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

CF OPERATING PROCEDURE
NO. 60-17, Chapter 2

Personnel

PROTECTED HEALTH INFORMATION COMPLAINT/GRIEVANCE PROCEDURES

2-1. Purpose. This chapter establishes uniform procedures for clients' complaints about alleged violations of their rights relating to protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) within the Department of Children and Families.

2-2. Definitions.

a. Protected Health Information (PHI). 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.

b. Designated Record Set. A group of records maintained by or for a covered entity including the medical billing records relating to an individual maintained by or for a health care provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan; or used, in whole or part, by or for a covered entity to make decisions about individuals.

c. Complaint. Any concern communicated by a person questioning any act or failure to act relating to an individual's rights to access to his/her health information, to maintain privacy of his/her health information, to request restrictions on uses or disclosures of his/her PHI, to request confidential communications regarding his/her PHI, to request amendment of his/her PHI, or to receive a complete listing of disclosures of his/her PHI.

d. Complainant. The person who initiates a complaint or appeal.

2-3. Policy. The Health Insurance Portability and Accountability Act (HIPAA) grants individuals specific rights relating to their protected health information, many of which overlap with client rights mandated by state law. Specifically, in addition to privacy rights related to their PHI, individuals are granted the right to access their designated record set, to request restrictions on uses or disclosures of their PHI, to request that communications related to PHI be confidential, to request amendment of their designated record set and to receive a complete listing of disclosures of their PHI. *[For details, see Notice of Privacy Practices; in the "Your Information. Your Rights. Our Responsibilities." section.]* HIPAA also mandates that a process be in place for individuals to complain about an entity's privacy related policies and procedures and/or the entity's compliance with those policies and procedures.

This operating procedure supersedes CFOP 60-17, Chapter 2, dated June 2, 2008.
OPR: ASHRC
DISTRIBUTION: A

a. Clients and potential clients who believe their rights relating to protected health information (PHI) have been violated may file a complaint. The complaint may be either formal or informal, but must be in writing. Complaints must be filed within 180 days of the alleged violation. Complaints may be filed with the following:

FL Department of Children and Families
Attention: Office of Civil Rights, Human Resources
1317 Winewood Boulevard, Building 1, Room 110
Tallahassee, Florida 32399-0700

or

United States Department of Health and Human Services (HHS)
Attention: Office for Civil Rights
Atlanta Federal Center, Suite 3B70
61 Forsyth Street SW
Atlanta, Georgia 32303-8909

b. The Administrator for Civil Rights is designated as the person responsible for receiving complaints relating to individuals' privacy rights, rights to access their designated record set, to request restrictions on the use or disclosure of their PHI, to request confidential communications of health related information, to request amendment of their designated record set, or to request a complete listing, or accounting of disclosures made of their PHI.

c. When a HIPAA related complaint is communicated to any Department employee, that employee shall immediately notify the Administrator for Civil Rights or designee, and shall inform the complainant where to file their complaint.

2-4. Receipt of Complaint. The Office of Civil Rights in Human Resources is the Department's central intake point for all filed PHI complaints and any complaints received in the regions, mental health treatment facilities, or headquarters must be forwarded immediately to the Office of Civil Rights upon receipt.

2-5. Complaint/Investigative Process. The Office of Civil Rights is responsible for investigating the circumstances of the alleged HIPAA rights violation, and, if appropriate, shall take all reasonable steps to mitigate the effects of any violation.

a. All complaint investigations will be completed within sixty (60) days of receipt. The HIPAA Compliance Officer will complete a position statement within forty-five (45) days of receipt of complaint assignment. All position statements must be reviewed by legal.

b. The Administrator for Civil Rights shall communicate the results of the investigation and resolution of the complaint to HHS or the complainant within sixty (60) working days unless a greater amount of time is necessary to complete the investigation. If such greater time is necessary, the Administrator shall, within sixty (60) days, notify HHS or the complainant of the delay. The Administrator shall request an extension of time from HHS as appropriate or inform the complainant of the expected time frame for completion of the investigation.

c. If the complainant is dissatisfied with the result, he or she shall be informed of their right to file with the US Department of Health and Human Services (HHS).

2-6. Decision and Disposition. If the results of the investigation indicate that a Department employee has made an unauthorized use or disclosure of PHI, or otherwise violated HIPAA Polices and

Procedures, the Administrator for Civil Rights shall report such finding to the Regional Director, Hospital Administrator, or the Assistant Secretary's Office.

a. Any employee, who discloses or permits the unlawful disclosure of PHI, will be subject to sanctions as described in CFOP 60-17, Chapter 6. In addition, employees who violate the provisions of this policy may also be subject to criminal penalties under federal law.

b. The Administrator for Civil Rights shall document all HIPAA related complaints, their resolution, and any actions taken. This documentation shall be kept for a minimum period of six (6) years from the date of final resolution. This documentation shall be reviewed quarterly to determine if any pattern or systematic problems exist and, if so, shall take necessary steps to address the problem.

2-7. No Retaliation. There shall be no retaliation against any individual or person served, or employee, for having filed or assisted on the filing of a complaint or for investigating or acting on a complaint. Any employee who becomes aware of any such retaliatory action shall immediately report it to the Office of Civil Rights.

2-8. Monitoring. The HIPAA Compliance Officer will collect and analyze information from regions headquarters, and mental health treatment facilities annually during the month of April, to determine compliance with this procedure.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

DENNISE G. PARKER
Human Resources Director

SUMMARY OF REVISED, ADDED, OR DELETED MATERIAL

This revision reflects organizational changes within the Department, current addresses and information required by the 2013 HIPAA Omnibus Rule. The timeframe for preparing a position statement has been reduced to (45) days. The timeframe for communicating complaint investigation results has been reduced from (90) days to (60) days.

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 Administrator for 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.