STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, January 6, 2014

CF OPERATING PROCEDURE
NO. 60-17, Chapter 7

HIPAA BREACH NOTIFICATION PROCEDURES

7-1. Purpose. This operating procedure establishes a uniform process for notification to the Privacy Officer by the Department and its Business Associates when an impermissible or unauthorized acquisition, access, use, or disclosure of PHI or ePHI has occurred which compromises the security or privacy of such information.

7-2. Scope. This operating procedure applies to all Departmental ‘‘workforce members’’ as defined in 45 C.F.R. § 160.103.

7-3. References.

a. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

b. Title 45 C.F.R. Subparts 160, 162 and 164, Security and Privacy of Individually Identifiable Health Information.

c. Sections 13400, 13402, 13410 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA) enacted February 2009.

d. 2013 HIPAA Omnibus Rule – 78 FR 5566, No. 17.

7-4. Definitions.

a. Breach. Section 13400(1) of the HITECH Act defines ‘‘breach’’ as 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.

(1) Where an exception applies there is no duty or obligation to give notice of a breach.

(2) If protected health information is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740, 42742), then it is not a breach and no breach notification is required following an impermissible use or disclosure of the information. Reporting the issue to the HIPAA Privacy Officer is still required.

b. Inadvertent Disclosure. The access, or use of protected health information from one person authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated person at the same facility and the information received is not further acquired, accessed, used or disclosed without authorization by any other person (section 13400(1)(B)(ii) and (iii) of the HITECH Act).

c. Unauthorized Disclosure. The access, or use of protected health information by an unauthorized person to whom protected health information is disclosed in an instance where such

person would not reasonably have been able to retain the information (section 13400(1)(A) of the HITECH Act).

d. Unintentional Acquisition. The access, or use of protected health information by an employee or other person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such person with the covered entity or business associate and such information is not further acquired, accessed, used, or disclosed by any other person (section 13400(1)(B)(i) of the HITECH Act).

7-5. Conducting a Risk Assessment. An unauthorized acquisition, access, use or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach as defined in 45 CFR 164.402(2), unless the Department demonstrates through a Risk Assessment that there is a low probability that the protected health information has been compromised.

a. A **Risk Assessment** based on the following factors must be completed.

(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 acquired, accessed, used or disclosed 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 of compromise to the protected health information has been mitigated.

b. Evaluate the overall probability that the protected health information has been compromised by considering all the factors in their totality. If the evaluation of the factors fails to demonstrate the low probability the protected health information has been compromised, Breach Notification is necessary and required.

7-6. Breach Notification Requirements. If it is determined that a Breach **has occurred** based upon the results of a properly completed the Risk Assessment, identify the individuals who's PHI has been compromised. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of the breach, pursuant to 45 C.F.R. 164.404. A breach shall be treated as discovered on the first day the breach is known, or by exercising reasonable diligence, would have been known. Time for notifications starts when a breach is discovered or should have been discovered.

a. Individual Notification. The Department must notify affected individuals following the discovery of a breach of unsecured PHI or ePHI. The notice must be in writing as described in paragraph 7-7 of this operating procedure, written in plain language, delivered by first-class mail to the affected person's last known address, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically and that agreement has not been withdrawn.

(1) If the Department has insufficient or out-of-date contact information for 10 or more individuals, the Department 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.

(2) If the Department has insufficient or out-of-date contact information for fewer than 10 individuals, it may provide substitute notice by an alternative form of written, telephone, or other means.

(3) If the individual is deceased, the notification will be sent by first-class mail at the last known address to the next of kin or personal representative.

(4) In cases where the individual affected by a breach is a minor or otherwise lacks legal capacity due to a physical or mental capacity concerns, notice will be sent to the parent or other person who is the personal representative of the individual.

b. Breach Affecting 500 or More Residents.

(1) Media Notification. If a breach affects more than 500 residents of the State, or of a jurisdiction within the State, in addition to notifying the affected individuals, the Department must notify prominent media outlets serving the State or jurisdiction, as applicable. Notice may be in the form of a press release to appropriate media outlets serving the appropriate affected area. Like individual notice, media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for giving individual notice.

(2) Posting a press release regarding a breach of unsecured protected health information on the home page of the covered entity's Web site will not fulfill the obligation to provide notice to the media.

c. Notification to the Secretary of the U.S. Department of Health and Human Services. In addition to notifying affected individuals and the media, where appropriate, the Department must notify the Secretary of the U.S. Department of Health and Human Services (HHS) of breaches of unsecured protected health information. The Department will notify the Secretary by utilizing the HHS website and completing and electronically submitting a breach report form. If a breach affects 500 or more individuals, the Department must notify the Secretary without unreasonable delay and in no case later than 60 days following discovery of the breach.

d. Breaches Affecting Less Than 500 Residents. The Department shall maintain a log (as described in paragraph 7-8 of this operating procedure) of all breaches affecting less than 500 residents and submit the information annually to the Secretary of HHS for breaches occurring during the preceding calendar year. The information must be submitted no later than 60 days after the end of each calendar year.

e. Notification by a Business Associate. If a breach of unsecured protected health information occurs at or by a Business Associate, the Business Associate must notify the Department following discovery of the breach. A Business Associate must provide notice to the Department without unreasonable delay and no later than (5) five days from the discovery of the breach.

(1) The Business Associate shall provide the Department with the identification of each individual affected by the breach, as well as any information required to be provided by the Department in its notification to affected individuals.

(2) A Business Associate that maintains the protected health information of multiple covered entities only needs to notify the covered entity(s) to which the breached information relates. However, in cases in which a breach involves the unsecured protected health information of multiple covered entities and it is unclear to whom the breached information relates, it may be necessary to notify all potentially affected covered entities.

f. Authorized Delay of Notification for Law Enforcement Purposes. If a law enforcement official states to the Department that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Department shall:

(1) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or,

(2) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily but no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during the 30-day time period.

7-7. Written Notice. The written notice must contain, per 45 C.F.R. 164.404(d)(1)(i):

a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach;

b. A description of the types of unsecured protected health information that was involved in the breach (such as whether full name, social security number, date of birth, home address, account numbers, diagnosis, disability code, or other types of information was involved);

c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

d. A brief description of what the Department is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

e. Contact procedures for individuals to ask questions or learn additional information, which must include an e-mail address, website, or postal address.

7-8. Breach Incident/Information Log. In addition to investigative reports for each incident of a breach, the Department shall record or log all reported breaches of PHI regardless of the number of individuals affected.

a. Pursuant to 45 C.F.R. § 164.530(j)(2), covered entities must maintain the log or other documentation for (6) six years.

b. A covered entity must make such information available to the Secretary of HHS upon request for compliance and enforcement purposes in accordance with 45 C.F.R. § 160.310.

c. The Breach Incident/Information Log must contain the following information for each reported breach:

(1) A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known;

(2) A description of the types of unsecured PHI that were involved in the breach (such as Social Security number, full name, date of birth, home address, treatment, etc.);

(3) A description of the action taken with regard to notification of individuals about the breach; and,

(4) Resolution steps taken to mitigate the potential harm caused by the breach and prevent future breach.

7-9. Reporting.

a. As soon as a known or suspected breach of protected health information is discovered:

(1) Report the known or suspected breach to the HIPAA Privacy Officer; and,

(2) Complete a HIPAA Privacy or Security Incident Report using form CF 10C (available in DCF Forms) and send the report to the Office of Civil Rights.

b. The Administrator for Civil Rights is the HIPAA Privacy Officer. The HIPAA Privacy Officer is responsible for reviewing and investigating reported HIPAA privacy incidents and violations of privacy policies.

c. The Information Technology (IT) Staff Director of Audits and Compliance is the HIPAA Security Officer. The HIPAA Security Officer and the Information Security Manager are responsible for reviewing and investigating reported HIPAA security incidents and violations of security policy.

d. Even if it is determined that a privacy or security incident does not constitute a breach, the Office of Civil Rights must be notified of the incident by the Program Office or Business Associate. The Office of Civil Rights shall maintain the Breach Incident/Information Log as described in paragraph 7-8 above.

7-10. Sanctions. Discipline will be in accordance with CFOP 60-17, Chapter 6.

7-11. Enforcement Rule. The HIPAA Enforcement Rule, 45 CFR Part 160, Subparts C–E, establish rules governing the compliance responsibilities of covered entities and Business Associates with respect to the enforcement process. This includes the rules governing investigations by the Department, rules governing the process and grounds for establishing the amount of a civil money penalty where a violation of a HIPAA Rule has been found, and rules governing the procedures for hearings and appeals where the covered entity challenges a violation determination.

7-12. Factors for Determining Civil Monetary Penalties. In determining the amount of any civil money penalty, the Secretary of HHS will consider the following factors, which may be mitigating or aggravating, as appropriate:

a. The nature and extent of the violation, consideration of which may include but is not limited to:

(1) The number of individuals affected; and,

(2) The time period during which the violation occurred.

b. The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;

(2) Whether the violation resulted in financial harm;

(3) Whether the violation resulted in harm to an individual’s reputation; and,

(4) Whether the violation hindered an individual’s ability to obtain health Care.

c. The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar to previous indications of noncompliance;

(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary of HHS provided in the context of a compliance effort; and,

(4) How the covered entity or business associate has responded to prior complaints.

d. The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and,

(3) The size of the covered entity or business associate.

7-13. Monetary Penalty Amounts. There are four tiers of penalty amounts that correspond with four categories of violations that reflect increasing levels of culpability with a maximum penalty amount of $1.5 million annually.

Violation Category	Each Violation	All Identical Violations/Calendar Year
Did Not Know	$100-$50,000	$1,500,000
Reasonable Cause	$1,000-$50,000	$1,500,000
Willful Neglect-Corrected	$10,000-$50,000	$1,500,000
Willful Neglect-Not Corrected	$50,000	$1,500,000

7-14. Training. The Department will train all employees, volunteers, and contracted staff on the policies and procedures with respect to PHI, ePHI and their job responsibilities. Training shall include how to identify and report breaches. Business Associates' staff will have access to training developed by the Department.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

DENNISE G. PARKER
Human Resources Director

GLOSSARY OF TERMS

a. Accounting of Disclosures. A log that is maintained for each client listing all disclosures that have been made of his or her PHI.

b. Alternative Communication Means. Information or communications delivered to clients by the Facility in a manner different than the normal practice of the Facility. For example, the client may ask for delivery at an alternative address, phone number or post office box; or that discussion of PHI be limited when specified people are present.

c. Amend/Amendment. An amendment to PHI will always be in the form of information *added to* the existing PHI. This additional information may contain items that substantially change the initial PHI, make parts of the initial PHI more precise, or show some of the original PHI to be incorrect. However, the original PHI is never altered. Changes are indicated by the addition of the amended information.

d. Authorization. A client's statement of agreement to the use or disclosure of Protected Health Information to a third party. See also “conditioned authorization”.

e. Breach. The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.

f. Business Associate (BA). An individual or organization that creates, receives, maintains, or transmits protected health information on behalf of the Department. A business associate might also be an individual or entity that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services involving the use or disclosure of PHI.

g. Civil Monetary Penalty. The amount of money the Department or Business Associate would have to pay where a violation of a HIPAA Rule has been found.

h. Client. As used in this operating procedure includes patient.

i. CMS – Centers for Medicare and Medicaid Services. The agency formerly known as HCFA (Health Care Financing Administration) that regulates and enforces Federal Regulations for Medicare in Long Term Care and other health care entities.

j. Conditioned. An authorization is “conditioned” if a client cannot obtain treatment or service unless he or she signs that authorization.

k. Covered Entity. A business or agency such as DCF, who transmits health care information using one of the transaction standards defined by the Department of Health and Human Services. An example of this would be billing Medicare and Medicaid electronically for services the Department, a Business Associate, or a contracted client services provider provides to a client.

l. Covered Functions. Functions of a covered entity, the performance of which make the entity a health plan, a health care clearinghouse, or a health care provider.

m. De-Identification. The process of converting individually identifiable information into information that no longer reveals the identity of the client. Information may be de-identified by statistical de-identification or the safe harbor method of de-identification.

n. De-Identified Health Information. Health information that does not identify an individual and does not contain information that can identify or link the information to the individual to whom the information belongs.

o. Department of Health and Human Services (HHS). The federal agency charged with the development, statement and implementation of the Health Insurance Portability and Accountability Act.

p. Designated Record Set. A group of medical records and billing records relating to an individual, maintained and used by the Department or health care provider to make decisions about the client. In this context a record is any item, collection, or grouping of information that contains Protected Health Information (PHI) and is maintained, collected, used or disclosed by the Department. The Designated Record Set also includes billing information that may contain ICD-9-CM codes that represent health conditions of the client and which are part of the clients Protected Health Information.

q. Directory Information. The four pieces of information that are considered “Directory Information” include:

(1) Client name;

(2) Location in the facility (room/bed number);

(3) Condition described in general terms (e.g., "He is not feeling well." or "She is having a good day."); and,

(4) Religious affiliation (available only to members of the clergy).

Note: You would not want to post or display more than the client’s name and room/bed number on your facility directory.

r. Disclosure. To release, transfer, provide access to or divulge in any way a client’s health information to third parties. Disclosures are either permissible or impermissible.

(1) Permissible - Disclosure of health information that does not require an authorization or an opportunity to agree or object before the disclosure is made. Permissible disclosures include, but are not limited to those made for treatment, payment and operation or required by law.

(2) Impermissible - A disclosure of health information that is prohibited under the privacy rule without first obtaining the client’s authorization. An impermissible disclosure is presumed to be a breach unless the covered entity or business associate demonstrates through a risk assessment that there was a low probability that the protected health information had been compromised.

s. Electronic Protected Health Information (ePHI). Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

t. Financial Records. Admission, billing, and other financial information about a client included as part of the Designated Record Set.

u. Fundraising. An organized campaign by a private, non-profit or charitable organization designed to reach out to certain segments of the population or certain identified populations in an effort to raise monies for their organization or for a specific project or purpose espoused by their organization.

v. Health Care Operations. Any of the following activities of a Covered Entity, Facility, or Institution:

(1) Conducting quality assessment and improvement activities, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; protocol development, case management and care coordination, contacting of health care providers and clients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating employee and facility performance, conducting training programs under supervision to practice or improve skills, training of non-health care professionals, accreditation, certification, licensing or credentialing activities;

(3) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(4) Business planning and development such as conducting cost-management and planning related analyses related to managing and operating a facility;

(5) Business management and administrative activities of a covered entity, including, but not limited to:

(a) Customer service;

(b) Resolution of internal grievances;

(c) Due diligence in connection with the sale or transfer of assets to a potential successor in interest; and,

(d) Creating de-identified health information, fundraising for the benefit of the covered entity and marketing for which an individual's authorization is not required.

w. Health Care Provider. An entity that provides health care, service or supplies related to the health of an individual, e.g., medical, dental, physical therapy, or chiropractic clinics; hospitals, etc.

x. Health Oversight Agency. 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.

y. HIPAA. The Health Insurance Portability and Accountability Act of 1996, including the portion of the Act known as Administrative Simplification (Subpart F) dealing with the privacy of individually identifiable health information.

z. Hybrid Entity. A single legal entity that is a covered entity whose business activities include both covered and non-covered functions and who designates health care components in accordance with law.

aa. Indirect Treatment Relationship. A relationship between an individual and a health care provider in which the health care provider delivers health care to the individual based on the orders of another health care provider and the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

bb. Individually Identifiable Health Information (IIHI). Any information, including demographic information, collected from an individual that:

(1) Is created or received by a health care provider, health plan, or employer; and

(2) Relates to the past, present or future physical or mental health or condition of an individual; and,

(a) Identifies the individual; or,

(b) With respect to which there is reasonable basis to believe that the information can be used to identify the individual.

cc. Law Enforcement Official. 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.

dd. Limited Data Set (LDS). A data set that includes elements such as dates of admission, discharge, birth and death as well as geographic information such as the five digit zip code and the individual's state, county, city or precinct but still excludes the other 16 elements that "de-identify" information. In addition, this limited data set can only be used if a covered entity enters into a "data use agreement" with the data recipient similar to the agreements entered into between covered entities and their business associates.

ee. Marketing.

(1) To provide information about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

(a) To describe a health-related product or service (or payment for such product or service) that is provided by or included in a plan of benefits of the covered entity making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancement to, a health plan; and health-related products or services available only to a health plan enrollee that add values to, but are not part of, a plan of benefits;

(b) For treatment of that individual; or,

(c) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual.

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses Protected Health Information to the other entity in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

ff. Medical Record. The collection of documents, notes, forms, test results, etc., which collectively document the health care services provided to an individual in any aspect of health care delivery by a provider; individually identifiable data collected and used in documenting healthcare services rendered. The Medical Record includes records of care used by healthcare professionals while providing client care services, for reviewing client data, or documenting observations actions or instructions. The Medical Record is included as part of the Designated Record Set.

gg. Minimum Necessary. The least amount of Protected Health Information needed to achieve the intended purpose of the use or disclosure. Covered Entities are required to limit the amount of Protected Health Information it uses, discloses or requests to the minimum necessary to do the job. Use or disclosure of more than the minimum necessary may constitute a breach and subject the covered entity to sanctions.

hh. Notice of Privacy Practices. A document required by HIPAA that provides the client with information on how the covered entity generally uses a client's Protected Health Information and what the client's rights are under the Privacy Rule.

ii. Operations. Health Care Operations includes functions such as: quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arrange for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

jj. Payment. The activities undertaken by a health care provider to obtain or provide reimbursement for client health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.

kk. Personal Representative. A person who has authority under 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 who is authorized under law to make health care decisions on behalf of a child or unemancipated minor. For purposes of the Privacy Rule a covered entity must treat a personal representative as having the same rights as the client unless there is a reasonable belief that the personal representative has subjected the client to abuse or neglect, or treating the person as the personal representative could endanger the client.

ll. Privacy Officer. A position mandated by HIPAA. The person designated by the organization who is responsible for development and implementation of the HIPAA policies and procedures and is responsible for reviewing and investigating reported HIPAA privacy incidents and violation of privacy policies. Within the Department, the Assistant Staff Director for the Office of Civil Rights has been designated the HIPAA Privacy Officer.

mm. Privacy Rule. The regulation issued by the Department of Health and Human Services entitled Standards for Privacy of Individually Identifiable Health Information.

nn. Protected Health Information (PHI) (if electronic may be referenced as “ePHI”). Individually identifiable information that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and

(1) That identifies the individual; or,

(2) There is a reasonable basis to believe the information can be used to identify the individual.

PHI does not include the following:

(1) Individually identifiable health information in education records covered by the Family Education Rights and Privacy Act (20 U.S.C. 1232g), and,

(2) Employment records held by a covered entity in its role as an employer.

oo. Psychotherapy Notes. Notes that are recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session. Psychotherapy notes must be kept separate from the rest of the client's Medical Record.

pp. Public Health Authority. 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 responsible for public health matters as part of its official mandate.

qq. Reasonable Cause. An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

rr. Reasonable Diligence. Is the care and attention that is expected from and is ordinarily exercised by a reasonable and prudent person under the same circumstances.

ss. Re-Identification. The process of converting de-identified health information back to individually identifiable health information. Re-identified health information does reveal the identity of the client and must be treated as PHI under the HIPAA Privacy Rule.

tt. Research. A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

uu. Resident. The term Resident in these operating procedures refers to someone that resides in the State of Florida or is under our jurisdiction.

vv. Revoke. To cancel or withdraw an authorization to release medical information.

ww. Role Based Access. Access to PHI based on the duties of employees. The Facility will identify persons or classes of persons in its workforce who need access to PHI to carry out their duties and make a reasonable effort to limit access of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

xx. Safeguarding. To ensure safekeeping of Protected Health Information for the client.

yy. Sanctions. Penalties associated with the unauthorized or impermissible access, release, transfer, or destruction of a client's health information. Federal regulations require the development and enforcement of a strict sanctions policy.

zz. Security Officer. A position mandated by HIPAA. The responsibilities of this person are to oversee implementation of the requirements mandated by the Final Security regulation and any security requirements included in the other sections of the HIPAA regulation. Within the Department, the IT Staff Director of Audits and Compliance has been designated the HIPAA Security Officer.

aaa. State Operations Manual (SOM). Federal Regulations that govern all Skilled Nursing Facilities that receive federal funding from Medicare and/or Medicaid.

bbb. Security Incidents. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. As defined by Security Standards, a "Security Incident" includes all of the unsuccessful "hacking" attempts that might take place. Security incidents require a report be made to the Security Officer within a reasonable period of time.

ccc. Subcontractor. Is a person to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for the Department. A subcontractor is then a business associate where that function, activity, or service involves the creation, receipt, maintenance, or transmission of protected health information.

ddd. Subpoena (2 types). A process to cause a witness to appear and give testimony, commanding him to lay aside all pretenses and excuses, and appear before a court or magistrate therein named at a time therein mentioned to testify for the party named under a penalty thereof.

(1) Duces Tecum – A request for witnesses to appear and bring specified documents and other tangible items. The subpoena *duces tecum* requires the individual to appear in court with the requested documents, or simply turn over those documents to the court or to counsel requesting the documents.

(2) General Subpoena (AKA *Ad Testificandum*) – A command to appear in court at a certain time and place to give testimony regarding a certain matter, for example, to testify that the record was kept in the normal course of business.

eee. TPO. (See Treatment, Payment, and Operations.)

fff. Treatment . The provision, coordination or management of health care and related services by the Facility, including the coordination or management of health care by the Facility with a third party; consultation with other health care providers relating to a client; or the referral of a client for health care between the Facility and another health care provider.

ggg. Treatment, Payment and Operations (TPO) Exclusion. The Privacy Rule allows sharing of information for purposes of treatment, payment and health care operations. Treatment includes use of client information for providing continuing care. Payment includes sharing of information in order to bill for the care of the client. Health care operations are certain administrative, financial, legal, and quality improvement activities that are necessary for your Facility to run its business and to support the core functions of treatment and payment.

hhh. U. S. Department of Health and Human Services (HHS). The federal agency charged with the development, statement and implementation of the HIPAA Privacy Rule. (www.hhs.gov/)

iii. U.S. Department of Health and Human Services (HHS) Office of Civil Rights. The federal agency that has responsibility for enforcement of the HIPAA Privacy Rule. (www.hhs.gov/cr/)

jjj. Unconditioned. Research that does not condition treatment or services upon signing an authorization.

kkk. Unsecured Protected Health Information. Is protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.

lll. Use. To share, apply, use, examine or analyze health information within the Facility. (See also Disclosure).

mmm. Whistleblower. A person, usually a staff member, who reveals wrongdoing within an organization to the public, government agencies or to those in positions of authority.

nnn. Willful Neglect. Conscious, intentional failure, or reckless indifference to comply.

ooo. Workforce. Employees, volunteers, trainees and other persons whose conduct, in the performance of work for the Facility, is under the direct control of the Facility, whether or not they are paid. Members of the workforce are not business associates.