

CF OPERATING PROCEDURE
NO. 60-17, Chapter 4

STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE May 2, 2016

Human Resources

AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

4-1. Purpose. This operating procedure establishes a uniform process for when an authorization is required for the use or disclosure of clients Protected Health Information (PHI) and the required elements the authorization must contain.

4-2. General.

a. In compliance with 45 CFR, Part 164.508, all uses and disclosures of PHI beyond those allowed pursuant to a client's consent or as otherwise permitted or required by law require a signed authorization. A separate authorization is required for each separate entity that is to receive this PHI.

b. The provision of treatment, payment, or eligibility for benefits may not be conditioned on the client's provision of an authorization for the use or disclosure of PHI except:

(1) Where treatment relates to the provision of research related treatment; or,

(2) Where treatment relates to health care that is to be provided solely for the purpose of creating PHI for disclosure to a third party.

4-3. When is an Authorization Required.

a. General Rule. Except as otherwise permitted or required by this chapter, the Department and its Business Associates may not use or disclose PHI without a valid authorization as described below. When you obtain or receive a valid authorization for the use or disclosure of PHI, such use or disclosure must be consistent with such authorization.

b. Authorization Required for Psychotherapy Notes. The Department and its Business Associates must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(1) To carry out the following treatment, payment, or health care operations:

(a) Use by the originator of the psychotherapy notes for treatment;

(b) Use or disclosure by the Department or its Business Associates for their own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or,

(c) Use or disclosure by the Department or its Business Associates to defend themselves in a legal action or other proceeding brought by the individual; and

(2) A use or disclosure that is required by 45 CFR §164.502(a)(2)(ii) or permitted by §164.512(a); §164.512(d) with respect to the oversight of the originator of the psychotherapy notes; §164.512(g)(1); or §164.512(j)(1)(i).

This operating procedure supersedes CFOP 60-17, Chapter 4, dated June 2, 2008.

OPR: ASHR

DISTRIBUTION: A

c. Authorization Required for Marketing.

(1) The Department and its Business Associates must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

(a) A face-to-face communication made by a covered entity to a client; or,

(b) A promotional gift of nominal value provided by the Department or its Business Associate.

(2) If the marketing involves financial remuneration, as defined in the Glossary of Terms, to the Department or Business Associate from a third party, the authorization must state that such remuneration is involved.

d. Authorization Required for Sale of PHI.

(1) The Department and its Business Associates must obtain an authorization for any disclosure of PHI which is a sale of PHI, as defined in the Glossary of Terms.

(2) Such authorization must state that the disclosure will result in remuneration to the Department or Business Associate.

4-4. Requirements of a Valid Authorization. A valid authorization will include the following elements and the additional elements that are required by the specific applicable law.

a. Each authorization for the use or disclosure of a client's PHI must be written in plain language and must contain:

(1) A specific and meaningful description of the PHI to be used or disclosed;

(2) A description of each purpose of the use or disclosure in question;

(3) The name or specific identification of the person(s) or class of person(s) authorized to make the requested use or disclosure;

(4) The name or specific identification of the person(s) or class of person(s) to whom the use or disclosure may be made;

(5) An expiration date or event;

(6) A statement of the client's right to revoke the authorization in writing, and limitations on that right to revoke;

(7) A description of how the client may revoke the authorization;

(8) A statement acknowledging that the health information disclosed pursuant to the authorization may be re-disclosed by the recipient and no longer protected by the Department's privacy practices;

(9) If the use or disclosure is for fundraising purposes, a clear and conspicuous statement that the client can choose to opt out of future fundraising communications at any time;

(10) If the use or disclosure is for sale or marketing purposes, a statement that informs the client that the use or disclosure will result in remuneration;

(11) A statement of the Department's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization; and,

(12) Signature of the client or the client's personal representative and the date signed. The signature of the personal representative must be accompanied by a description of the representative's authority to act on the client's behalf.

b. A copy of the signed authorization (form CF 772, available in DCF Forms) must be given to the client.

4-5. Invalid Authorizations. An authorization is invalid if any of the following occur:

- a. The expiration date or event has passed;
- b. The authorization lacks any of the required elements (see paragraph 4-4 above);
- c. The authorization has not been filled out completely;
- d. The authorization contains information that the Department or Business Associate knows to be false;
- e. The authorization is known by the Department or Business Associate to have been revoked;
- f. The authorization is prohibited by law; or,
- g. The authorization violates paragraph 4-6 or paragraph 4-7 of this operating procedure.

4-6. Compound Authorizations. A Compound Authorization allows the Department or Business Associate to combine conditioned and unconditioned authorizations for research on the same authorization form as described below.

a. An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:

(1) An authorization for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining:

- (a) An authorization for the use or disclosure of PHI for a research study with another authorization for the same research study;
- (b) An authorization for the creation or maintenance of a research database or repository; or,
- (c) A consent to participate in research.

(2) Where the provision of research related treatment is conditioned on the provision of one of the authorizations, as permitted under paragraph 4-7a of this operating procedure, any compound authorization must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt-in to the research activities described in the unconditioned authorization.

b. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

c. An authorization under the HIPAA regulations, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under the HIPAA regulations, except when the Department or Business Associate has conditioned the provision of treatment, payment, or eligibility for benefits under paragraph 4-7a of this operating procedure on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, or eligibility for benefits under paragraph 4-7a does not apply to a compound authorization created in accordance with paragraph 4-6a of this operating procedure.

4-7. Prohibition on Conditioning of Authorizations. A covered entity may not condition a client's treatment, payment, or eligibility for benefits on the provision of an authorization, except:

a. The Department or Business Associate may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research under the HIPAA regulations; or,

b. The Department or Business Associate may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.

4-8. Revocation of Authorizations. A client may revoke an authorization provided under the HIPAA regulations at any time.

a. The revocation must be in writing.

b. The revocation is not effective until the Department or Business Associate receives the written revocation.

c. A written revocation is not effective with respect to actions that have already been taken in reliance on a valid authorization.

4-9. Authorization Retention Requirements. The Department or Business Associate must document and maintain all client authorizations for a period of at least six (6) years.

4-10. Accounting of Disclosures. Pursuant to CFOP 60-17, Chapter 5, the program office, facility, or employee must document and retain all information about uses or disclosures of PHI required to be in an accounting of disclosures for a period of six (6) years, including:

a. Date of disclosure;

b. Client's name;

c. Name and, if known, address of recipient of PHI;

d. Description of PHI disclosed; and,

e. Statement of purpose and basis for disclosure, or copy of authorization or request for disclosure.

4-11. Compliance Monitoring. The Privacy Officer will collect and analyze information from regions and mental health treatment facilities annually to determine compliance with this operating procedure.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

SHELBY JEFFERSON
Interim Human Resources Director

SUMMARY OF REVISED, ADDED, OR DELETED MATERIAL

This operating procedure has been updated to comply with the 2013 Omnibus Rule to specify when an authorization is required and the requirements of a valid authorization. Form CF 772, Authorization for Use or Disclosure of Protected Health Information (available in DCF Forms), has also been revised.

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 is 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 PHI to a third party. See also "conditioned authorization".
- e. Breach. The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information.
- f. Business Associate (BA). An individual or organization that creates, receives, maintains, or transmits PHI 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. De-Identified Health Information.
- n. 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.
- o. 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 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 PHI.

p. 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.

q. 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 PHI had been compromised.

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

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

t. Financial Remuneration. The direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

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 or mental health treatment facility:

(1) Conducting quality assessment and improvement activities, provided that the obtaining of generalized 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 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 PHI 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, and 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 PHI needed to achieve the intended purpose of the use or disclosure. Covered Entities are required to limit the amount of PHI 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 PHI 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 Human Resources 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, 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. Revoke. To cancel or withdraw an authorization to release medical information.

vv. 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.

ww. Safeguarding. To ensure safekeeping of PHI for the client.

xx. 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.

yy. 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 Information Security Manager has been designated the HIPAA Security Officer.

zz. State Operations Manual (SOM). Federal Regulations that govern all skilled nursing facilities that receive federal funding from Medicare and/or Medicaid.

aaa. 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.

bbb. 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 (PHI).

ccc. 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.

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

eee. 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.

fff. 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.

ggg. 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/)

hhh. 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/)

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

jjj. Unsecured Protected Health Information. Is PHI 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.

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

III. 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.

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

nnn. 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.