the federal Department of Health and Human Services shall also be provided.

4.6.2. Form of complaints.

Procedures must identify the form in which complaints must be filed, i.e. verbal or written or both.

[8]It is generally assumed that because OMH facilities and programs have the most direct interaction with patients, the majority of filed complaints will probably involve activities that took place within such facility or programs. As such, these complaints are best addressed on that level. However, because Central Office also uses and discloses PHI, if a complaint is filed that involves activities that took place at the Central Office level, the complaint should be filed through the facility or program that is currently serving, or which last served, the patient (i.e., the facility or program which provided the patient with its Notice of Privacy Practices) and the contact person of that facility shall collaborate with the Central Office Privacy Official on the review and resolution of such complaints.

4.6.3. Time frames.

The complaint process must specify the time frames within which, upon receipt of a complaint by a patient, the facility's decision with regard to the complaint shall be provided to the patient in writing. For all filed complaints, the Facility Director, or his or her designee, must review and timely render a determination in a written decision that shall be communicated to the patient in a language and manner the patient understands.

4.6.4. Appeals.

If a patient's complaint resolution attempts are unsuccessful at the facility level, the patient shall be informed that he or she may contact the Bureau of Quality Management in Central Office for further review, who shall consult with the OMH Privacy Official as appropriate.

4.7. Sanctions.

4.7.1. Office of Mental Health Employees.

The Office shall take appropriate disciplinary action for breaches of patient confidentiality by Office employees under the HIPAA Privacy and Security Regulations, which shall be consistent with the disciplinary action taken for breaches of patient confidentiality by employees under the New York State Mental Hygiene Law. As is current practice, penalties will be applied based on the severity of the violation(s) committed, and may range from a reprimand through fine, suspension without pay, to termination of employment. Existing disciplinary processes, as identified in applicable collective bargaining agreements, will be followed for violations of patient confidentiality under both New York State law and HIPAA regulations.

4.7.2. Persons Who are Not Office of Mental Health Employees.

For breaches of confidentiality by workforce members who are not employees, the Office of Mental Health shall refer the matter to such workforce member's employer or contract agency for appropriate disciplinary action and/or may terminate its business relationship with such workforce member, as appropriate.

4.7.3. Good Faith Disclosures.

For purposes of this policy directive, it shall not be considered to be a breach of patient confidentiality if a member of the Office's workforce believes in good faith that the Office has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or the care, services, or conditions provided by the Office potentially endangers one or more patients, workers, or the public, and such workforce member therefore discloses PHI to:

(a) a public health authority, health oversight agency, or healthcare accreditation organization authorized to investigate or oversee the conduct at issue; or

(b) an attorney retained by the workforce member or Business Associate for the purpose of determining legal options of the workforce member or Business Associate with regard to the conduct.

4.7.4. Disclosures by Workforce who are Victims of Criminal Acts.

For purposes of this policy directive, it shall not be considered to be a breach of patient

confidentiality if a member of the Office's workforce who is a victim of a criminal act discloses PHI to a law enforcement officer, provided that the PHI disclosed is about the suspected perpetrator of the criminal act, and the PHI disclosed is limited to the information listed in 45 C.F.R. §164.512(f)(2)(i)[9].

4.7.5. Training.

To ensure that all workforce members are sufficiently advised of their responsibilities and obligations under the HIPAA Privacy and Security Regulations, the Office shall provide training on this topic.

4.8. Mitigation Efforts Required.

The Office of Mental Health must mitigate, to the extent practicable, any harmful effects of unauthorized uses or disclosures of PHI by such Office or by any of its Business Associates[10]. Unauthorized uses or disclosures shall be reviewed in accordance with Section 12.3 of this directive.

4.9 Intimidating or Retaliatory Acts Prohibited.

Neither the Office nor any workforce member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of his/her rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, or for participating in a HIPAA related investigation, compliance review, proceeding or hearing, or for engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA regulations as long as the action does not involve disclosure of PHI in violation of the regulations.

4.10 Prohibition on Waiver of Rights.

No workforce member of the Office shall require individuals to waive any of their rights under HIPAA as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

5. INFORMATION COVERED BY THE OMH PRIVACY POLICY:

5.1. Protected Health Information.

The directives in this policy that govern the use, disclosure, safeguarding, or accounting of information apply to any protected health information, as defined in subdivision (aa) of Section 3 of this policy, that the Office of Mental Health creates or receives.

---

[9]This information is limited to: (1) name/address;(2)date/place of birth;(3) social security number; (4) ABO blood type and rh factor; (5)type of injury; (6) date/time of treatment; (7) date/time of death, if applicable; and (8) a description of distinguishing physical characteristics, including height, weight, gender, race, hair/eye color, presence/absence of facial hair, scars, and tattoos.

[10]Some examples of "mitigation efforts" include: (1) if PHI was released without a proper authorization, OMH could require that the recipient of the information be asked to destroy or return the PHI; (2) if a Business Associate released PHI to a subcontractor who used PHI for an unauthorized purpose, OMH could ask the Business Associate if the subcontract also contained a Business Associate Agreement, as required by HIPAA; if not, and the Business Associate refused to remedy, OMH could explore termination of the contract with its Business Associate.

5.2 Designated Record Set.

The directives in this policy that govern patient access to, or amendment of, records apply to that information contained in the designated record set, as defined in subdivision (i) of Section 3 of this policy.

5.3. De-Identified Information.

5.3.1 Defined.

Information is considered de- identified, and therefore can be used or disclosed without violating any of the provisions of this policy directive, if:

(a) a person with appropriate knowledge and experience with generally acceptable statistical and scientific principles and methods determines that the risk is very small that the information could be used, alone or with other reasonably available information, to identify the individual who is the subject of the information; or

(b) all of the following identifiers of the individual (and relatives, employers or household members) are removed:

(1) names;

(2) all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes[11];

(3) elements of dates (except year) directly related to the individual, and all ages and elements of dates that indicate age for individuals over 89, unless aggregated into a single category of age 90 and older;

(4) telephone numbers; fax numbers; email addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers;

(5) Web Universal Resource Locators (URLs);

(6) Internet Protocol (IP) address numbers;

(7) biometric identifiers;

(8) full face photographic images; and

(9) any other unique identifying number, characteristic or code (e.g. indictment numbers or docket numbers).

5.4. Limited Data Set.

5.4.1. Conditions for Use.

The use or disclosure of a “limited data set,” as identified in this paragraph, is permitted without

[11] Use of the initial 3 digits of a zip code is permissible if, according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes within the same 3 initial digits contains more than 20,000 people; and (2) the initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

patient consent or authorization for the purposes of research, public health, or health care operations if a Data Exchange Agreement has been executed with the entity which shall receive the limited data set.

(a) A standard Confidentiality and Non Disclosure Agreement and Data Exchange Agreement must be utilized for this purpose.

5.4.2. Defined.

A "limited data set" is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(a) names;

(b) postal address information, other than town or city, State, and zip code;

(c) telephone numbers; fax numbers; email addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers;

(d) Web Universal Resource Locators (URLs);

(e) Internet Protocol (IP) address numbers;

(f) biometric identifiers, including finger and voice prints; and

(g) full face photographic images and any comparable images.

6. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION (PHI):

6.1. Minimum necessary standard.

6.1.1. Defined; Exceptions.

To the extent practical, the Office of Mental Health will limit disclosures of information to the "limited data set, "or to the minimum amount of PHI necessary to fulfill the intended purpose or function of the use or disclosure, provided, however, that in the event the federal Department of Health and Human Services issue guidance in making "minimum necessary" determinations, disclosures shall be made in accordance with such guidance. Exceptions to the minimum necessary standard include:

(a) disclosures to the individual who is the subject of the information;

(b) disclosures made pursuant to an authorization requested by the individual;

(c) disclosures to or requests by healthcare providers for treatment purposes, provided such disclosure is made in accordance with Section 33.13 of the NYS Mental Hygiene Law;

(d) disclosures required for compliance with the standardized HIPAA transactions;

(e) disclosures made to HHS pursuant to a privacy investigation; and

f) disclosures otherwise required by the HIPAA Privacy Regulations or other law, including but not limited to State law.

6.1.2. How Determined.

The following process shall apply until such time as the federal Department of Health and Human Services issues guidance in making "minimum necessary" determinations. At such time, the following process shall be interpreted consistent with such guidance. For each individual function performed at the Office of Mental Health, there shall be an assessment of the level of access to PHI appropriate to that function.

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of the Office of Mental Health:

(a) Central Office and each facility will identify its respective systems containing PHI and the extent of PHI to which access is needed, and will establish any conditions appropriate to such access, provided, however, that unless otherwise limited by a Facility Director, all direct caregivers shall have the authority to view all PHI on a patient within their care.

(b) Reasonable efforts will be made to limit each PHI user's access to only the PHI that is needed to carry out his/her duties. These efforts will include internal workforce member- to- workforce member use of PHI.

(c) Individual requests for disclosure (other than pursuant to an authorization, e.g., to funeral directors, court orders, etc), will be reviewed in accordance with Central Office or Facility procedures to limit the information disclosed to that which is reasonably necessary to accomplish the purpose for which disclosure is sought. A request may be presumed to be limited to the minimum necessary if:

(1) the request is from a public official, another Covered Entity, or a professional for the purpose of providing services to the Covered Entity; and

(2) the request states that the PHI requested is the minimum necessary for its intended purpose.

(d) Requests for disclosure from external non-Covered Entities will be reviewed to ensure that the response limits the disclosed information to that which is reasonably necessary to accomplish the purpose for which disclosure is sought[12]. All requests for PHI made by workforce members of the Office of Mental Health must be reviewed to ensure that the request limits the disclosed information to only that which is reasonably necessary to accomplish the purpose for which disclosure is sought[13].

6.1.3. Incidental disclosures.

Many customary treatment communications and practices play an important or even critical role in ensuring that patients receive prompt and effective health care. Due to the

[12]Again, the "minimum necessary" rule does not apply for uses and disclosures of PHI for treatment purposes. In most cases, these uses and disclosures will likely be made to other covered health care providers; however, it is possible that such uses and disclosures might be made to non covered health care providers (i.e., a health care provider that does not engage in any of the standard electronic transactions). In these instances, the minimum necessary rule would not apply to uses or disclosures of PHI to non covered health care providers for treatment purposes.

[13]In implementing this provision, for ongoing or routine access by workforce members, a one-time review of workforce functions shall suffice.

nature of these communications and practices, as well as the various environments in which patients receive health care or other services from the Office of Mental Health, the potential exists for health information to be disclosed incidentally. This policy directive is not intended to impede customary and essential communications. safeguards[14] to protect PHI, incidental disclosures (such as a patient overhearing a fragment of conversation about another patient) shall not be considered an impermissible disclosure for purposes of this policy directive. Examples of permissible incidental disclosures include:

(1) a health care professional may discuss a patient's condition or treatment regimen in the patient's semi-private room;

(2) health care professionals may discuss a patient's condition during training rounds in an academic or training institution; or

(3) a pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

(b) Common sense must be employed in making a determination as to whether or not a disclosure is a permissible incidental disclosure. There are some activities that could result in unintentional disclosures that, by their nature, reflect both a lack of understanding of the need for confidentiality and a lack of care in taking reasonable safeguards to protect PHI. Because such unwitting disclosures are easily preventable, they would not be considered permissible incidental disclosures and could, in fact, be considered privacy breaches and/or violations of the HIPAA privacy regulations. Examples of impermissible incidental disclosures include:

(1) posting patient art work in public areas with the patient's name on it, without his or her authorization to do so;

(2) leaving a clinical record in an unsecured area;

(3) disposing of unshredded materials containing PHI in a public trash can; and/or

(4) discussing a patient with a colleague in an area where non-authorized personnel can easily overhear the discussion.

6.2. Uses and disclosures for treatment, payment, and health care operations purposes.

PHI may be used or disclosed as necessary to deliver treatment (including health, mental health, and/or emergency treatment), seek payment or pay claims for services, and to operate the facilities and programs within the Office of Mental Health. Written or verbal permission from patients is not required to use or disclose PHI for these purposes, provided, however, that disclosures for treatment purposes must be made in accordance with Section 33.13 of the NYS Mental Hygiene Law.

[14]Examples of reasonable safeguards include speaking quietly when discussing a patient's condition with family members in a public area or moving to a private area; avoiding the use of patient names in public hallways and elevators, and posting signs to remind workforce members to protect patient confidentiality; isolating or locking file cabinets or record rooms; or providing additional security, such as passwords, on computers maintaining PHI.

6.3. Uses and disclosures for purposes related to the Office of Mental Health's public responsibility.

State and federal law permit and/or require certain uses and disclosures of PHI for various purposes related to public responsibility. Written or verbal permission from patients is not required to use or disclose PHI for these purposes.

In all of these cases, the most recent edition of the New York State Office of Mental Health Guidebook: Confidentiality and the Limits to Disclosure of Patient Records and Information should be consulted for additional guidance in individual circumstances. The following uses and disclosures fall within this category[15]:

6.3.1. Health Oversight Activities.

The Office may use or disclose PHI for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as: audits; civil, administrative and criminal investigations and proceedings; inspections; and licensure and disciplinary actions. Some examples of such uses/disclosures are those made to the federal Department of Health and Human Services for audit activities (e.g. Medicaid, Medicare), disclosures made to the Commission for Quality of Care and Advocacy for Persons with Mental Disabilities (or its successor agency, the Justice Center for the Protection of People with Special Needs), disclosures made to the Office for Human Research Protections (for compliance investigations) and disclosures made to the Board of Visitors in accordance with their statutory authority. Specifically excluded from this category are investigations of an individual that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.

6.3.2 Public Health Activities.

PHI may be used or disclosed to:

(a) a public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions; (e.g., under this provision, PHI can be disclosed to the New York State Department of Health to report cases of Lyme disease, pesticide poisoning, and infectious diseases);

(b) a public health or other government authority authorized by law to receive reports of child abuse or neglect (e.g., the Office for Children and Family Services);

(c) a representative of the Food and Drug Administration (FDA), to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance; or

(d) a person who may have been exposed to a communicable disease, or otherwise is at risk for contracting or spreading a disease or condition, if such notice is authorized by law relating to public health investigations or interventions.

[15] If it is not clear whether or not a particular use or disclosure is included within a public responsibility category, Counsel's Office should be consulted.

6.3.3. Required by Law.

PHI may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law[16]. Some examples of these disclosures include those made in accordance with the involuntary hospitalization requirements of Article 9 of the Mental Hygiene Law, or disclosures made with respect to all persons who apply for permits to possess or use handguns.

6.3.4. Abuse and Neglect.

Unless disclosure of PHI is permitted under another provision of HIPAA and State law, (for example, the disclosure is "required by law"), and except for reports of child abuse or neglect, PHI about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or the reporting entity believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm. If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law enforcement activity. The individual whose PHI has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.

6.3.5. Judicial or Administrative Proceedings.

PHI may be disclosed in response to a court order requiring disclosure upon a finding by the court that the interests of justice significantly outweigh the need for confidentiality.

(1) The order must be executed by a judge or clerk of the court, since they are impartial parties with no vested interest in the outcome and can make a determination that the interests of justice significantly outweigh the need for confidentiality.

(2) Only the PHI expressly authorized by such to be disclosed should be released.[17]

(3) A cover letter should accompany the PHI so released, in which a request is made that the PHI be reviewed in camera by an authorized judge or clerk of the court.

6.3.6. Law Enforcement.

PHI may be disclosed for the following law enforcement purposes and under the specified conditions[18]:

(a) for law enforcement purposes, including in response to a law enforcement official's request for such information to identify and locate a suspect, fugitive, material witness, or missing person;

---

[16]Refer to the OMH Preemption Analysis for specific guidance on this category.

[17]In certain limited cases, PHI may be disclosed pursuant to a subpoena, discovery request, or administrative tribunal; Counsel's Office should be consulted for guidance

[18] Proof of identification must be obtained before releasing any PHI to the official requesting the information.

(b) to a district attorney, when the request for information is in connection with and in to the furtherance of a criminal investigation of patient abuse;

(c) in response to a court order or court-ordered subpoena;

(d) in response to a law enforcement official's request for PHI about an individual who is or is suspected to be a victim of a crime[19]. Disclosure is permitted if:

(1) the individual agrees to the disclosure, or;

(2) if the agreement cannot be obtained because of incapacity or other emergency circumstance, provided that the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim; or the law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would materially and adversely be affected until the individual is able to agree to the disclosure; or the disclosure is in the best interests of the individual, using the exercise of professional judgment.

(e) to report a crime on facility, program, or other Office of Mental Health premises, or to report a crime in accordance with Section 31.11 of the Mental Hygiene Law.

6.3.7. Serious Threats to Health or Safety.

Consistent with applicable law and ethical standards, PHI may be used or disclosed if the entity believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and are not permitted when the information is learned in the course of treatment to affect the propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

6.3.8. Correctional Facilities or Facilities Serving Forensic Patients.

(a) PHI may be disclosed to any correctional institution, facility serving forensic patients, or law enforcement official having custody of an inmate or forensic patient when the correctional institution, facility serving forensic patients, or law enforcement official represents that the PHI is necessary to provide care to the forensic patient or inmate, or for the health and safety of the individual, other inmates, or correctional/forensic facility employees, transport employees, law enforcement personnel at the location, and for the safety, security, and good order of the institution[20].

(b) Where a facility serving forensic patients provides treatment to a forensic patient, it may use PHI, without patient consent or authorization, as necessary to provide care to

[19] This does not include a law enforcement official's request for information relating to public health inquiries or neglect/abuse inquiries, which are addressed in paragraphs 6.3.2 and 6.3.4, respectively.

[20] Also note that an individual is no longer an inmate once released on parole or is otherwise no longer in lawful custody.

(c) the patient, or for the health and safety of the patient, other patients, facility employees, transport employees, law enforcement personnel at the location, and for the safety, security, and good order of the facility.

6.3.9. Decedents.

PHI may be disclosed to coroners, medical examiners, or funeral directors, as necessary for carrying out their duties. If necessary for funeral directors to carry out their duties, PHI may be disclosed prior to, and in reasonable anticipation of, a patient's death.

6.3.10. Organ Donation.

PHI may be used or disclosed by the Office of Mental Health to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue in order to facilitate organ, eye, or tissue donation and transplantation[21].

6.3.11. Specialized Government Functions[22]

(a) National Security and Intelligence: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter intelligence, and other activities authorized by the National Security Act.

(b) Protective services: PHI may be disclosed to authorized federal officials for the provision of protective services to the President (e.g., the Secret Service), foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.

(c) Public Benefits: PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

6.3.12. Workers' Compensation.

PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

6.4. Uses and disclosures requiring the patient be given an opportunity to agree or object.

The Office of Mental Health may use or disclose PHI without the written or verbal permission of the patient in the following situations, provided the patient is informed in advance (in writing or verbally) and has the opportunity to agree to, or to prohibit or restrict, the disclosure:

---

[21]These requirements are detailed further in OMH Official Policy PC-450, Procedures Following the Death of Patient.

[22]Proof of identification and written documentation of the request must be obtained and verified prior to the release of information under this subparagraph. In all of these cases, the minimum amount of information necessary to fulfill the purpose of the request should be released.

6.4.1. Facility Directories.

The use of facility directories[23] by Office of Mental Health facilities is not a common practice. However, for those facilities that do choose to utilize a facility directory system, patients must be given the opportunity to agree or object to the inclusion of their name and information in the directory. If the patient does not object, the Office of Mental Health may use PHI to maintain patient directories within its facilities, and to disclose certain information[24] to the clergy and to persons who ask for the patient by name.

(a) It must be explained to each patient that inclusion of his/her name in the directory would enable the facility to provide the designated information to any person who contacts the facility and asks for the patient by name.

(b) If the patient wishes to restrict disclosures to certain individuals, the patient should object to being included in the facility directory.

(c) The patient's response must be appropriately documented.

6.4.2. Disclosures to family and those involved in a patient's care.

Under certain circumstances, it is permissible to share certain PHI with family or friends who are involved in the care, or payment of care, of a patient[25]. The PHI disclosed should be limited to that which is directly relevant to such person's involvement with or payment related to the patient's health care[26].

(a) If the patient is present and available and has capacity to make his/her own health care decisions, the Office may share PHI with a family member, other relative, close personal friend, or any other person identified by the patient, if:

(1) the patient agrees to the disclosure(s);

(2) the patient is provided with an opportunity to object and the patient does not object; or

---

[23] "Facility directories," in the context of the HIPAA Privacy regulations, are general directories that receive inquiries from the public, (e.g. family members, clergy, and florists) as to a named patient's location and general condition.

[24]The specific information permitted to be disclosed includes the patient's name, location within the facility, condition (in general terms that does not communicate specific medical information) and the patient's religious affiliation.

[25]Note that disclosures to family members required pursuant to involuntary admission statutes (e.g. Mental Hygiene Law Sections 9.29 and 9.33) are not governed by this provision. These disclosures can be made without patient consent or authorization, and the patient need not be provided the opportunity to agree or object to these disclosures, since they are required by law (see subparagraph 6.3.3 of this directive).

[26]This subparagraph addresses disclosures made to family or friends of PHI which is directly relevant to that person's involvement in the individual's health care. This may include participation in the development and revision of a patient's treatment plan, in accordance with Mental Hygiene Law Section 29.13. It should be noted that, for purposes of treatment plan development, if a patient over age 16 objects to the participation of his/her parent(s) in the development of the plan and there has been a documented clinical determination by a physician indicating that the involvement of the parent(s) is not clinically appropriate, their participation is not required. To conform this section of law with HIPAA, facilities should give patients the ability to agree or object to the participation of family or friends in treatment plan development for purposes of MHL Section 29.13. If a patient over age 16 objects to such participation yet there is no documented adverse clinical determination, it is recommended that staff work with the patient to voluntarily remove his or her objection.

(3) professional staff of the Office of Mental Health, in the exercise of professional judgment, reasonably infers from the circumstances that the patient does not object to the disclosure. Such circumstances, and the fact of the disclosure, must be appropriately documented.

(b) If the opportunity for the patient to agree or object cannot practicably be provided due to incapacity or emergency circumstance, professional staff may, in the exercise of its professional judgment, determine whether the disclosure is in the best interests of the patient. If so, only that PHI that is directly relevant to the person's involvement with the patient's health care may be disclosed. Such circumstances, and the fact of the disclosure, must be appropriately documented.

(c) Assuming emergency circumstances are not present and/or a patient is not mentally incapacitated, there is no provision in either the New York State Mental Hygiene Law or HIPAA that would permit families of adult patients to have access to their relative's clinical record or to privileged information (i,e., information that should be kept between therapist and patient) contained in it without his or her permission, assuming the patient is not mentally incapacitated. As a general rule, an adult patient must give permission before families can be provided with information about them, and the fact that this permission has been obtained should always be documented, provided, however:

(1) if the patient is deemed mentally incompetent and a family member has legal authority to make medical decisions on behalf of the patient, the family member can access clinical information the same way the patient would be able to access his or her own record;

(2) the Director of a State operated psychiatric center is required by law to inform the family of an involuntary-status patient of the fact that their relative has been involuntarily hospitalized, and must further advise the family where the relative has been hospitalized;

(3) absent express objection by the patient (who must be informed ahead of time) or compelling evidence that it would be counter-therapeutic, the family of a voluntary-status patient may be informed of the fact that their relative has been hospitalized and where he/she is. In this case, information can also be obtained from the family in order to obtain facts about the patient that are necessary for his/her treatment; and

(4) if a patient is going to be discharged from a facility to the care of his or her family, information regarding the patient can be disclosed to the family to the extent that the information is necessary to provide appropriate care to the patient. For example, the fact that a patient is afraid of cats may be useful for his/her family to know, but it is not necessary for the family to know the clinical causes of the patient's fear). Although prior permission from the patient in this case is desirable, it is not mandatory under the law.

(d) Even in situations where families are unable to obtain permission to receive information about their relative, unless it is plainly contraindicated, New York State Mental Hygiene Law Section 29.13 not only allows but requires family involve ment in treatment planning, (when authorized by the patient) because it is presumed that such involvement has important therapeutic benefits. When done in such a manner as to not compromise or reveal information that should be kept between therapist and patient, family involvement can be accomplished without obtaining the express permission of the patient and without violating confidentiality. For example, staff could discuss the programs that are available for the patient, privileges, family visits, legal status, and plans for discharge. Also, if not clinically contraindicated and appropriate, staff could share information provided by the family with the patient, such as relaying messages of support.

6.4.3. Special Provisions for Disaster Relief Efforts.

The Office of Mental Health recognizes the role of the Red Cross and similar organizations in disaster relief efforts, and encourages cooperation with these entities in notification efforts and other means of assistance. Thus, PHI may be disclosed to a public or private entity that is authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities to notify, or assist in the notification (including identifying and locating) of a family member, personal representative, or other person responsible for the care of the individual, of the individual's location, general condition, or death, if any of the following criteria apply, to the extent that, in the exercise of professional judgment, the Office has determined that such criteria do not interfere with the ability to respond to the emergency circumstances:

(a) the patient agrees to the disclosure(s);

(b) the patient is provided with an opportunity to object and the patient does not object;

(c) professional staff of the Office of Mental Health, in the exercise of professional judgment, reasonably infers from the circumstances that the patient does not object to the disclosure. Such circumstances, and the fact of the disclosure, should be appropriately documented, if practicable; or

(d) the opportunity to agree or object cannot practicably be provided due to incapacity or emergency circumstance, and, in the exercise of its professional judgment, professional staff have determined the disclosure is in the best interests of the patient. If so, only that PHI that is directly relevant to the person's involvement with the patient's health care may be disclosed. Such circumstances, and the fact of the disclosure, should be appropriately documented, if practicable.

6.5. Uses and Disclosures requiring an Authorization; Authorization forms.

6.5.1. Standards and Procedures.

In compliance with federal regulations (45 CFR Part 164) and New York State law, all uses and disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization.

6.5.2. Special Protections for Psychotherapy Notes Not Applicable:

The HIPAA privacy regulations establish special protections for "psychotherapy notes." However HIPAA defines "psychotherapy notes" as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *It is important to note that the definition of "psychotherapy notes" excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date – which, for facilities of the Office of Mental Health, is all of the information required to be maintained in the clinical record*.

While the HIPAA privacy regulations require authorizations for most used of psychotherapy notes, this protection is not extended to the same information if it is maintained in a clinical record. *Therefore, the special protections for psychotherapy notes established in HIPAA do not apply to the mental health clinical record*. Instead, uses and disclosures of the mental health clinical record of New York State operated psychiatric centers are governed by NYS Mental Hygiene Law Section 33.13 and HIPAA, as it applies to protected health information in general.

6.5.3. Conditioning Use.

If an authorization is required before PHI can be used or disclosed[27], the provision of treatment, payment, or eligibility for benefits may not be conditioned on the patient's provision of such an authorization for the use or disclosure of PHI except:

(a) if the treatment to be provided is research related treatment; or

(b) if the sole purpose of creating the PHI is for disclosure to a third party.

6.5.4. Form and Content of Authorization.

(a) Form. As a matter of general procedure, OMH Form 11 or 11C[28] shall be utilized to record authorizations, provided, however, that permission to grant access to information by the media, as set forth in section 8 of this policy directive, may be documented via OMH Forms 445 and 446 if all information required in subparagraph 6.5.3 is contained therein.

If OMH Form 11 is used and the PHI contains HIV related information, an additional "Authorization for Release of Confidential HIV Related Information" form, DOH 2557[29], must be completed. A prohibition on redisclosure notice must accompany disclosures of such information, in accordance with Public Health Law Article 27F. This additional DOH form is not required if OMH Form 11C is used.

(b) Content. If an authorization is received by a facility or program that has been recorded on other than an OMH-11 or 11C form, it can be accepted if legally valid. To be legally valid, an authorization must include at least the following information:

(1) a specific and meaningful description of the information to be used or disclosed;

(2) the name or identification of the person or class of person(s) authorized to make the use or disclosure;

(3) the name or identification of the person or class of person(s) to whom the requested use or disclosure may be made;

(4) the purpose of the disclosure (unless, if the disclosure is being made at the request of the patient, no other purpose need be identified);

(5) an expiration date, condition or event that relates to the individual or the purpose of the use or disclosure;

(6) a statement that the patient may refuse to sign the authorization;

(7) a statement that unless an exception set forth in paragraph 6.5.2 of this section applies[30], treatment, payment, or eligibility for benefits may not be conditioned on the patient's provision of an authorization for the use or disclosure of PHI;

---

[27]Keep in mind, however, that consent or authorization is not required to use or disclose PHI for treatment, payment, or health care operations purposes.

[28]OMH Forms 11 and 11C are included as an Appendix to this directive.

[29]DOH Form 2557 is included as an Appendix to this directive.

[30]Keep in mind that consent or authorization is not required to use or disclose PHI for treatment, payment, or health care operations purposes.

(8) if applicable, a statement identifying any remuneration to the Office of Mental Health from the use or disclosure;

(9) a statement of the patient's right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how the patient may revoke the authorization. Upon written notice of revocation, further use or disclosure of PHI shall cease immediately except to the extent that the office, facility, program or employee has acted in reliance upon the authorization or to the extent that use or disclosure is otherwise permitted or required by law;

(10) a statement that the information may only be re-released with the written authorization of the patient, except as required by law;

(11) the dated signature of the patient; and

(12) if the authorization is signed by a personal representative of the patient, a description of the representative's authority to act on behalf of the patient.

6.5.5. Copy Distribution.

A copy of each executed (i.e., signed) authorization must be provided to the patient and the patient's personal representative, where applicable. If, in the judgment of a professional, it is in the patient's best interest to provide the copy of the authorization solely to his/her personal representative, this may be done, with appropriate documentation.

6.5.6. Record Retention.

A written or electronic copy of the authorization must be retained for a period of 6 years from the later of the date of execution or the last effective date.

7. RESEARCH: USE AND DISCLOSURE; RIGHTS OF ACCESS; ACCOUNTING OF RESEARCH RECORDS:

7.1. Uses and Disclosures.

7.1.1. When Authorization Required.

Use or disclosure of PHI created for research generally requires an authorization unless such use or disclosure is permitted without same pursuant to paragraph 7.1.2 of this paragraph.

(a) The authorization must contain the elements set forth in paragraph 6.5.3 of this section, provided, however, that an authorization for a research purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues "until the end of the research study."

(b) An authorization for the use/disclosure of PHI for research may be combined in the same document with the consent to participate in research, or with any other legal permission related to the research study.

7.1.2. When Authorization Not Required.

(a) De-Identified Information: The Office of Mental Health may always use or disclose,

for research purposes, PHI which has been de-identified, in accordance with paragraph 5.3 of this policy directive.

(b) IRB Waiver: PHI may be used or disclosed for research purposes if documentation that an alteration or waiver or a research participant's authorization for use/disclosure about him/her for research purposes has been approved by an Institutional Review Board (IRB) or Privacy Board, provided documentation of all of the following is obtained:

(1) identification of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;

(2) a statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the following criteria:

(i) The use/disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

A. an adequate plan to protect the identifiers from improper use/disclosure;

B. an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

C. adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project or for other research for which the use/disclosure of PHI would be permitted under the federal HIPAA regulations;

(ii) The research could not practicably be conducted without the waiver or alteration; and

(iii) The research could not practicably be conducted without access to and use of the PHI.

(c) Uses/Disclosures Preparatory to Research: PHI may be used/disclosed without the individual's authorization if the Office of Mental Health has received representations from the researcher, either in writing or verbally, that the use/disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research[31], that the researcher will not remove any PHI from the Office of Mental Health, and that the PHI for which access is sought is necessary for the research purpose [32].

[31]Examples of such purposes include to design a research study or to assess the feasibility of conducting a study.

[32]A researcher who is an employee or member of the Office of Mental Health's workforce can use PHI to contact prospective research subjects, for purposes of seeking their authorization to use/disclose PHI for a research study. Furthermore, it is permissible disclose PHI to the individual who is the subject of the information, and thus to discuss the option of enrolling in a clinical trial, without patient authorization and without an IRB or Privacy Board waiver.

(d) Research on Decedents: PHI may be used/disclosed without the individual's authorization if the Office of Mental Health has received representations from the researcher, either in writing or verbally, that the use/disclosure being sought is solely for research on the PHI of decedents, that the PHI sought is necessary for the research, and that documentation of the death of the individuals about whom information is being sought is provided[33].

(e) Limited Data Sets with a Data Use Agreement: PHI may be used/disclosed without the individual's authorization if the Office of Mental Health and the researcher have entered into a Data Use Agreement and have otherwise met the requirements of subparagraph 5.4.1 of this policy directive.

(f) Research databanks: The Office of Mental Health may use/disclose PHI without an individual's authorization for the creation of a research databank, provided the Office obtains documentation that an IRB or Privacy Board has determined that the specific waiver criteria, as set forth in subparagraph 7.1.2(b)(2) are met. PHI maintained in a research databank can be used/disclosed for further research studies in cases where individual authorization has been obtained or when authorization is not required, in accordance with (a)-(e) of this subparagraph.

7.2 Accounting for Research Disclosures.

7.2.1. Right to Accounting.

In general, persons have a right to receive an accounting of disclosures of their PHI in accordance with paragraph 10.5 of this policy directive. With regard to research disclosures, the following shall apply:

(a) Research disclosures made pursuant to an individual's authorization are exempt from the accounting requirement[34].

(b) Disclosures of the limited data set to researchers with a data use agreement, in accordance with subparagraph 7.1.2 (e) of this directive, are exempt from the accounting requirement.

(c) For disclosures of PHI for research purposes for which the individual's authorization is not required (i.e., disclosures made pursuant to subparagraph 7.1.2 of this directive), and which involve at least 50 records, a simplified accounting of such disclosures may be made, which includes:

(1) the name of the protocol or research activity;

(2) a description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(3) a brief description of the PHI that was disclosed;

[33]If the Office of Mental Health has otherwise confirmed the death of the individual(s) about whom information is being sought, and the requirement to provide documentation of the death of such individuals may be waived.

[34]Note that all disclosures made pursuant to a patient authorization are exempt from the accounting requirement.

(4) the date/period of time during which the disclosure occurred (or may have occurred) including the date of the last such disclosure during the accounting period;

(5) the name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(6) a statement that the PHI of the individual may or may not have been disclosed for a particular protocol or research activity.

7.3. Participant access to records.

7.3.1. Right to Access.

In accordance with subparagraph 10.1 of this policy directive, individuals have the right to inspect and obtain a copy of PHI about themselves that is maintained by the Office of Mental Health in a Designated Record Set.

7.3.2. Designated Record Set.

In cases where an Office facility is engaged only in research and it is not simultaneously providing treatment to the research participant, it may be unlikely that a Designated Record Set is maintained. If so:

(a) any research records or results that are actually maintained by the Office of Mental Health as part of a Designated Record Set are accessible to research participants unless an exception, as set forth in subparagraph 10.1, applies; and

(b) an individual's right to access his/her Designated Record Set may be suspended while a clinical trial is in progress, provided the research participant agreed to this denial of access when consenting to participate in the clinical trial. In addition, the Office of Mental Health must inform the research participant that the right to access PHI will be reinstated at the conclusion of the clinical trial[35].

7.4. Transition provisions.

7.4.1. Use/disclosure of Research PHI Prior to Effective Date.

The Office of Mental Health may use/disclose PHI that was created or received for research, either before or after April 14, 2003, if the Office obtained any of the following prior to April 14, 2003:

(a) an authorization or express legal permission from the individual to use/disclose PHI for the research; or

(b) the informed consent of the individual to participate in the research; or

(c) a waiver of informed consent by an IRB in accordance with the Common Rule or an exception under the Food and Drug Administration's human subject protection regulations at 21 CFR §50.24.

[35]These notifications are contained in the Notice of Privacy Practices for Research Facilities, which should be utilized for this purpose.

8. PROCEDURES REGARDING INFORMATION DISCLOSURES:

8.1. Recording Disclosures.

8.1.1. Procedure Required.

Each facility must establish and implement a routine procedure for recording disclosures of information from patient designated record sets, regardless of a patient's legal status.

8.1.2. Recording Disclosures.

Whenever a disclosure of information from a patient's designated record set is made to a third party, a notation of such disclosure must be made in the patient's clinical record, including electronic medical records, in accordance with facility procedure.

8.1.3. Content of Recording Notations.

At a minimum, each notation must identify the nature of the information disclosed, the date of the disclosure, the purpose of the disclosure, and to whom the disclosure was made.

8.2. Verification - General Requirements.

8.2.1. Verification Standard.

Except with respect to disclosures made pursuant to subparagraph 6.4 of this policy directive (i.e., disclosures made after giving the patient the opportunity to agree or object), the Office of Mental Health must make good faith efforts to verify the identity of the person requesting PHI and the authority of such person to access the PHI (if not previously known).

8.2.2. Reasonable Reliance on Documentation, Statements, Representations

If a disclosure is conditioned under this policy directive, or applicable federal or state regulations, on particular documentation, statements, or representations from the person requesting the PHI, the Office may rely, if reasonable under the circumstances, on documentation, statements, or representations that on their face meet the applicable requirements.

8.2.3. Public officials.

(a) With regard to verifying the identity of public officials, the Office of Mental Health may rely, if reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of a public official:

(1) if the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of governmental status;

(2) if the request is in writing, on appropriate government letterhead;

(3) if the disclosure is to a person acting on behalf of a public official, a written

statement on appropriate government letterhead that the person is acting with authority, or other evidence of agency (e.g., a contract for services, Memorandum of Understanding, or purchase order) that the person is acting on behalf of the public official.

(b) To verify the authority of public officials, the Office of Mental Health may rely, if reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of a public official:

(1) a written statement of legal authority under which the information is requested, or, if a written statement would be impractical, a verbal statement of such authority; or

(2) a request made by legal process, warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal is presumed to constitute legal authority.

8.2.4. Professional Judgment.

Verification requirements are met if the Office of Mental Health relies on the exercise of professional judgment, or acts on good faith belief, in making a use or disclosure in accordance with this policy directive.

8.3. General procedure for handling telephone requests for information.

8.3.1 Standard.

With the exception of uses and disclosures that, with patient agreement, may be disclosed as facility directory information under subparagraph 6.4.1 of Section 6 of this directive, as a general rule, information regarding patients is not permitted to be disclosed in response to a telephone request, since it may not be known whether or not the patient has authorized the disclosure and due to the difficulty in verifying the identity of the caller and ensuring the security of the transmission. Therefore, telephone requests for patient information must be handled in accordance with the procedures established in this paragraph.

8.3.2. Procedure.

Callers must be advised that it is against Office of Mental Health policy to provide information about patients over the telephone, including informing the caller whether or not the individual in question is or is not a patient of the facility or program. They may then be given the option of providing their requests for information in writing, on letterhead (all such written requests must contain original signatures). In the alternative, the caller can provide his/her name, phone number, relationship to the patient and/or reason for the call. The caller should then be advised that if the patient is, in fact, being treated at the facility or program, the call will be returned after appropriate follow up. If the caller selects the latter option, the information provided by the caller should be promptly forwarded to an appropriate member of the patient's treatment team for further handling.

8.3.3. When Permitted.

In cases where information requested for the purpose of treatment, payment, or health care operations is sought by means of a telephone call, the recipient of the call is

certain that the disclosure is permissible (e.g. the call is made by a physician from an acute care hospital that is providing emergency care to the patient and quickly needs information for treatment purposes), and the call recipient relies on the exercise of professional judgment, or acts on good faith belief, and employs reasonable efforts to verify the caller, the PHI may be disclosed over the telephone[36].

8.3.4. Documentation.

All written requests for information or documentation of requests for information must be appropriately retained in accordance with facility policy, so that they are easily accessible by authorized members of the Office of Mental Health workforce.

8.4. General procedure for handling inquiries regarding deceased patients.

8.4.1. Standard.

Under both New York State law and the HIPAA Privacy regulations, an individual's privacy rights with regard to PHI do not change upon his or her death. A genealogist, even if a related family member, generally has no legal entitlement to non-public medical information. Therefore, all requests for information regarding deceased individuals must be in writing, and, when receiving requests for information about a deceased individual, the procedures established in this paragraph must be taken.

8.4.2. Vital Records.

Birth records, death records, and marriage records are considered Vital Records in New York State and generally can be accessed by the public. Such records can be obtained through the New York State Department of Health. More information on how to obtain these records is contained on the New York State Vital Records website at www.doh.state.ny.us. Facility staff may wish to direct inquiries to this resource.

8.4.3. Requests by Qualified Researchers.

If the request is from a qualified researcher[37], it is permissible to release the information if the written request for information contains all of the following:

(a) a representation that the use or disclosure sought is solely for research on the PHI of decedents;

(b) documentation of the death of the subject individuals; and

(c) representation that the PHI for which the use or disclosure is sought is necessary for the research purposes.

8.4.4. Requests by Family or Other Persons.

If the request is from a family member or other individual:

---

[36]This provision is intended to address, for example, routine uses and disclosures that are made over the telephone to other known service providers for the purpose of ongoing coordination of care.

[37]Approval of an Institutional Review Board or other committee specially constituted for the approval of research projects at the facility remains a requirement.

(a) If such person was otherwise involved in the care (or payment for care), of the patient prior to death, appropriate information may be provided unless doing so would be inconsistent with any prior expressed preference of the patient of which the provider is aware. The information that can be provided must be relevant to the person's involvement in the care or payment of care. (e.g., the circumstances that led to a patient's passing may be shared with a sibling who is asking about the patient's death; or billing information may be disclosed to a family member of a decedent who is assisting with wrapping up the decedent's estate). These types of disclosures are permitted, not required, and thus, if the provider questions the relationship of the person to the decedent or otherwise believes, based on the circumstances, that disclosure of the decedent's protected health information would not be appropriate, the disclosure should not be made.

(b) If a representation is made that the information is relevant to the treatment of a family member, the information may be released to the family member's physician, provided the physician submits a written request on the family member's behalf.

(c) If a representation is made that the individual is the executor of the deceased person's estate, or otherwise has legal authority to act on behalf of the deceased individual or his/her estate[38], the information can be released.

(d) If the information is being sought for general genealogy purposes and none of the conditions in this subparagraph, subparagraph 8.4.2, or subparagraph 8.4.3 are met, nor is there any other regulatory exception under which the information could appropriately be released, the information cannot be released. The individual requesting the information should be advised that under agency policy and current interpretation of federal regulations governing the privacy of individually identifiable health information, 45 C.F.R. Parts 160 and 164, the information cannot be released.

8.4.5. Historical Records

HIPAA limits the period for which covered entities must protect health information to 50 years after a person's death. However, the federal Department of Health and Human Services has also stated that covered entities may continue to provide privacy protections to decedent information beyond the 50 year period. Because the New York State Mental Hygiene Law does not similarly remove privacy protections from the clinical records of decedents after a period of time, if available, such information should not be released unless specifically permitted under other New York State law.

8.4.6. Review Required Prior to Release.

In all cases, the record must be reviewed prior to its release to ensure it does not infringe upon the privacy rights of any other individual who may be named in the record.

[38]Guidance on determining whether or not an individual "has the legal authority to act on behalf" of a patient is not specifically provided in the HIPAA Privacy Regulations, but the Office for Civil Rights 12/4/02 Implementation Guidance to the Privacy Regulations (p.34) indicates that a deceased individual's legally authorized executor or administrator, or a person who is otherwise legally authorized to act on the behalf of the deceased individual of his or her estate, is a personal representative with respect to PHI relevant to such representation. In the case of uncertainty in this regard, consult Counsel's Office.

8.5. Patient photographs

8.5.1. Standard.

For purposes of this policy directive, photographs, videotapes, and comparable images of patients, when created or received by a facility, constitute PHI.

It is permissible for facilities to take still photographs, videotapes, and scanned printouts of patients for treatment and health care operations purposes (e.g. as a method of identification). Such material, however, must be safeguarded from inappropriate use or disclosure to the same degree as any other type of PHI.

8.5.2. Required Notification.

(a) Notification to patients that a facility may use and disclose PHI in the form of photographs or other images for treatment or health care operations purposes shall be included in the Notice of Privacy Practices that is distributed in accordance with section 9 of this policy directive.

(b) In the event that it is not possible to provide the Notice of Privacy Practices prior to recording the patient's image for treatment or health care operations purposes, such images may be recorded if there is no other practical alternative. The Notice must be provided as quickly thereafter as feasible.

8.5.3. Informal Photographs/Videography.

In some circumstances, staff may wish to take informal photographs or videotapes of patients engaged in recreational activities or outings to document enjoyable memories that may later be displayed internally within the facility. Although the purpose and use of such photographs or videotapes is related to treatment and, as such, is incorporated within subparagraph 8.5.2 of this paragraph, patients should be given the opportunity to agree or object to be photographed or videotaped in this manner before their images are recorded and/or displayed within the facility.

8.6. Facsimile Transmission of PHI.

8.6.1. Standard.

If there are no other timely or reasonable alternatives, and provided appropriate safeguards are followed, it is acceptable to transmit PHI via facsimile (fax) in accordance with a permissible use or disclosure and after following any requisite authorization procedures. Workforce members must limit information transmitted to that necessary to meet the requester's needs.

8.6.2. Procedures.

Reasonable efforts must be made to ensure the facsimile transmission is sent to the appropriate destination. These reasonable efforts must include, at a minimum:

(a) obtaining the name and phone number of the party receiving the information;

(b) verifying the fax phone number with the intended recipient of the information prior to transmission of the document (this is particularly critical for a new requester of information). When feasible, sender and information recipient shall agree on a

time to transmit the document, or take other appropriate steps, in order to reduce the time lag between transmission and pick-up;

(c) verifying the receipt of the information to the appropriate party, which may include requesting the information recipient to confirm his/her receipt, if there is any question of confidentiality on the receiving end;

(d) to the greatest extent reasonably possible, destination numbers must be pre- programmed into the machine to eliminate errors in transmission from misdialing;

(e) locating fax machines in secure areas (and never in areas that are open to the public), and limiting access to them as appropriate;

(f) establishing procedures, at each facility, for ensuring that incoming faxes are properly handled and are not left sitting or near the machine but are distributed to the proper persons expeditiously while protecting confidentiality during distribution; and

(g) the use of computer software to fax a document shall not be processed through the use of Internet technologies, unless encrypted using an encryption algorithm that has been approved by the Office of Mental Health Information Security Office.

8.6.3. Documentation.

A notation recording the information disclosure must appropriately be made, in accordance with facility policy, indicating what information was transmitted, to whom, where the information was sent, and the date and time that the information was sent. The fax cover sheet must be filed with such notation.

8.6.4. Cover Page.

The fax cover page must be on Office of Mental Health or applicable facility letterhead, and must contain a confidentiality notice that indicates, at a minimum, that the information is confidential and prohibits its redisclosure. The fax cover page must also include:

(a) sender's name;

(b) business address and phone number;

(c) business fax number;

(d) information recipient's name;

(e) information recipient's business address and phone number;

(f) information recipient's business fax number;

(g) transmission date and time (if not stamped by machine) and machine name, if available; and

(h) a standard OMH confidentiality mis/transmission footer.

8.6.5. Identification of Pages as Confidential.

Whenever appropriate, all pages of a facsimile, including the cover page, must be marked confidential.

8.6.6. AIDS/HIV Information.

PHI that contains AIDS/HIV information should never be transmitted via facsimile unless absolutely necessary. If done, however, in addition to all of the other requirements set forth in subparagraphs 8.6.1 through and including 8.6.5, the following shall apply:

(a) If Form OMH 11 (not OMH 11-C) is used for this purpose, a "No Redisclosure of HIV Related Information" form must accompany the Transmission. Regardless of the form that is used, a notation that the HIV information was disclosed must be made in accordance with facility procedure; and

(b) the recipient of the information must be notified of the time of transmittal, and the facility shall take all reasonable efforts to ensure that an authorized person is present at the fax machine at the time of transmission.

8.7. Access to Information by the Media - General Procedures[39].

8.7.1. Standard.

It is the legal and ethical responsibility of the Office of Mental Health to protect each patient's right to confidentiality with respect to information regarding his/her care and treatment. In accordance with Section 33.13 of New York State Mental Hygiene Law and the HIPAA Privacy regulations, such confidential information shall generally be disclosed only with the written informed consent of the patient or his/her personal representative, which shall satisfy the procedural requirements set forth in paragraph 6.5 of this directive. It is the concurrent responsibility of the Office, as a State agency, to inform the public of agency activities and to respond appropriately to inquiries from the media. To the extent that a conflict may occur in fulfilling these responsibilities, it is the policy of the Office that such a conflict be resolved in a manner which is consistent with the patient's best interests.

8.7.2. Principles and Procedures: Statements regarding Office policies, facilities, and activities.

(a) All statements in response to media inquiries, as well as any other formal statements to the media, shall be issued by the Central Office Director of Communication, field office director, facility director, or others as designated by the Commissioner, field office director, or facility director. The Central Office Director of Communication, who is responsible for coordinating information on all requests from the media, must be notified prior to the release of all such statements.

(b) Except as otherwise provided in this subparagraph, no statements issued to the media shall disclose PHI/confidential information unless:

[39]These provisions supersede OMH Official Policy Directive QA-620.

(1) the media has a demonstrable need for such information, the disclosure is not reasonably expected to be detrimental[40] to the patient or others, and written informed consent has been obtained from the patient or the patient's personal representative in accordance with the procedural requirements set forth in paragraph 6.5 of this directive; or

(2) a court order requires such disclosure to the media.

(3) If a patient has been officially charged with the commission of a crime, the public has a substantial and legitimate interest in information regarding criminal activity in the community and the alleged participants. However, unless the patient has authorized a disclosure to the media in accordance with paragraph 6.5 of this directive, disclosures of PHI/confidential information can be made only to government officials involved in the investigation or prosecution of the case. Media requests for information or inquiries under these circumstances must be directed to such officials.

8.7.3. Principles and Procedures: Access to Facilities.

(a) The media may visit a State-operated psychiatric facility only under the following conditions:

(1) a formal request has been submitted by the media to the facility director prior to the planned visit;

(2) the Central Office Director of Communication has been notified by the facility director regarding requests for visits by the media; and

(3) prior approval of the media's request has been granted by the Commissioner or the facility director.

(b) During an approved visit at a State-operated psychiatric facility, the media may interview or photograph patients for public information and education purposes only under the following conditions:

(1) the patient must be informed of the nature of the media contact and of his/her right to refuse to participate; and

(2) written informed consent has been obtained in accordance with paragraph 6.5 of this directive via the patient's execution of OMH Form 446A (Consent for Patient Photograph), and/or OMH Form 445A (Consent for Patient Interview), as applicable, or only de-identified information is utilized in any story, program, or filmed account which results from the media contact such that the identity of the patient cannot reasonably be determined. In no event shall censor's marks be used as a means of shielding a patient's identity.

9. NOTICE OF PRIVACY PRACTICES:

9.1. Patient Right to Notice.

Except as otherwise provided in subparagraph 9.2.1 of this section, a patient has a right to adequate notice of the uses and disclosures of his/her PHI that may be made by or on behalf of the Office of Mental Health, and of the patient's rights and the Office of Mental Health's legal duties with respect to his/her PHI.

[40] i.e., result in mental or physical harm.

9.2. Use of Standard Notice.

Central Office shall supply each facility with an official Office of Mental Health Notice of Privacy Practices template, which shall be used for the purpose set forth in paragraph 9.1 of this section[41]. Because the Notice of Privacy Practices must contain the requisite contents set forth in 45 C.F.R. Section 164.520(b), all facilities must utilize such official Notice unless otherwise authorized by the Commissioner.

9.2.1. Special Provisions - Inmates.

Neither an inmate of a correctional institution nor a forensic patient has a legal right to receive a Notice of Privacy Practices. However, if practical and appropriate, facilities may opt to do so in their own facility policies and procedures.

9.3. Revisions to Notice.

Whenever there is a material change to the uses or disclosures, the individual's rights, the Office of Mental Health's legal duties, or other privacy practices described in the notice, Central Office shall revise and redistribute a Revised Notice of Privacy Practices to each facility. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflecting the change.

9.4. Provision of Notice.

Each facility or program must establish a procedure to provide, and shall provide, its patients (and personal representative of the patient, if applicable) with the Notice of Privacy Practices at the time of first service delivery. It is permissible to provide a short notice that briefly summarizes the patient's rights, as well as other information, provided that the standard Notice of Privacy Practices is layered beneath such short notice.

9.4.1. Good Faith Effort/Written Acknowledgment.

Every reasonable effort must be employed to obtain the written acknowledgment of the patient indicating that he or she has received the Notice. If such written acknowledgment cannot be obtained, a notation must be made explaining the reasons for failing to obtain the acknowledgment. Whenever practical, the facility must make continued attempts to obtain such acknowledgment as reasonable and shall document all such attempts. A sample Notice of Privacy Practices Acknowledgement Form is included with the Notice of Privacy Practices Template in Appendix 6. Facilities may use this form, develop their own, or modify existing forms for this purpose.

9.4.2. Posting of Notice.

The current Notice in effect (i.e., the original Notice or any subsequent revisions) must be prominently posted at each service delivery site. Copies must be available for patients to access at any service delivery site.

9.4.3. Inclusion on Website.

The Notice of Privacy Practices shall be posted on the Office of Mental Health's web site and shall be available electronically from such web site.

[41]A copy of the Standard Notice is included in the Appendix to this policy directive. Central Office may produce different versions of the Notice for use by facilities as appropriate, depending on whether a facility is primarily involved in treatment or research.

9.5. Documentation Requirements.

The Office of Mental Health must retain copies of all versions of Notices issued for a period of at least six years from the later of the date of creation or the last effective date. Such copies shall be retained by the Central Office.

10. PATIENT RIGHTS RELATED TO PHI:

10.1. Right of Access by Qualified Persons to Designated Record Set[42]

10.1.1 Right to Access Designated Record Set

Qualified persons have a right to access (i.e., inspect and obtain a copy of) PHI in a Designated Record Set, for as long as the PHI is maintained in the Designated Record Set, except for:

(a) information contained in the Designated Record Set that has been compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding[43]; or

(b) PHI contained in the Designated Record Set that is maintained by the Office of Mental Health and that is subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), to the extent the provision of access to the patient would be prohibited by law or exempt from CLIA.

10.1.2. Request for Access.

(a) A request for access to all or part of a Designated Record Set must be made by the qualified person in writing to the identified contact person at the facility, as indicated in the Notice of Privacy Practices. Upon receipt of a request for access, at the discretion of the facility director or designee, appropriate staff may discuss with the qualified person to clarify what information is actually needed and otherwise review the request with the individual.

(b) Because the Designated Record Set includes information that may not be centralized in one location (e.g. financial information may be located at the Patient Resource Office), it may be necessary to coordinate review of the request with other appropriate workforce members to ensure that all relevant information is considered in the course of the review (e.g., there may be a clinical reason to consider when reviewing a request to access fiscal information).

(c) The facility director or designee must respond to the request within 10 days of receipt of the request, in accordance with the actions prescribed in either subparagraph 10.1.5. or 10.1.6.(b), as applicable.

[42]These provisions supersede OMH Official Policy Directive QA-615.

[43]Note that this provision is intended to reference information that generally would be protected by the attorney- client privilege. It is not intended to be interpreted to mean summaries used for documents prepared for court that, under New York State law, are routinely included in the clinical record and are available for review, e.g., the mental hygiene calendar for retentions and Model Competency Reports for certification back to court.

(1) If unable to act on the request within such time frame, the facility director or designee may extend the time for such actions by no more than 30 days, provided that the individual is given a written statement of the reasons for the delay and the date by which the action on the request will be completed.

(2) Only one such extension of time for action on a request for access is permitted.

(d) If a request for access to all or part of the Designated Record Set represents a second or subsequent request for information that was previously denied by the facility, and the request is submitted again by the same qualified person, the facility director or designee must make a determination to grant or deny access each time a request is received and respond accordingly. Since the facts and circumstances of denial may change over time, such determination cannot be made in advance or on an ongoing basis.

(e) All correspondence and documentation related to a request for access to all or part of a Designated Record Set must be filed in the patient's clinical record. All responses to requests for access must be made on the form Acknowledgement of Request for Access to, Amendment or Correction of Records, 323 ADM (MH).

(f) Each facility must establish procedures to ensure documentation and retention, in accordance with OMH Official policy directive OM-740 (Records Retention) or 6 years, whichever period of time is longer, of the Designated Record Sets subject to access and the names or titles of persons responsible for receiving and processing requests for access.

(g) Access to electronic health records. In the event that a facility uses or maintains an electronic health record with respect to an individual's PHI:

(1) Individuals must be provided with a copy of their PHI that is maintained as electronic PHI in the electronic form and format they request, if such format is readily producible. If the requested format is not readily producible, the facility must offer to produce the electronic PHI in at least one readable electronic format.

(i) While facilities are not required to purchase software or hardware to accommodate requests for various types of formats, it is the expectation that they should be able to provide some form of readable copy.

(ii) A hard copy may be provided if the requesting individual rejects any of the offered electronic formats.

(2) The electronic copy that is provided must include all electronic PHI held by the facility in a designated record set, or appropriate subset if only specific information is requested, at the time the request is fulfilled. If the electronic PHI contains a link to images or data, the images or other data must be included in the electronic copy that is provided.

(3) If records are in mixed media (i.e., some paper and some electronic PHI), a combination of electronic and hard copies may be provided to the individual.

(4) If the individual chooses, to direct the facility to transmit such copy directly to an entity or person designated by the individual, the individual has the right to do so, provided that any such choice is clear, conspicuous, and specific;

(5) Facilities are not required to use an individual's flash drive or other device to transfer the electronic PHI if the facility has any security concerns regarding the external portable media.

(6) If an individual requests to receive the electronic copy via unencrypted email and secure email is not available, he or she should be advised that it is against the policy of the Office of Mental Health to share PHI via unsecure email due to the risk that the information could be read by a third party.

(7) any fee that the facility may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy, summary, or explanation is in an electronic form shall not be greater than the facility's labor costs in responding to the request for the copy, summary or explanation

(8) The following may be included in fees:

(i) labor costs for copying PHI, whether in paper or electronic form;

(ii) the costs of supplies for creating electronic media (e.g., discs, flash drives) if the individual requests the copy on portable media; and

(iii) postage, if the individual requests mailing or delivery of electronic media.

(9) The following may not be included in fees:

(i) costs of new technology, maintaining systems for electronic PHI, data access, and storage infrastructure; and

(ii) retrieval fees (whether a standard fee or actual costs) for electronic copies.

10.1.3. Review of Request for Access.

(a) Upon receipt of a written request for access to all or part of a Designated Record Set, the facility director or designee must identify a designated staff member to review the information requested and provide a recommendation to grant access (in whole or in part), or deny access (to all or part), of a Designated Record Set.

(1) When the request for access concerns a patient about whom the facility has current clinical information the designated staff member should discuss the patient's clinical condition and the potential effect of granting access with the patient's treatment team.

(2) When the request for access concerns a patient over the age of 12 and is made by a qualified person other than the patient, the designated staff member must determine, in consultation with the patient's treatment team, whether or not the patient should be notified of the request. Such determinations should be based on a consideration of the patient's current clinical condition, if known, and other relevant factors. As indicated, notification of the patient and his/her response to the request for access, if any, must be documented in the patient's clinical record.

(3) When the request for access concerns a patient over the age of 18 and is made by a committee for an incompetent or guardian of the person appointed pursuant to Article 81 of the Mental Hygiene Law or Article 17-A of the Surrogate's Court Procedure Act, the patient must be notified of the request.

(b) In reviewing a request for access to all or part of a Designated Record Set, the designated staff member must identify all relevant facts and circumstances, including, but not limited to, the following:

(1) the patient's need for, and the fact of, continuing care and treatment;

(2) the extent to which knowledge of the information in a Designated Record Set would reasonably be expected to have an adverse effect on the health or safety of the patient or others, including the life or physical safety of the patient or others;

(3) the extent to which the Designated Record Set contains sensitive information provided in confidence by family members, friends, and/or others;

(4) where the request for access is made by the guardian or parent of a minor patient, the reasonable expectation that access to a Designated Record Set would have a detrimental effect on the professional relationship between staff and the minor, the minor's care and treatment, and/or the minor's relationship with the guardian or parent;

(5) where the request for access is made by a qualified person other than the patient, the extent to which a clinical record contains sensitive information provided by the patient which would be harmful to the patient's relationship with others;

(6) where a patient over the age of 12 has been notified of a request for access by another qualified person, the patient's objection to such access;

(7) where the request for access is made by a minor patient, the minor's age; and

(8) any other relevant information.

(c) The designated staff member must submit a written recommendation to grant or deny access to the facility director or designee. The facility director or designee will make the final determination, in accordance with subparagraph 10.1.4 or 10.1.6 as applicable, and will communicate the decision to the qualified person as prescribed in such subparagraphs, as applicable.

(d) To the extent possible, the qualified person must be given access to any information requested after excluding the information for which the facility has grounds for denying access. If the facility does not maintain the information for which access has been requested, but knows where it is maintained, the facility must inform the qualified person where to direct the request for access.

10.1.4. Grounds for Denial of Access.

Access to all or part of a Designated Record Set may be denied for any of the following reasons; in these cases, the qualified person has a right to request review of the determination, in accordance with the procedures set forth in paragraph 10.1.5 of this Section:

(1) the information is not part of the Designated Record Set;

(2) the information was compiled in anticipation of litigation;

(3) the qualified person is a forensic patient or an inmate, as both are defined in Section 3 of this policy directive, and the facility director or designee has determined that provision of access would jeopardize the health, safety, security, custody, or rehabilitation of the qualified

person or other individuals, or the safety of any officer, employee, or other person at the facility or responsible for transportation of the qualified person;

(4) the information was collected in the course of research that includes treatment, and the subject of the information agreed to a temporary suspension of the right of access during the research period;

(5) the information is protected under the federal Privacy Act (5 USC 552a);

(6) the information was obtained from someone other than the Office of Mental Health under a promise of confidentiality and the access requested would likely reveal the source of the information;

(7) it has been determined that access would be reasonably likely to endanger the life or physical safety of the qualified person or another individual;

(8) when the PHI makes reference to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person, or

(9) the request for access has been made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

10.1.5. Procedures when Access is Denied.

(a) When the facility director or designee determines that access to the Designated Record Set is denied (or granted only in part), a prepared summary of the record (or those portions withheld) may be provided to the qualified person at the discretion of the facility director or designee.

(b) The facility director or designee must provide a timely, written denial to the qualified person within 10 days of the date of the request for access, unless an extension has been obtained by the facility in accordance with subparagraph 10.1.2.(b) of this policy directive. The denial must be in plain language and must contain:

(1) the basis for the denial;

(2) a statement of the qualified person's rights, including a description of how the qualified person may exercise his/her rights by appealing the denial to the appropriate Clinical Records Access Review Committee, without cost, and the process for filing such an appeal; and

(3) a description of how the qualified person may complain to the Office of Mental Health or the U.S. Secretary of Health and Human Services (as indicated in the Notice of Privacy Practices). The description must include the name, or title, and telephone number of the contact person(s) designated in the Notice of Privacy Practices.

(c) Appeal process

(1) If a qualified person wishes to appeal a denial for which an opportunity for review is provided, he/she must submit a written appeal to the facility. The facility director or designee must submit the following materials to the chairperson of the appropriate Clinical Records Access Review Committee within 10 days of receipt of the appeal:

(i) the appeal;

(ii) a copy of the Designated Record Set or the specific information requested from the Designated Record Set; and

(iii) a statement of the specific reason(s) which form the basis of the facility's denial.

(2) The facility director or designee must inform the qualified person how to contact the Clinical Records Access Review Committee and that the qualified person will have the opportunity to be heard by the Committee.

(3) Upon notification of a determination by the Committee to grant access to all or part of a Designated Record Set, the facility director must ensure that access is granted accordingly to the qualified person in the manner set forth in subparagraph 10.1.6 of this paragraph.

(d) Clinical Records Access Review Committee.

(1) The Clinical Records Access Review Committee (formerly known as the Medical Access Review Committee) is responsible for reviewing appeals filed by qualified persons who have been denied access to all or part of a Designated Record Set by a State operated or State licensed mental health facility.

(2) Composition.

(i) The Committee shall consist of no less than 3 and no more than 5 members.

(iii) The Committee must have one physician member licensed to practice medicine in New York State. Other committee members may include psychologists, nurses, social workers, or other mental health practitioners, including individuals currently in administrative titles, who meet the criteria of a designated staff member The Committee must also be constructed in such a way as to ensure, for each denial reviewed, a New York State licensed health care professional who was not directly involved in the initial decision to deny access participates in the review of the decision to deny access.

(3) Organization and Administration.

(i) The Committee must confer at intervals sufficient to respond to appeals within the designated time frame.

(ii) The Committee may conduct its business through meetings, conference calls or written communication.

(ii) A Committee member must disqualify himself/herself from the review of an appeal if a conflict of interest or bias exists. If necessary to maintain a minimum of 3 members, the chairperson shall appoint an alternate to review

the appeal.

(6) Responsibilities.

(i) Within a reasonable period of time, but no later than 45 days, of receipt of a qualified person's appeal, the Committee must initiate a review of the materials provided. Within 15 days of initiating the review, the committee must issue a determination to grant access in whole or in part or to deny access to all or part of a Designated Record Set.

(ii) In considering the appeal, the Committee must determine whether the grounds for denial outweigh the qualified person's right of access. The Committee may request additional information from the facility director and/or the qualified person as necessary. Upon request, the Committee may provide the qualified person with the opportunity to be heard by the Committee either face to face or through written communication.

(iii) The Committee must promptly notify the facility director and the qualified person of the Committee's determination. When the Committee denies access (or grants access only in part), the Committee must inform the qualified person in writing of the reason(s) for denial or withholding of certain portions of the record and his/her right to judicial review and that such review must be commenced by the qualified person within 30 days of notification of the Committee's denial.

(7) Data Collection and Maintenance.

The Committee is responsible for collecting and maintaining data on the number of determinations made to grant access in whole, grant access in part, and deny access. These data should distinguish between determinations made for State operated mental health facilities and those made for State licensed mental health facilities.

10.1.6. Procedures when Access is Granted.

(a) If the facility director or designee determines that access to the Designated Record Set will be granted, in whole or in part, the facility must provide the qualified person with access to the information in the form or format he or she has requested, if it is readily producible in such form or format. If not so readily producible, the information may be provided in a readable hard copy or other form or format as mutually agreed to, either by arranging for a convenient time and place for inspection and provision of copies, or mailing the information at the qualified person's request. The facility may encourage the qualified person to come to the facility to review the records, if possible.

(1) If the information is maintained in more than one place, the information need only be produced once in response to a current request for access.

(2) The facility may provide a summary of the information in lieu of providing access, or may provide an explanation of the information to which access is provided if the qualified person, in advance, agrees.

(b) Time frames.

(1) If access to all or part of a Designated Record Set has been requested, and the qualified person elects to inspect the records, notice as to which

portions of the request have been granted and the opportunity for the qualified person to inspect the records must be provided within 10 days of the date of receipt of the request.

(2) If access to all or part of a Designated Record Set has been requested, and the qualified person elects to receive copies of the records without previous inspection, notice as to which portions of the request have been granted and provision of the copies of the information must be provided within 30 days of the date of receipt of the request, to allow for written notification and recovery of charges.

(3) If access to all or part of a Designated Record Set has been requested, and the qualified person elects to receive the information in a readily producible form or format other than via inspection or readable hard copies, notice as to which portions of the request have been granted and provision of the information must be provided within 30 days of the date of receipt of the request.

(c) Fees

(1) A qualified person who is granted access to all or part of a Designated Record Set may be required to pay a reasonable, cost-based fee for copying, or preparing a summary or explanation of the information, provided that the fee includes only the cost of copying supplies, postage, and labor for preparing the summary or explanation as agreed to by the qualified person. The copying fee shall not exceed 75¢ per page.

(2) The qualified person must be informed of the estimated cost of providing the requested information prior to the furnishing of the information. Appropriate facility staff should discuss with the qualified person what information is actually needed, and prepare access only to that information. Copying fees should be collected before copies are made, in the event that the qualified person modifies the request.

(d) Review of a Designated Record Set by a Qualified Person - Procedures

(1) Although access to records must be provided, to the extent possible, in the form or format requested by the qualified person, the facility director may set reasonable limitations on the time, place, and frequency of reviews.

(2) When a qualified person contacts facility staff to review records, an appointment should be scheduled that is mutually convenient. In the case of hearing-impaired or non-English speaking qualified persons, the facility director or designee must make a reasonable effort to obtain an interpreter. In the event that an interpreter cannot be obtained, the qualified person may be accompanied by an interpreter of his/her choosing, subject to the approval of the facility director or designee.

(3) Every effort should be made to encourage the qualified person to review the Designated Record Set with a designated staff member. Staff participation, however, shall not be required as a condition for review. If the qualified person does not agree to staff participation, the facility director shall require that the review be observed by a staff member in order to ensure that the review is conducted in an appropriate manner.

(4) The facility must provide an area where the review may be conducted with the participation or observation of a staff member. During the review of a Designated Record Set, the qualified person may take notes on information in the record. However, the qualified person may not remove or alter any documents in a Designated Record Set. Upon request, the qualified person must be provided with copies of the information reviewed, if access has been granted to such copies, within 45 days of receipt of the request and in accordance with the provisions of this paragraph.

(5) When a patient reviews a Designated Record Set, the staff member who observes or participates in the review must prepare a note for inclusion in the patient's clinical record. This note must provide an overall summary of the review including, at a minimum, the patient's reaction during the review and any significant events that occurred during the review.

10.2. Right to Request Amendment of PHI.

10.2.1. Right to amend and right to deny request to amend.

(a) A qualified person has a right to dispute the accuracy of and/or request that the Office of Mental Health amend PHI or other information in the Designated Record Set for as long as the Office maintains the record sets.

(b) The Office of Mental Health has the right to deny the request for amendment if it determines that the PHI or other record:

(1) was not created by the Office of Mental Health, unless the qualified person provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the request;

(2) is not part of the Designated Record Set;

(3) is not available for inspection in accordance with paragraph 10.1.of this Section; or

(4) is accurate and complete.

(c) If the Office denies a request for amendment, the qualified person must be permitted to submit a statement of disagreement in accordance with subparagraph 10.2.3 (b) of this paragraph.

(d) Each facility must have a procedure for designating and documenting the titles of the persons or offices responsible for receiving and processing requests for amendments and maintaining documentation related to the amendment process.

10.2.2. Request for amendment and timely action.

(a) The Office of Mental Health must permit a qualified person to request that it amend PHI or a record maintained in the Designated Record Set and shall advise the qualified person, through its Notice of Privacy Practices, that such request must be in writing and justification and support for the request must be provided. Such support shall be indicated through a brief written statement supplying information and/or challenging the accuracy for inclusion in the clinical record. Each facility director shall designate to whom requests for amendment shall be submitted within its respective facility, which shall be indicated on the Notice provided by the facility.

(b) If a qualified person submits a request to amend PHI, in accordance with the instructions set forth in the Notice of Privacy Practices, the staff member who has been designated to receive the request shall have 60 days to act on it, as follows:

(1) the request may be granted, in whole or in part, or denied, in accordance with this subparagraph; or

(2) if more time is needed to comply, the facility may obtain one extension for up to 30 days, provided that the qualified person is notified in writing within the first 60 days after receipt of the request of the reasons for the delay and of the date by which action will be taken.

10.2.3. Accepting the amendment.

If the facility accepts the amendment, in whole or in part, it must:

(a) make the amendment by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment, i.e. the brief written statement prepared by the qualified person pursuant to subparagraph 10.2.2 (a);

(1) This statement shall be considered an amendment or correction of a clinical record and shall become a permanent part of the clinical record. Such amendments may be included in a general supplemental information section of the clinical record.

(2) When such a statement is a part of a clinical record, it must be released whenever the clinical record is released. Clinical records containing such statements must be flagged in some manner to ensure that the statements are appropriately released.

(b) inform the qualified person in a timely manner that the amendment has been accepted and obtain his/her identification of and agreement to notify relevant persons with which the amendment needs to be shared, as further set forth in (c) of this subparagraph;

(c) make reasonable efforts to inform and timely provide the amendment to:

(1) persons identified by the qualified person has having received PHI and needing the amendment; and

(2) persons, including Business Associates, that the facility reasonably knows to have PHI that is the subject of the amendment and who may have relied, or could foreseeably rely, on such information to the detriment of the qualified person.

10.2.4. Denying the amendment.

If the facility elects to deny the amendment, in whole or in part, it must:

(a) provide the qualified person with a timely, written denial in plain language that contains:

(1) the basis for the denial, in accordance with subparagraph 10.2.1 (b);

(2) a statement notifying the qualified person of his/her right to submit a written statement disagreeing with the denial, and informing him/her how to file such a statement;

(3) a statement that, if the qualified person does not submit a statement of disagreement, that he/she may request that the facility provide a copy of the qualified person's request and the denial with any future disclosures of the PHI that is the subject of the request; and

(4) a description of how the qualified person may complain to the Office of Mental Health (including the name or title, and telephone number of the contact person or office) or to the Secretary of HHS.

(b) Statement of disagreement. The facility must permit the qualified person to submit a written statement disagreeing with the denial and the basis for the disagreement. The facility may reasonably limit the length of the statement.

(c) Rebuttal statement. If a statement of disagreement is submitted, the facility has the right to prepare a written rebuttal to such statement. Whenever a rebuttal is prepared, the facility must provide a copy of it to the qualified person.

(d) Recordkeeping. The facility, as appropriate, must identify the record or PHI that is subject to the disputed amendment and append or otherwise link the request for amendment, the denial, any statement of disagreement by the qualified person, and any facility rebuttal to the Designated Record Set.

(e) Future disclosures.

(1) If a statement of disagreement has been submitted, the facility must include the material appended in accordance with (d) of this subparagraph, or, at the election of the facility, an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates.

(2) If a statement of disagreement has not been submitted, the facility must include the request for amendment and the denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the qualified person has requested such action in accordance with (a)(3) of this subparagraph.

(3) When a subsequent disclosure is being made using a standard electronic transaction in accordance with 45 CFR Part 162 that does not permit additional material to be included, the facility must separately transmit the material required by (e)(1) or (e)(2) of this subparagraph, as applicable, to the entity that is receiving the standard transaction.

(f) If the Office of Mental Health is informed by another Covered Entity of an amendment to a qualified person's PHI, it must make the amendment to the PHI in its own Designated Record Set in accordance with this subparagraph.

10.3. Right to Request Restrictions on Disclosures of PHI.

10.3.1. Standard.

(a) A patient has a right to request that a facility restrict the uses and disclosures of his or her PHI[44] made:

(1) for treatment, payment or health care operations purposes; or

(2) to family members, other relatives, close personal friends, or others involved with the patient's care or payment for his/her care.

(b) Notwithstanding subparagraph (a) of this paragraph, upon request of a patient, a facility must restrict disclosures of PHI to a health plan for payment or health care operations if the facility has already been paid in full by the patient for the health care services.

10.3.2. Facility's Right to Reject.

(a) The facility is not required to agree to a restriction of uses or disclosures of PHI that may be requested by a patient under subparagraph 10.3.1 (a), *unless*: the request is to restrict disclosures to a health plan for the purpose of carrying out payment or health care operations and is not otherwise required by law, and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the facility in full.

(b) The facility cannot agree to a restriction that prevents uses or disclosures that are permitted or required to be made to the patient, for a facility directory, or where the use or disclosure does not require the patient's permission. Furthermore, the facility should not agree to any restrictions unless it is certain that such restrictions will not, under any circumstances, compromise:

(1) the ability to provide effective care and treatment;

(2) the ability to receive payment for such care and treatment;

(3) the ability to monitor or oversee such care and treatment; and/or

(4) the health and safety of the patient or other persons.

(c) If it does agree with the restriction, the facility must document the agreed upon restriction in writing and abide by it. However, the facility is permitted to make a use or disclosure of the PHI to provide the patient with emergency treatment if the information is necessary to do so. In this case, if the information is disclosed to another health care provider, the facility must request that the information so disclosed not be further disclosed by that health care provider.

(d) The facility may terminate an agreed upon restriction if:

(1) the patient agrees to terminate the restriction, as documented in writing; or

[44]Though required, it is anticipated that this provision will have limited relevance to the operations of the Office of Mental Health.

(2) the facility gives notice to the patient that it is terminating the restriction. In this case, the termination is only effective as to PHI created or received after providing such notice.

10.4. Right to Request Confidential Communications.

10.4.1. Standard.

The facility must have a procedure that permits patients to request that communications including PHI be made by alternative means or at alternative locations[45], and must accommodate all reasonable requests. Such requests must be in writing and shall be made as indicated in the Notice of Privacy Practices.

10.5. Right to an Accounting of Disclosures.

10.5.1. Standard.

Patients have a right to receive an accounting of disclosures (not uses) of PHI made by the Office of Mental Health in the 6 years prior to the date upon which the accounting is requested.

10.5.2. Procedures.

Each facility must establish procedures to ensure that all disclosures that are subject to the right to an accounting of disclosures are routinely documented, such that they are readily accessible and producible in the event that a patient elects to exercise his/her right to such accounting. Such procedures must also facilitate the ability to comply with the documentation requirements of subparagraph 10.5.7 of this paragraph.

10.5.3. Exceptions.

The following information is not subject to the right of accounting of disclosures[46]:

(a) information that has been disclosed for treatment, payment, or health care operations purposes, provided, however, for facilities that use or maintain electronic health records, patients are entitled to receive an accounting of treatment, payment and health care operation disclosures made in the three years preceding the request for an accounting;

(b) disclosures made directly to patients (or their personal representatives) of PHI that is about them;

(c) disclosures permitted by the patient in accordance with paragraph 6.4 of this policy directive (i.e., for the facility's directory or to persons involved in the patient's care or other notification purposes);

[45]For example, a patient could request that any PHI that will be mailed to him/her be sent to a Post Office Box as opposed to his/her home address. Though required, it is anticipated that provision will have limited relevance to the operations of the Office of Mental Health.

[46]This provision contains a list of disclosures which are not subject to the right of an accounting of disclosures. In general, unless included on this list, disclosures made in accordance with paragraph 6.3 of this policy directive are, in fact, subject to the right of accounting. These include, for example: disclosures made to DOH to report communicable diseases; child abuse reporting; disclosures made as directed by subpoena.

(d) disclosures made pursuant to a written authorization by the patient in accordance with paragraph 6.5 of this policy directive; or judicial proceedings; disclosures made to the FDA for adverse events; and disclosures to law enforcement.

(e) disclosures made for national security or intelligence purposes;

(f) disclosures to correctional institutions, facilities that serve forensic patients, or law enforcement officials in accordance with paragraph 6.3 of this policy directive; or

(g) disclosures that occurred prior to April 14, 2003, provided, however, that patients shall retain the right to be informed of such disclosures in accordance with New York State Mental Hygiene Law Section 33.13(f).

10.5.4. Special Provisions: Health Oversight/Law Enforcement Disclosures.

The patient's right to receive an accounting of disclosures of PHI made to a health oversight agency or law enforcement official must be suspended for the time period specified by such agency or official if the agency or official provides a written statement which asserts that the provision of an accounting would be reasonably likely to impede the activities of the agency or official and which specifies a time period for the suspension. Such a suspension may be requested and implemented based on a verbal notification for a period of up to 30 days. Such verbal request must be documented, including the identity of the agency or official making the request. The suspension may not extend beyond 30 days unless the required written statement is submitted during that time period.

10.5.5. Content of the Accounting.

The written accounting must meet the following requirements:

(a) The accounting must include disclosures of PHI subject to the right to an accounting that occurred during the 6 years (or any shorter time period that is specified in the request) prior to the date of the request, including disclosures made by or to Business Associates.

(b) The accounting for each disclosure must include:

(1) date of disclosure;

(2) name of entity or person who received the PHI, and, if known, the address of such entity or person;

(3) a brief description of the PHI disclosed;

(4) a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure, or in lieu thereof, a copy of the patient's authorization or the request for a disclosure;

(5) if, during the time period for the accounting, multiple disclosures have been made to the same entity or person for a single purpose, or pursuant to a single authorization, the accounting may provide the required information for the first disclosure, and then summarize the frequency, periodicity, or number of disclosures made during the accounting period and the date of the last such disclosure during the accounting period.

10.5.6. Provision of the Accounting.

(a) The patient's request for an accounting must be acted upon no later than 60 days after receipt. Within such time period, the facility must:

(1) provide the accounting as requested, or;

(2) if unable to provide the accounting within 60 days, the time for response may be extended by no more than 30 additional days, provided that:

(i) within the first 60 days, the patient is given a written statement of the reasons for the delay and the date by which the accounting will be provided, and;

(ii) no additional extensions of time for response are requested.

(b) In the event the request for an accounting of disclosures includes disclosures made by Business Associates of a facility, the facility may:

(1) include disclosures made by a Business Associate in the facility's own accounting; or

(2) account only for its own disclosures and include a list of all Business Associates and their contact information for the individual, at which point the individual may contact those Business Associates directly to request an accounting of disclosures made by them. If a Business Associate receives a request for an accounting of disclosures directly from an individual, the Business Associate must provide the accounting directly to the individual directly.

(c) The first accounting in any 12 month period must be provided to the patient without charge. A reasonable, cost-based fee may be charged for additional accountings within the 12 month period, provided the patient is informed in advance of the fee, and is permitted an opportunity to withdraw or amend the request.

10.5.7. Documentation Requirements.

The facility must document, and retain documentation, in written or electronic format, for a period of at least 6 years, the following information:

(a) all information required to be included in an accounting of disclosures of PHI;

(b) all written accountings provided to individuals; and

(c) titles of persons or offices responsible for receiving and processing requests for an accounting from individuals.

11. BUSINESS ASSOCIATES - GENERAL PROCEDURES:

11.1 Standard.

(a) A "Business Associate" is a person or entity who, for or on behalf of the Office of Mental Health, (but not in the capacity of a workforce member), performs, or assists in the performance of, a function or activity for which the use or disclosure of PHI is necessary. It does not refer to other health or mental health providers who are rendering services to a patient, nor to another governmental agency that makes public benefit eligibility or enrollment determinations as authorized in law.

(b) The Office of Mental Health may disclose PHI to a Business Associate, or allow a Business Associate, to create or receive PHI on the Office of Mental Health's behalf, if the Office first obtains adequate assurance that the Business Associate will safeguard the PHI in a manner that complies with the HIPAA Privacy and Security regulations.

11.2 Procedures.

The Office of Mental Health must document these assurances through a written agreement, as follows:

(a) for contracts that are processed through the Office of Mental Health Central Business Office, requisite Business Associate contract provisions will be contained within the standard clauses for all Office of Mental Health Contracts, via Appendix F.

(b) for facility agreements or contracts that are not processed through the Office of Mental Health Central Business Office, standard Business Associate language, as provided by Central Office, must be included as appropriate by the facility.

(c) if the Business Associate is another governmental entity, a Memorandum of Understanding addressing the requisite terms shall be executed, unless reliance can be placed on other law that imposes upon the Business Associate requirements specified in subparagraph 11.3 of this paragraph. If the Business Associate is required by law to perform a function, activity or service on behalf of the Office of Mental Health, the Office may disclose PHI to the extent necessary to comply with that mandate as long as the Office documents an attempt to obtain the required assurances and the reasons that such assurances could not be obtained.

11.3 Business Associate Agreement Content Requirements.

The following standard provisions must be contained in any Business Associate Agreement, as applicable:

(a) Permitted uses and disclosures of PHI that are consistent with those authorized for the Office of Mental Health must be established, except that the agreement may permit the Business Associate to use or disclose PHI for its own management and administration if such use or disclosure is required by law or the Business Associate obtains reasonable assurance that the confidentiality of the PHI will be maintained.

(b) Provisions must be included[47] to ensure that the Business Associate will:

[47]Both Appendix F and the standard language provided to facilities by Central Office for inclusion in facility contracts or memoranda of understanding contain these requisite provisions.

(1) not use or disclose the PHI except as authorized under the agreement or required by law;

(2) use HIPAA compliant safeguards to prevent unauthorized use or disclosure;

(3) report breaches of unsecured PHI or other unauthorized uses or disclosures to the Office of Mental Health;

(4) execute Business Associate Agreements with any subcontractors or agents with whom they will share PHI;

(5) make PHI available for access by the patient or his/her personal representative, in accordance with applicable law and this policy directive;

(6) make PHI available for amendment, and incorporate any approved amendments to PHI, in accordance with applicable law and this policy directive;

(7) make information available for the provision of an accounting of uses and disclosures in accordance with applicable law and this policy directive;

(8) make its internal practices, books and records relating to its receipt or creation of PHI available to the Office of the U.S. Secretary of Health and Human Services for purposes of determining the Office of Mental Health's compliance with HIPAA Privacy regulations;

(9) if feasible, return or destroy all PHI upon termination of contract; if any PHI is retained, continue to extend the full protections specified herein as long as the PHI is maintained;

(10) authorize termination of the agreement by the Office of Mental Health upon a material breach by the Business Associate; this element of the agreement may be omitted if the Business Associate is another governmental entity and the termination would be inconsistent with the statutory obligations of the Office of Mental Health or the Business Associate; and

(11) comply with certain provisions of the Security and Privacy Rules as required by the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009, including, but not limited to, provisions mandating notification by a Business Associate to a Covered Entity of suspected breaches of privacy or security of protected health information.

11.4 Oversight Responsibilities.

If the Office of Mental Health knows of a pattern or practice of its Business Associate that amounts to a material violation of the agreement, the Office shall attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement, if feasible, and, if not, report the problem to the Office of U.S. Secretary of Health and Human Services.

11.5 Non-Business Associate Contracts/Services.

(a) In many instances, although a vendor or a contractor is providing a service to the Office of Mental Health, the nature of the relationship is not one of a Business

Associate since the services are not being provided to or on behalf of the Office or the provision of PHI is not necessary in order to perform such services[48].

However, even in these instances, indirect, or incidental, exposure to PHI is possible.

(1) In all of these cases, a Business Associate Agreement is not legally necessary.

(2) To adequately safeguard the confidentiality of PHI, facilities shall provide all such vendors with information that clearly outlines the need to protect the privacy of all patients at Office of Mental Health facilities, and that any PHI encountered, directly or indirectly, while performing the respective service must be treated as confidential.

(b) Conduits of PHI, such as the United States Postal Service, Unites Parcel Service, delivery truck line employees and/or their management, are not considered to be Business Associates of the Office of Mental Health.

(c) All visitors to Office of Mental Health facilities must be provided with a sign- in sheet that contains a prominent heading advising of the need to protect the confidentiality of all PHI that may be encountered during the visit. The heading shall be repeated on each page of the sign-in sheet.

(d) The Office of Mental Health may retain services from entities where disclosure of PHI is not limited in nature, but the work being performed is under the direct control of the Office. For example, some facilities have training contracts with educational institutions, wherein students of such institutions are placed at a facility for training experience. In these cases, workers such as the students (whether they are paid for their services or are volunteers) shall be considered part of the Office's workforce and shall receive training in accordance with subparagraph 4.4 of this policy directive. Although these entities themselves do not meet the legal definition of a "Business Associate," all contracts with such entities must include language that indicates that any worker (or student) performing services or participating in the training shall be considered part of the Office of Mental Health's workforce and their compliance with the HIPAA Privacy regulations, as well as the New York State Mental Hygiene Law, shall be required.

11.6. Additional Agreements: Confidentiality & Non Disclosure Agreement, Data Exchange Agreement, Computer Application Sharing Agreement.

In addition to the Business Associate Agreement, if the business relationship between the Office of Mental Health and its Business Associate entails the sharing of confidential data (which is defined to include PHI as well as other information determined by the Office to be "confidential") or access to Office of Mental Health computer information systems, execution of a standard Confidentiality & Non-Disclosure Agreement, Data Exchange Agreement, and/or Computer Application Sharing Agreement (as applicable) may be

---

[48]Examples of such services include janitorial services, routine maintenance services, or supply deliveries because the work performed for the Office of Mental Health does not involve the use/disclosure of PHI, and any disclosure of PHI that occurs in the performance of their duties (e.g., such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their duties, and could not be reasonably prevented.

required. Copies of these agreements may be obtained from the Information Security Office [49].

12. SECURITY MEASURES/ PHYSICAL AND TECHNICAL SAFEGUARDS:

12.1. Additional Reference: *New York State Office of Mental Health Information Security Policy*.

Specific guidance containing the physical and technical safeguards to be employed by the workforce in safeguarding PHI, including details regarding breach notification requirements, are contained in the New York State Office of Mental Health Information Security Policy.

12.2. Standard.

It is the policy of the Office of Mental Health that all members of its workforce shall preserve the integrity and confidentiality of PHI. All such workforce members must, in accordance with their respective duties:

(a) use their best efforts to ensure the accuracy, timeliness, and completeness of PHI data and ensure that appropriately authorized persons can access it when needed;

(b) implement reasonable safeguards to protect the security and integrity of all PHI, regardless of the medium in which it exists or through which it is transmitted;

(c) recognize that patients have a right of privacy, and respect such right consistent with providing high quality mental health care and with the efficient administration of the facility;

(d) act as responsible information stewards and treat all PHI as sensitive and confidential in accordance with applicable professional ethics, accreditation standards, and legal requirements;

(e) not divulge PHI in violation of the provisions of this policy directive and/or applicable law;

(f) when releasing PHI, take appropriate steps to prevent unauthorized redisclosures, such as specifying that the recipient of the data may not further disclose the information without patient authorization or as authorized by law; and

(g) remove patient identifiers whenever appropriate, such as in statistical reporting.

[49]Note that the term "confidential information," for purposes of these agreements, includes far more than PHI, e.g. OMH proprietary information. As such, their utility extends beyond this policy directive.

12.3. Breach Notification Requirements.

12.3.1. Definition of breach. A breach is the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. In general, any unauthorized acquisition, use, or disclosure of PHI is *presumed* to be a breach unless there is a low probability that the PHI has been compromised.

12.3.2. Exceptions. A breach does not include the unintentional acquisition, access or use of PHI by a member of a Covered Entity's workforce acting under the authority of a Covered Entity when made in good faith and within the course and scope of employment or other professional relationship, and there are no further actions to acquire, access or use the information. It also does not apply to inadvertent disclosures of PHI within the same facility or its Business Associate when the disclosure is from one individual to another and both are authorized to access the PHI.

12.3.3. Determining if a breach has occurred: To determine if a breach has occurred, the following must be considered:

(a) The potential breach must involve unsecured PHI. PHI that is de-identified or that is rendered unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified in guidance from HHS is exempt from notification.

(b) There must have been an impermissible use or disclosure (i.e., the potential breach must violate the HIPAA Privacy Rule). Violations of the Privacy Rule that do not involve the use or disclosure of PHI do not constitute a breach.

(c) If it can be demonstrated that there is only a *low probability* that the PHI has been compromised, a breach has *not* occurred. To make this determination, the performance of a fact specific risk assessment is necessary, taking into consideration at least the following factors:

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the protected health information or to whom the disclosure was made;

(3) Whether the protected health information was actually acquired or viewed; and

(4) The extent to which the risk to the protected health information has been mitigated.

(d) Because covered entities and Business Associates have the burden to prove why a breach notification is not required, risk assessments and the applicability of any exceptions must be carefully documented.

12.3.4 Notification – General requirements: Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary of HHS, and, in certain circumstances, to the media. In addition, Business Associates must notify covered entities that a breach has occurred. The following provides a general overview of notification requirements; specific procedural steps that are required for members of the OMH workforce to follow are detailed in the OMH Information Security Policy.

(a) Individuals. Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI.

(1) Covered entities must provide individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

(2) If the Covered Entity has insufficient or out-of-date contact information for 10 or more individuals, the Covered Entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the Covered Entity has insufficient or out-of-date contact information for fewer than 10 individuals, the Covered Entity may provide substitute notice by an alternative form of written, telephone, or other means.

(3) Individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the Covered Entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the Covered Entity.

(4) For substitute notice provided via web posting or major print or broadcast media, the notification must also include a toll-free number for individuals to contact the Covered Entity to determine if their protected health information was involved in the breach.

(b) Media Notice

(1) In addition to notifying the affected individuals, covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction in which the Covered Entity operates are required to provide notice to prominent media outlets serving the State or jurisdiction in which they operate. Covered entities may provide this notification in the form of a press release to appropriate media outlets serving the affected area.

(2) Media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach. Such notification must include the same information required for the individual notice.

(c) Notice to the Secretary of HHS

(1) In addition to notifying affected individuals and the media (where required), covered entities must notify the Secretary of HHS of breaches of unsecured PHI. Covered entities must notify the Secretary by visiting the HHS web site and electronically submitting a breach report form.

(2) If a breach affects 500 or more individuals, covered entities must notify the Secretary of HHS without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the Covered Entity may notify the Secretary of such breaches on an annual basis.

(3) Reports of breaches affecting fewer than 500 individuals are due to the Secretary of HHS no later than 60 days after the end of the calendar year in which the breaches occurred.

(d) Notification by a Business Associate

(1) If a breach of unsecured PHI occurs at or by a Business Associate, the Business Associate must notify the Covered Entity following the discovery of the breach.

(2) A Business Associate must provide notice to the Covered Entity without unreasonable delay and no later than 60 days from the discovery of the breach.

(3) To the extent possible, the Business Associate should provide the Covered Entity with the identification of each individual affected by the breach as well as any information required to be provided by the Covered Entity in its notification to affected individuals.