Child & Family Center

Guide for Privacy, Confidentiality & Security of Health Information

The information contained in this Guide is not intended to serve as legal advice nor should it substitute for legal counsel. The Guide is not exhaustive and users are encouraged to seek additional detailed technical guidance from supervisors and managers at Child & Family Center to supplement the information contained herein.

Contents

DEFINITIONS

The glossary of terms and acronyms that follow are helpful for all employees and other staff at Child & Family Center as part of their daily work in the provision of behavioral health care, treatment and services. These terms are contained in many of the policies and procedures contained in this *Guide*.

Authorization: A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances. An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party.

Breach: the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security, privacy, or integrity of the health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The HITECH Act clarifies that an unauthorized activity compromises the privacy or security of PHI or electronic PHI if it poses a significant risk for financial, reputational, or other harm to the individual**.**

Consent: written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations).

Covered entity: organization subject to the HIPAA Privacy Rule is a covered entity. Child & Family Center is a covered entity as a health care provider.

Discovered: A breach of PHI or electronic PHI will be deemed 'discovered' as of the first day the staff member knows of the breach, or by exercising reasonable diligence, would or should have known about the breach.

False Claims Act (FCA): False Claims Act imposes liability on any person who submits a claim to the government that he or she knows (or should know) is false. There are federal level and state level FCAs.

Privacy of Individually Identifiable Health Information ("Privacy Rule"): national standards for the protection of certain health information established by HIPAA. The Privacy Rule standards address the use and disclosure of individually identifiable health information - called "protected health information" by covered entities. The Privacy Rule assures that individual health information is properly protected and provides standards for the individual's privacy rights to understand and control how their health information is used.

Health Information Technology for Economic and Clinical Health (HITECH) Act: Passed in 2009, the HITECH Act supports the concept of electronic health records - meaningful use. HITECH proposes the meaningful use of interoperable electronic health records throughout the United States health care delivery system as a critical national goal.

Health care provider: Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

Individually identifiable health information: information, including demographic data, that relates to: 1) the individual's past, present or future physical or mental health or condition, 2) the provision of health care to the individual, or 3) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security number).

Identifiers: Individually identifiable health information that is a subset of health information, including demographic information collected from an individual to include:

1. Names.
2. Geographic subdivisions smaller than a state (e.g., street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code, if according to the currently available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people. If such geographic units contain 20,000 people or less, then the initial three digits of the zip codes must be changed to 000 and thus treat them as a single geographic area.)
3. All elements of dates, except year, directly related to an individual including birth date, admission date, discharge date, date of death; and for all ages over 89, all elements of date including year indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older. Note, however, that for research or other studies relating to young children or infants, C&FC's policy does not prohibit age of an individual from being expressed in months, days or hours.
4. Telephone numbers.
5. Fax numbers.
6. Electronic-mail addresses.
7. Social Security Numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers including finger and voice prints.
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic or code.

Meaningful Use: the use of certified EHR technology in a meaningful manner (for example electronic prescribing); ensuring that the certified EHR technology is connected in a manner that provides for the electronic exchange of health information to improve the quality of care; and that in using certified EHR technology the provider must submit to the Secretary of Health & Human Services (HHS) information on quality of care and other measures. The concept of meaningful use rested on the '5 pillars' of health outcomes policy priorities, namely: 1. Improving quality, safety, efficiency, and reducing health disparities; 2. Engage patients and families in their health; 3. Improve care coordination; 4. Improve population and public health; and, 5. Ensure adequate privacy and security protection for personal health information. Health Insurance Portability and Accountability Act of 1996 (HIPAA): Public Law 104-191 was enacted on August 21, 1996 and established standards for the electronic exchange, privacy and security of health information.

Mental Health Records: under California law, is defined as client/patient records, or discrete portions thereof, specifically relating to evaluation or treatment of a mental disorder and includes, but is not limited to, all alcohol and drug abuse records (Cal. Health & Saf. Code § 123105).

Privacy Officer: oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, client health information in compliance with federal and state laws and the healthcare organization's information privacy practices.

Protected Health Information: The HIPAA Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)." Full face photographic images and any comparable images are considered PHI and subject to the Privacy Rule.

Removal of Identifiers. Health Information is considered de-identified if all eighteen (18) of the identifiers of the individual or relatives, employers, or household members of the client are removed and the C&FC does not have any actual knowledge that the information could be used alone or in combination with other information to identify the person.

Security Officer: primarily responsible for all ongoing activities related to the availability, integrity and confidentiality of client, provider, employee, and business information in compliance with the healthcare organization's security policies and procedures, regulations and law.

42 Code of Federal Regulation Part 2: 42 CFR Part 2 applies to any individual or entity that is federally assisted and holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment (42 CFR § 2.11).

- The regulations restrict the disclosure and use of alcohol and drug client records maintained in connection with the performance of any federally assisted alcohol and drug abuse program (42 CFR § 2.3(a)).
- The restrictions apply to any information disclosed by a covered program that "would identify a patient as an alcohol or drug abuser …" (42 CFR §2.12(a) (1)). In laymen's terms, the information protected by 42 CFR Part 2 is any information disclosed by a covered program that identifies an individual directly or indirectly as having a current or past drug or alcohol problem, or as a participant in a covered program.
- With limited exceptions, 42 CFR Part 2 requires client consent for disclosures of protected health information even for the purposes of treatment, payment, or health care operations. Consent for disclosure must be in writing.

ACRONYMS

AIDS Acquired Immune Deficiency Syndrome

BA Business Associate

BAA Business Associate Agreement

CD Compact Disc

CE Covered Entity

CFR Code of Federal Regulations

CMS Centers for Medicare & Medicaid Services

EHR Electronic Health Record

ePHI Electronic Protected Health Information

FR Federal Register

Health IT Health Information Technology

HHS U.S. Department of Health and Human Services

HIPAA Health Insurance Portability and Accountability Act

HITECH Health Information Technology for Economic and Clinical Health

HIV Human Immunodeficiency Virus

IT Information Technology

NPP Notice of Privacy Practices

OCR Office for Civil Rights

ONC Office of the National Coordinator for Health Information Technology

PHI Protected Health Information

SRA Security Risk Assessment

NOTE: This *Guide* encompasses and replaces Child & Family Center HIPAA policies and procedures with the original effective dates of April 14, 2003.

INTRODUCTION

It is the intent of Child & Family Center to increase trust and information integrity through its privacy and security practices in all aspects of behavioral health care, treatment and services. To reap the promise of digital health information to achieve better care, smarter spending, and healthier people, providers and individuals alike must trust that an individual's health information is private and secure. If clients and families lack trust in recordkeeping practices and the confidentiality of behavioral information (e.g., mental health records, electronic health records), they may not want to disclose health information that is critical for care, treatment and services at Child & Family Center. Withholding their health information could have life-threatening consequences. This is one reason why it's so important to ensure the privacy, confidentiality, and security of health information. When clients trust C&FC and its health information technology enough to share their behavioral health information, there is a more complete picture of client's overall health and together, the treatment team and the client can make more-informed decisions.

In addition, when breaches of health information occur, they can have serious consequences for C&FC, including reputational and financial harm or harm to clients. Poor privacy and security practices heighten the vulnerability of client information in the C&FC information systems. To help cultivate trust, C&FC must:

- Maintain accurate information in the client record
- Make sure clients and their authorized representatives have a way to request access to their clinical record and know how to do so
- Carefully handle client health information to protect privacy and maintain confidentiality
- Ensure client behavioral health information is accessible to authorized representatives when needed

Effective privacy and security measures help C&FC clinical practices meet requirements of the HIPAA Rules and avoid costly civil money penalties for violations. Whether client information is on a computer, in an Electronic Health Record (EHR), on paper, or in other media, providers have responsibilities for safeguarding the information by meeting the requirements of the Rules.

The intent of the *Guide* is to help C&FC staff better understand how to integrate rules and standards about privacy, confidentiality and security requirements into daily practices. This includes guidance to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the U.S. Department of Health and Human Services (HHS) privacy and security requirements to protect the security of electronic health information, to comply with 42 Code of Federal Regulation's Part 2 to provide extra protection for substance use treatment information as well as to fulfill the duty to protect the confidentiality, integrity, and availability of confidential medical information as required by law, professional ethics, and accreditation requirements. All C&FC staff must be familiar with the Guide and demonstrate competence related to prudent and respectful privacy, confidentiality and security practices in accordance with the requirements.

Responsibilities under HIPAA and Other Regulations

The Health Insurance Portability and Accountability Act (HIPAA) Rules provide federal protections for health information held by Covered Entities (CEs) and Business Associates (BAs) and give clients an array of rights with respect to that information. This suite of regulations includes the

- **Privacy Rule**, which protects the privacy of individually identifiable health information;

- **Security Rule**, which sets national standards for the security of electronic Protected Health Information (ePHI); and the
- **Breach Notification Rule**, which requires CEs and BAs to provide notification following a breach of unsecured Protected Health Information (PHI).

C&FC comply with the HIPAA Privacy, Security and Breach Notification Rules. C&FC BAs must comply with the HIPAA Security Rule and Breach Notification Rule as well as certain provisions of the HIPAA Privacy Rule.

There are two main categories of regulations under HIPAA, the Privacy Regulations and the Security Regulations. The Privacy Regulations establish certain minimum standards for (a) the use and disclosure of the client's health information by health care providers and (b) access and control by individuals of their own health information. The Security Regulations provide for the integrity and security of health information when that information is stored or transmitted electronically. The Privacy Regulations and the Security Regulations are found in the Code of Federal Regulations, 45 CFR Parts 160 and 164.

Overview of External Stakeholders

Office/Agency	Health Information-Related Responsibilities	Website
Centers for Medicare & Medicaid Services (CMS)	• Oversees the Meaningful Use Programs	www.cms.gov
Office for Civil Rights (OCR)	• Administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules • Conducts HIPAA complaint investigations, compliance reviews, and audits	www.hhs.gov/ocr
Office of the National Coordinator for Health Information Technology (ONC)	• Provides support for the adoption and promotion of EHRs • Offers educational resources and tools to assist providers with keeping electronic health information private and secure	www.HealthIT.gov
California Department of Healthcare Services Office of HIPAA Compliance: Information Protection Unit	• The Office of HIPAA Compliance (OHC) office is responsible for implementing the regulations of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.	http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx
State of California Department of Justice Office of the Attorney General (OAG)	• California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. • The OAG accepts security breach reports from state agencies, businesses or residents in California.	https://oag.ca.gov/ecrime/databreach/reporting
Los Angeles County Department of Mental Health (LAC DMH)	• • Complaints against an LACDMH-contracted provider are directed to the Patient's Rights Office or submitted in writing to LACDMH.	http://dmh.lacounty.gov/wps/portal/dmh/our_services/services_detail/?current=true&urile=wcm

Office/Agency	Health Information-Related Responsibilities	Website
		:path:/DMH+Content/DMH+Site/Home/Our+Services/Our+Services+Detail/Forms
Los Angeles County Substance Abuse Prevention and Control (SAPC)	• Complaints against a SAPC-contracted provider, are directed to SAPC Help Line or submitted in writing to SAPC.	http://publichealth.lacounty.gov/phn/docs/Public%20Health%20Information%20Technology%20and%20Security%20Policy.pdf

PRIVACY AND CONFIDENTIALITY

The privacy of health information is a critical information management concern. Privacy of health information applies to electronic, paper, and verbal communications. Protecting the privacy of health information is the responsibility of everyone at Child & Family Center. Privacy is protected by limiting the use of information to only what is needed to provide care, treatment, or services. Privacy, along with security, results in the confidentiality of health information. Health information is kept confidential when the information is secure (kept from intentional harm) and its use is limited (privacy). The end result of protecting the security and privacy of the information system is the preservation of confidentiality. To illustrate this relationship, confidentiality is violated in situations when an individual's health information is used or accessed by someone who does not have permission to access the information or uses it for purposes outside of delivering care, treatment, or services. A confidentiality violation occurs when someone is able to bypass security measures and systems to gain access to health information. Although maintaining the confidentiality of health information and providing access to appropriate care providers can be challenging, this *Guide* offers direction on the privacy and confidentiality of behavioral health and other health information.

Clients have the right to direct Child & Family Center to disclose his/her PHI to him or herself and to third parties designated by the client. When a client consents to treatment, he or she consents to the use of his or her PHI by C&FC for payment, treatment and healthcare operations as described in the C&FC Notice of Privacy Practices. Except in certain circumstances when state or federal law either permits or requires the disclosure, PHI is not to be used or disclosed for purposes other than payment, treatment and healthcare operations without the client's written authorization. No PHI is released to any third party without a valid written authorization from the client or his or her duly authorized representative.

Notice of Privacy Practices

The HIPAA Privacy Rule requires that health care providers like C&FC develop and distribute a notice that provides a clear, user friendly explanation of individual rights to clients. The Notice of Privacy Practices (NPP) outlines the personal health information and the privacy practices used by C&FC to help improve the client experience and understanding using plain language. The HIPAA Privacy Rule requires that organizations like C&FC with direct treatment relationships with individuals do the following:

1. Give the NPP to every client no later than the date of first service delivery.
2. Make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice.

3. Post the notice in the facility in a clear and prominent location where individuals are likely to see it.
4. Make the notice available to those who ask for a copy.

The NPP includes the following information:

- How C&FC may use and disclose an individual's PHI
- The individual's rights with respect to the information including a statement that C&FC is required by law to about the C&FC's privacy policies and how the individual may exercise these rights
- C&FC's legal duties to maintain the privacy of PHI
- How the individual may file a complaint
- Whom individuals can contact for further information.

Authorization to Disclose

C&FC obtains the authorization of the client or the client's representative (e.g., parent, guardian) in accordance with all federal and California laws on the applicable Authorization Form whenever it desires to use (obtain) or disclose (release) PHI for a purpose other than providing treatment, payment or carrying out health care operations.

Requirements for Valid Authorization

To be valid, an authorization for release of PHI must meet the following criteria (45 CFR 164.508(c)):

- Be signed and dated by the client or his/her legal representative;
- State specifically the person(s) or entity to whom the information is to be released, and the purpose for which the information is required;
- State specifically what information is to be released, with dates of service;
- Be addressed to Child & Family Center;
- Include an expiration date, if desired by the client; otherwise, authorization expires within ninety (90) days of receipt thereof;
- Contain a statement that authorization may be revoked at any time (together with a description of how it is to be revoked), except to the extent that disclosure is made in reliance on the authorization;
- Contain a statement that the information disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by 42 CFR 160 et seq.; and
- If the client's legal representative signed the authorization, the authorization must contain a description of the representative's authority to act for the client (e.g., parent, guardian).
- In the case of a minor (anyone under eighteen (18) years of age), the client (if legally could have consented to his/her own treatment) or court-appointed legal guardian must sign the authorization; and unless the parent is the authorized party, proof of appointment by a court of competent jurisdiction should accompany the authorization. In the case of a minor with divorced parents, the signature of either parent will suffice as a valid authorization, although we may request it from both parents in certain circumstances where custody is shared.

Any such authorization received by Child & Family Center is kept on file with the client's medical record along with documentation of the information released. Each transaction disclosing PHI is documented as to the nature and dates of the information released, to who released, and the date of release.

C&FC may use or disclose PHI that it created or received prior to April 14, 2003 pursuant to an authorization or other express legal permission obtained from a client prior to April 14, 2003 *if* (a) the authorization or other express legal permission specifically permits such use or disclosure, and (b) there is no agreed upon restriction.

Court Orders

Upon receipt of a court order (a document issued by a state or federal court with jurisdiction) ordering the release of PHI, Child & Family Center staff should consult with legal counsel. In most instances, the court order constitutes sufficient authority for the release of the designated records, but the advice of an attorney should be sought to ensure that the client's privacy rights are protected.

Subpoenas

Staff should seek the advice of an attorney or designated staff person when a subpoena is received.

1. Subpoenas Requiring Witness to Appear in Court or at a Deposition to Testify. Upon receipt of a subpoena that is not accompanied by a written authorization signed by the client or the client's legal representative, C&FC staff should consult legal counsel. Prior to providing any testimony, C&FC staff should be counseled by an attorney about any applicable legal privilege that would preclude his or her testifying about certain subject matters (e.g. statutes protecting from disclosure certain client information, quality improvement activities, etc.).
2. Subpoena Requiring the Production of Documents Only. Upon receipt of a subpoena that requires the production of documents only (known as Subpoena Duces Tecum), C&FC staff should consult legal counsel. If a Subpoena Duces Tecum is not accompanied by a proper authorization signed by the client or the client's legal representative or by a court order or a "letter of assurance" required by HIPAA (45 CFR 164.512(e)), then C&FC does not release the information and notifies the requestor accordingly.

Instances Justifying Release of PHI without Authorization

There are other circumstances when disclosure of PHI is permitted without a client's authorization, such as:

- Release to accrediting agencies and licensing agencies as required by state and federal law; with respect to quality improvement material or other sensitive documents seek legal counsel.
- Release to other health care providers who are directly involved in the medical care of the client or involved in the financial or administrative review of the client's record.
- Release directly to client upon request of the client.
- Release to report suspected child abuse.

Use and Disclosure of De-Identified Health Information

C&FC may use or disclose de-identified health information without obtaining the client's authorization. De-identified health information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

C&FC may use health information to create de-identified health information or disclose health information to a Business Associate to create de-identified health information so long as C&FC and the Business Associate execute a Business Associate agreement. C&FC may not use PHI to create de-identified health information for research purposes without obtaining a client's authorization or a waiver from an Institutional Review Board/Privacy Board.

A code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified may not be disclosed except as otherwise permitted under C&FC's policies for disclosure of PHI. De-identified Health Information that has been re-identified may not be disclosed or used except as otherwise permitted under C&FC's policies for disclosure and use of PHI.

The "MINIMUM NECESSARY" Policy

The HIPAA Privacy Regulations require in general that C&FC must limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure. In addition, C&FC must limit their requests for PHI held by other entities to the minimum necessary to accomplish the intended purpose of their request. Disclosures that are not for treatment purposes must exclude direct identifiers of a client, to the extent possible. Child & Family Center is also required to implement standard protocols for disclosures that occur on a routine and recurring basis to ensure that such disclosures are limited to the amount necessary to accomplish the purpose of the disclosure. C&FC staff follow the procedures set forth by the Agency with respect to the use and disclosure of the minimum necessary amount of PHI necessary to accomplish the intended purpose.

The Privacy Officer (or designee) implements standard protocols for disclosures that occur on a routine and recurring basis. C&FC staff should direct all nonroutine requests for PHI to the Privacy Officer (or designee). For nonroutine disclosures, the Privacy Officer develops criteria by which to evaluate requests for PHI and should review requests for disclosures of PHI on a case by case basis. The Privacy Officer may rely on the representation of a person or entity that the request is limited to the minimum necessary required for the purpose of the disclosure when the following persons or entities request PHI:

- A public official
- Another covered entity
- Another member of the C&FC workforce
- Entities that request PHI for research purposes

The Privacy Officer (or designee) may rely on the person's or entity's request only if reliance is reasonable under the circumstances. It is also important to remember that the type of disclosure the person or entity requests must be otherwise permitted by the Privacy Rule (i.e., payment or healthcare operations). The Minimum Necessary Policy does not apply to:

- C&FC requests for PHI for treatment purposes
- Disclosures of PHI to other health care providers for treatment purposes
- Disclosures of PHI to the client or his or her representative
- Uses or disclosures made pursuant to a written authorization
- Uses or disclosures that are required by law

- Disclosures made to the Secretary of the U.S. Department of Health and Human Services for the purposes of compliance reviews and investigations

Finally, the Privacy Officer (or designee) must:

- Identify the staff who need access to PHI to carry out their duties
- For each such person, identify the types of PHI to which the person needs access and any appropriate conditions to such access (e.g., accounting staff generally does not need access to the entire medical record).

The Privacy Officer (or designee) must limit the access of the persons identified to the types of PHI to which they should have access. Routine disclosures to staff do not need to be evaluated on a case-by-case basis; rather each person's job description should identify the limits of that person's access to PHI.

Access to and Amendment of Behavioral Health Records

Clients should be able to view, copy, and amend information collected and maintained about them. An individual has the right to request that C&FC amend his or her health information. C&FC may require individuals to make such requests in writing and to provide a reason to support the amendment, provided that it informs individuals in advance of such requirements.

Child & Family Center may deny the request for amendment if the health information that is the subject of the request under the following circumstances:

- Information was not created by C&FC, unless the originator is no longer available to act on the request
- Information is not part of the individual's health record
- Information is accurate and complete.

Child & Family Center must act on an individual's request for amendment no later than sixty (60) days after receipt of the request. Provided that C&FC gives the individual a written statement of the reason for the delay, and the date by which the amendment will be processed, C&FC may have a onetime extension of up to thirty (30) days for an amendment request. If the request is granted, C&FC must:

- Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment.
- Inform the individual that the amendment is accepted.
- Obtain the individual's a) identification of and b) agreement to notify the relevant persons with whom the amendment needs to be shared.
- Within a reasonable time frame, make reasonable efforts to provide the amendment to persons identified including Business Associates that are the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the individual.

If Child & Family Center denies the requested amendment, it must provide the individual with a timely, written denial, written in plain language, which contains:

- Basis for the denial
- Individual's right to submit a written statement disagreeing with the denial and how the individual may

file such a statement

- Statement that if the individual does not submit a statement of disagreement, the individual may request that C&FC provide the individual's request for amendment and the denial with any future disclosures of PHI
- Description of how the individual may complain and to whom.

Other Procedures and Considerations

1. Child & Family Center must permit the individual to submit for inclusion in his/her record a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. C&FC may reasonably limit the length of a statement of disagreement.
2. Child & Family Center may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, C&FC must provide a copy to the individual who submitted the statement of disagreement.
3. Child & Family Center must, as appropriate, identify the record of PHI that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, our denial of the request, the individual's statement of disagreement, if any, and rebuttal, if any.
4. If the individual submitted a statement of disagreement, Child & Family Center must include the material appended or an accurate summary of such information with any subsequent disclosure of the PHI to which the disagreement relates.
5. If the individual has not submitted a written statement of disagreement, Child & Family Center must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action.
6. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, Child & Family Center may separately transmit the material required.
7. A Covered Entity that is informed by C&FC of an amendment to an individual's PHI must amend the PHI in written or electronic form, as applicable.

The Privacy Officer (or designee) is responsible for receiving and processing requests for amendments.

Receiving and Sending Faxes Including PHI

Child & Family Center interacts with other organizations as part of payment, treatment and operations and may need to transmit or receive PHI by fax. C&FC staff could, in error, send faxes to unauthorized recipients; faxes could be intercepted or lost in transmission; or C&FC may not receive a fax intended for it because of one of these or other reasons. To protect PHI that may be sent or received, staff must strictly observe standards relating to faxes that include PHI.

1. Staff will send PHI by fax only when the original record or mail delivered copies will not meet the needs of immediate client care, treatment and services or when it is impractical to send the PHI via encrypted email.
2. Staff will transmit PHI by fax to the client upon the client's request or to a third party upon the client's

request, provided the client provided a signed authorization.

3. Staff can transmit PHI by fax when required by a third party payer for payment purposes.
4. Staff must limit PHI transmitted to only that amount that is necessary to meet the requester's needs.
5. Staff may not send by fax especially sensitive medical information, including, but not limited to, HIV/AIDS, mental health and developmental disability, alcohol and drug abuse, and sexually transmissible diseases without the express authorization of the Privacy Officer (or designee).
6. The cover page accompanying the fax transmission must include the fax "Confidentiality Notice."
7. Staff must make reasonable efforts to ensure that they send the fax transmission to the correct destination.
    a. Staff can preprogram frequently used numbers into the machine to prevent misdialing errors.
    b. For a new recipient, the sender must verify the fax number before sending the fax, must verify the recipient's authority to receive PHI, and must confirm by telephone that the recipient received the information.
8. Fax machines must be in secure areas where incoming faxes are not visible to unauthorized persons.
9. Incoming faxes must not be left sitting on or near the machine, but immediately distributed to the intended recipient while protecting confidentiality during distribution.
10. Staff must report any misdirected faxes to the Privacy Officer (or designee).
11. Users must immediately report violations to their department head, the Privacy Officer or the Security Officer.
12. The Privacy Officer (or designee) may periodically and/or randomly check all speed dial numbers to ensure their currency, validity, accuracy, and to verify the authority of the recipient to receive PHI.

Using Email and/or Text to Send or Receive PHI

Clients often want to communicate with staff via email and/or text. However, transmitting PHI by email or text has a number of risks that clients should consider before using.

- Email can be immediately broadcast and received by many intended and unintended recipients.
- Recipients can forward messages to other recipients without the original sender's permission or knowledge.
- Users can easily misaddress an email.
- Copies of email / text may exist even after the sender or the recipient has deleted his or her copy.
- Messages containing information pertaining to a diagnosis and/or treatment must be included in the client's medical records. Thus, all individuals who have access to the medical record will have access to the email / text messages.
- There is no guarantee that any particular email / text message will be read and responded to within any particular period of time.
- Email / text messages should never be used in a medical emergency.

ll All email messages sent or received that concern the diagnosis or treatment are part of that client's medical record and such email messages are treated with the same degree of confidentiality as afforded other portions of the medical record. Reasonable means are used to protect the security and confidentiality of email information, including encryption of email communication when it is affordable and practicable. Because of the risks associated with email communication of PHI, clients must consent to the use of email for communication of PHI after having been informed of the above risks. Consent can be withdrawn in writing at any time. Consent to the use of email includes agreement with the following conditions:

- All emails to or from the client concerning diagnosis and/or treatment will be made a part of the client's medical record. As a part of the medical record, other individuals, such as other physicians, therapists, case managers and the like, and other entities, such as other healthcare providers and insurers, will have access to email messages contained in medical records.
- Emails may be forwarded within the facility as necessary for diagnosis, treatment, and reimbursement. C&FC will not, however, forward the email outside the facility without the consent of the client or as required by law.
- C&FC will strive to read client emails promptly and respond promptly, if warranted. However, no assurance can be provided that the recipient of a particular email will read the email message promptly. Because C&FC cannot assure clients that recipients will read email messages promptly, clients should be advised to not use email in a medical emergency.
- The client is responsible for following up to determine whether the intended recipient received the email and when the recipient will respond.

Because some medical information is so sensitive that unauthorized disclosure can be problematic, clients should not use email for communications concerning the diagnosis or treatment of HIV/AIDS or sexually transmissible or communicable diseases (e.g., syphilis, gonorrhea). Clients should be aware that information concerning mental health disorders, developmental disability, and substance use disorders has the same sensitivities and risks.

Employees and other staff at C&FC should not have an expectation of privacy in email / text they send or receive. Clients or their representatives who send or receive email / text from their place of employment risk having C&FC read email / text. Because employees and other staff do not have a right of privacy in the C&FC email system, Child & Family Center cannot guarantee that electronic communications will be private. The Agency takes reasonable steps to protect the confidentiality of client email but is not liable for improper disclosure of confidential information not caused by C&FC gross negligence or wanton misconduct and is not liable for breaches of confidentiality caused by client.

Protections Specific to Alcohol and Drug Abuse Treatment

There are special privacy protections afforded to alcohol and drug abuse treatment records by 42 Code of Federal Regulations ("CFR") Part 2. The privacy provisions in 42 CFR Part 2 intend to eliminate barriers that might prevent persons with substance use disorders from seeking treatment. The regulations outline under what limited circumstances information about the client's treatment may be disclosed with and without consent. 42 CFR § 2.20, states that "no State law may authorize or compel any disclosure prohibited by these [Part 2] regulations." However, States may impose additional confidentiality protections. Thus, § 2.20 provides that, "If a disclosure permitted under these regulations is prohibited under State law, neither these regulations

nor the authorizing statutes may be construed to authorize any violation of that State law." In California, the Health and Safety Code Section 11845.5 also gives special protections to records of certain substance abuse programs. Special protections are intended to apply to facilities such as outpatient methadone treatment programs and outpatient counseling programs, and not to general acute care hospitals or chemical dependency recovery hospitals.

The 42 CFR Part 2 applies to any individual or entity that is federally assisted and provides alcohol or drug abuse diagnosis, treatment or referral for treatment (42 CFR § 2.11). The regulations restrict the disclosure and use of alcohol and drug records that are maintained in connection with the performance of any federally assisted alcohol and drug abuse program (42 CFR § 2.3(a)). The restrictions apply to any information disclosed by a covered program that "would identify a patient as an alcohol or drug abuser …" (42 CFR §2.12(a) (1)). Simply, the information protected by 42 CFR Part 2 is any information disclosed by a covered program that identifies an individual directly or indirectly as having a current or past drug or alcohol problem, or as a participant in a covered program.

Communication of information between or among C&FC personnel who need such information to diagnose, treat, or refer for treatment of alcohol or drug abuse is permitted without client authorization, if the communications are within a program or between a program and an entity that has direct administrative control over the program [42 C.F.R. Section 2.12(c)(3)]. Under HIPAA, these uses of health information are permitted without authorization as they fall within the definition of "treatment, payment or health care operations."

With limited exceptions, 42 CFR Part 2 requires client consent for disclosures of protected health information even for the purposes of treatment, payment, or health care operations. Consent for disclosure must be in writing. Part 2 permits the disclosure of information under certain circumstances without consent during a medical emergency or in other limited situations. If a Part 2 program (or a healthcare provider that has received Part 2 client information) believes that there is an immediate threat to the health or safety of any individual, there are steps described below that the Part 2 program or healthcare provider can take in such a situation:

- *Notifications to medical personnel in a medical emergency*: A Part 2 program can make disclosures to medical personnel if there is a determination that a medical emergency exists, i.e., there is a situation that poses an immediate threat to the health of any individual and requires immediate medical intervention [42 CFR §2.51(a)]. Information disclosed to the medical personnel who are treating such a medical emergency may be redisclosed by such personnel for treatment purposes as needed. For additional information regarding disclosures during a medical emergency.
- *Notifications to law enforcement:* Law enforcement agencies can be notified if an immediate threat to the health or safety of an individual exists due to a crime on program premises or against program personnel. A Part 2 program is permitted to report the crime or attempted crime to a law enforcement agency or to seek its assistance [42 CFR §2.12(c)(5)]. Part 2 permits a program to disclose information regarding the circumstances of such incident, including the suspect's name, address, last known whereabouts, and status as a client in the program.
- *Immediate threats to health or safety that do not involve medical emergencies or crimes on programs premises or against program personnel:* Part 2 programs who have received Part 2 client information, can make reports to law enforcement about an immediate threat to the health or safety of an individual or the public if client-identifying information is not disclosed. Immediate threats to health or safety that do not involve a medical emergency or crimes (e.g., a fire) are not addressed in the regulations.

Programs should evaluate those circumstances individually.

- *Child abuse and neglect:* The restrictions on disclosure do not apply to the reporting under State law of incidents of suspected child abuse and neglect to the appropriate State or local authorities. However, Part 2 restrictions continue to apply to the original alcohol or drug abuse client records maintained by the program including their disclosure and use for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect [42 CFR § 2.12(c)(6)]. Also, a court order under Part 2 may authorize disclosure of confidential communications made by a client to a program in the course of diagnosis, treatment, or referral for treatment if, among other reasons, the disclosure is necessary to protect against an existing threat of life or of serious bodily injury, including circumstances which constitute suspected child abuse and neglect [42 CFR § 2.63(a)(1)].
- *Court ordered disclosures:* Under the regulations, Part 2 programs or "any person having a legally recognized interest in the disclosure which is sought" may apply to a court for an order authorizing disclosure of protected client information [42 CFR § 2.64]. Thus, if there is an existing threat to life or serious bodily injury, a Part 2 program or "any person having a legally recognized interest in the disclosure which is sought" can apply for a court order to disclose information.

Any employee or staff person with questions related to Part 2 should contact his/her supervisor or the Privacy Officer.

Reporting a Breach of Confidentiality

The federal HITECH Act requires that C&FC "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured protected health information." Each individual is notified when "unsecured PHI has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, or disclosed" because of a breach. Child & Family Center takes all reasonable steps to maintain the confidentiality of PHI. In the event of a confidentiality breach, the client is notified and if necessary, local, state and federal authorities are contacted. The following circumstances do not require client notification:

- Unintentional acquisition, access, or use of PHI by an employee or an individual acting under C&FC authority, provided that such unintentional activity was done in good faith, within the course of his or her duties and does not result in further use or disclosure that is not permitted by the HIPAA Privacy Regulations.
- Inadvertent disclosure of PHI by a person with authority to access PHI to another person who also has authority to access PHI (including a Business Associate), provided the recipient does not further disclose the information in violation of the HIPAA Privacy Regulations.
- Unauthorized disclosures where, based on the good faith belief of the disclosing person, the recipient to whom the PHI is disclosed would not reasonably have been able to retain the information.

Employees and other staff who becomes aware of a breach immediately report the incident to the Privacy Officer and the supervisor. The Privacy Officer (or designee) investigates the incident and confirms (1) whether unsecured PHI was involved (2) whether a breach occurred, (3) whether the breach affected more than 500 clients, and (4) the identity of the client or clients whose PHI was breached.

Child & Family Center will notify a client in writing by U.S. Mail as soon as possible, but in any event, no later than sixty (60) days following the discovery of the breach. If the breach involves ten (10) or more clients whose

contact information is out of date, C&FC will post a notice of the breach on the Agency's website home page. If the breach involves more than five hundred (500) clients, C&FC will send a notice of the breach to a prominent media outlet in Los Angeles County and immediately notify the Secretary of the US Department of Health and Human Services and any local authority as required.

The Notice will include the following:

- A brief description of the breach, including the date of the breach (if known) and the date of its discovery;
- A description of the types of PHI involved in the breach;
- Steps the client can take to protect himself/herself from potential harm resulting from the breach;
- A brief description of the actions C&FC is taking to investigate the breach, mitigate losses, and protect against further breaches;
- Contact information, including a toll-free telephone number, email address, or postal address to permit the client to ask questions or obtain additional information; and
- Any sanctions imposed.

The Privacy Officer (or designee) compiles a log of breaches and works with C&FC executives, directors, managers and supervisors to minimize such breaches.

SECURITY

The integrity and security of behavioral health information are closely related. Information is collected and processed through various information sources and systems throughout Child & Family Center. As a result, breaches in security can lead to the unauthorized disclosure or alteration of health information. When this occurs, the integrity of the data and information is compromised. Even simple mistakes, such as writing the incorrect date of service or diagnosis, can undermine data integrity just as easily as intentional breaches. For these reasons, an examination of the use of paper and electronic information systems is considered in Child & Family Center's approach to maintaining the security and integrity of health information. Regardless of the type of system, security measures address the use of security levels, passwords, and other forms of controlled access. Because information technology and its associated security measures are continuously changing, C&FC stays informed about technological developments and best practices that can help it improve information security and protect data integrity.

Monitoring access to health information can help organizations be vigilant about protecting health information security. Regular security audits help Child & Family Center identify system vulnerabilities in addition to security policy violations. For example, as part of the process, the organization could identify system users who have altered, edited, or deleted information. The results from this audit process can be used to validate that user permissions are appropriately set. Conducting security audits can be particularly effective in identifying when employee turnover causes vulnerabilities in security because user access and permissions were not removed or updated.

Child & Family Center has appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. These safeguards reasonably safeguard PHI and electronic PHI and make reasonable efforts to prevent any intentional or unintentional use or disclosure that violates the Privacy and Security Rules. Program directors,

managers and supervisors must ensure that their staff are in compliance with the security policies and procedures to include but not be limited to:

- Employees and other staff ("volunteers, interns and contractors") under their supervision implement security measures as defined in this Guide.
- Employees and other staff under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
- Employees and other staff who are authorized to use personal computers, portable computers or handheld devices are aware of and comply with the policies and procedures outlined in this manual and all Child & Family Center documents that address information security.
- Employees and other staff under their supervision complete the exit process upon their official termination of employment or contractual agreement.
- Employees and other staff under their supervision make backup copies of sensitive, critical, and valuable data files as often as is deemed reasonable

Information Security

The use of computers, computer networks and other technologies is an integral part of the Child & Family Center business and clinical operations. These technologies bring significant risks regarding confidentiality and privacy that require reasonable technological and physical safeguards to protect the security and integrity of all electronically maintained PHI. The specifics of security problems should not be discussed widely but should instead be shared on a "need to know" basis.

Reporting Security Concerns or Problems

1. If any client's PHI is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Security Officer (or designee) must be notified immediately.
2. If any unauthorized use of C&FC's information systems has taken place, or is suspected of taking place, the Security Officer (or designee) must be notified immediately.
3. Whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Security Officer (or designee) must be notified immediately.
4. All unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported to the Security Officer (or designee).

Security Responsibilities of All C&FC Staff

- Know and apply the appropriate policies and practices pertaining to Internet security.
- Not permit any unauthorized individual to obtain access to C&FC's Internet connections, or data, including but not limited to, the PHI of clients.
- Not use or permit the use of any unauthorized device in connection with personal computers.
- Only use C&FC Internet resources (software/hardware or data) for authorized company purposes.
- Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.

- Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess.
- Ensure that data under his/her control and/or direction are properly safeguarded according to its level of sensitivity.
- Report to the Security Officer or IT staff as designated, any incident that appears to compromise the security of C&FC information resources. These include missing data, virus infestations, and unexplained transactions.
- Access only the data and automated functions for which he/she is authorized in the course of his/her normal job functions (minimum necessary).
- Obtain supervisor authorization for any uploading or downloading of information to or from any C&FC multiuser information system if this activity is outside the scope of normal business activities.
- All Agency data are maintained on the C&FC network storage location.

Password Protection

Most client information is stored in electronic computer networks and devices at Child & Family Center. Efforts are taken to ensure that access to those computers, networks, and devices is strictly limited to authorized staff with a need to know and/or view that information. A key element of access control is the use of access codes and passwords. This section outlines the specific policies and procedures for management of those codes and passwords.

The confidentiality and integrity of data stored on Child & Family Center computers and other devices are protected by access controls to ensure that only authorized employees, staff and agents have access. Each person with a need to use Child & Family Center computer systems and networks will have a unique user name and password. Procedures related to password protection include:

- The password expires every 90 days.
- A password may not be reused in less than six months.
- Passwords should not be associated with personal information (e.g., PIN used for bank cards, date of birth for self or family members, telephone numbers, first or last name of self or family members, passwords used for Internet accounts).
- Passwords should be entered each time the user logs in; options should not be set to automatically log in or “remember” passwords.

<u>IT Department Responsibilities</u>

- The Information Technology Department is responsible for the administration of Access Controls to all Agency computer systems.
- The Information Technology Department deploys and maintains a set of system/network access and password procedures that require unique user identification codes and passwords that conform to the characteristics outlined above.
- The Information Technology Department assigns responsibility for maintenance of the access code and password assignment to a primary, qualified individual in the Information Technology Department. A

staff person of the Department will also be assigned these duties as a backup to the primary staff person.

- The Information Technology Department processes, adds, deletions, and changes upon receipt of a written request from the end user's supervisor. Deletions may be processed by an oral request prior to reception of the written request.
- The Information Technology Department conducts an audit of the access code and password policies to ensure that Child & Family Center staff is complying with these procedures. This will be done quarterly by selecting 10 random active accounts.

Employee and Other Staff Responsibilities

- Responsible for all computer transactions that are made with User ID and password.
- Do not disclose password to others.
- Immediately change password if it is suspected that it has become known to others. In the event that an employee or other staff suspects or knows that the password has become known to an unauthorized person, this should be immediately reported to the IT Help Desk.
- Do not record password where it may be easily obtained.
- Do not display passwords in any area that can be viewed by others.
- Do not use passwords that will be easily guessed by others.
- Log out when leaving a workstation for more than 15 minutes or when leaving the premises for any length of time.

Supervisor Responsibility

- Managers and supervisors should notify the Information Technology Department promptly whenever an employee or other staff leaves the company so that access can be revoked.
- Involuntary terminations must be reported concurrent with the termination.

Human Resources Responsibility

- The Human Resources Department will notify the Information Technology Department of transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

Violations and Penalties

Penalties for violating this Password Protection policy vary depending on the nature and severity of the specific violation. Any employee or other staff who violates the policy may be subject to:

- Disciplinary action as described in the Child & Family Center employee handbook, including but not limited to reprimand, suspension, and/or termination of employment.
- Civil or criminal prosecution under federal and/or state law.

Acknowledgment of Password Protection

Employees and other staff are asked to acknowledge receipt of and compliance with the Child & Family Center's

Password Protection Policy, which is retained in the employee's personnel records.

Software and Hardware Policy

Child & Family Center ensures the quality, maintenance and effectiveness of its software and hardware. Hardware devices, software programs, and network systems purchased and provided by C&FC are to be used only for creating, researching, and processing Agency materials. Employees and other staff assume personal responsibility for the appropriate use and agree to comply with this policy and other applicable C&FC policies, as well as city, county, state, and federal laws and regulations, including the HIPAA Privacy and Security Rules.

Software

All software acquired for or on behalf of C&FC employees or contract personnel is deemed Agency property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements. Software purchasing is centralized with the Information Technology Department to ensure that all applications conform to Agency software standards. All requests for software must be submitted to the IT Department for approval. Each employee or contracted personnel is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses that are part of the standard suite of software installed on Agency computers.

Hardware

All hardware devices acquired for or on behalf of Child & Family Center employees or contract personnel are deemed Agency property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements. All purchasing of hardware devices is centralized with the Information Technology Department to ensure that all equipment conforms to Agency hardware standards.

Violations and penalties

Penalties for violating the Software/Hardware Policy depend on the nature and severity of the specific violation. Any employee who violates the Software/Hardware Policy will be subject to:

- Disciplinary action as described in the Employee Handbook, including but not limited to reprimand, suspension, and/or termination of employment or contract
- Civil or criminal prosecution under federal and/or state law.

Laptop and Portable Device Policy

Laptop computers and other portable electronic devices pose a significant security risk because they may contain PHI. Being portable, these devices are more at-risk for loss, theft, or other unauthorized access. In addition, laptop computers may be more vulnerable to viruses and other threats because the user may not regularly use virus protection software and other electronic safeguards available on the C&FC network. Portable computer use is more difficult to audit so security breaches may be more difficult to identify and to correct.

No user may, for any purpose, download, maintain, or transmit PHI onto a personally owned computer or personally owned portable electronic device without the written authorization of the Information Technology Department. The Information Technology Department may issue Agency-owned laptops or portable electronic devices to an employee or other staff person who is determined by his or her supervisor to have a demonstrated need for such technology. The Information Technology Department keeps a record of all employees and other staff who have been issued such equipment.

Security Responsibilities

As defined below, the IT Department and staff members responsible for security are to establish a clear line of authority and responsibility.

- Information Technology staff will establish an Internet security infrastructure consisting of hardware, software, policies and standards, and department staff will provide technical guidance on PC security to all C&FC staff.
- The IT Department will also organize an emergency response plan and team to respond to virus infestations, hacker intrusions, and similar events.
- IT staff will monitor compliance with security requirements, including hardware, software, and data safeguards.
- IT staff provide administrative support and technical guidance to management on matters related to security.
- IT staff will periodically conduct a risk assessment of each production information system they are responsible for to identify risks and vulnerabilities.
- IT staff will check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
- IT staff will check that user access controls are defined on these systems in a manner consistent with the need to know.
- C&FC information owners will see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with Agency sensitivity classifications.

OTHER

Staff Training for Privacy, Confidentiality & Security

Child & Family Center provides initial and ongoing training to employees and other staff to ensure they have the knowledge required to protect the privacy and security of PHI in the delivery of behavioral health care, treatment and services. All personnel must have some degree of basic training concerning the policies and procedures; however, some employees and other staff require more training than others, depending upon their functions within the Agency.

Child & Family Center trains all employees and staff on the policies and procedures related to privacy, confidentiality and security of health information as necessary and appropriate for them to carry out their respective functions within the agency. Training is provided to Child & Family Center employees and other staff including volunteers, affiliates, contractors, students, residents, and other persons who are likely to have contact with protected health information. Child & Family Center documents that the training is provided.

Training on privacy, confidentiality and security may include but is not limited to the following topics:

- General awareness of privacy, confidentiality and security issues, including specific awareness of HIPAA regulations and special requirements with sensitive information such as substance use disorders and HIV/AIDs
- Child & Family Center policies and procedures with respect to protected health information and

information security

- Vulnerabilities of health information in Child & Family Center's environment
- Security responsibilities of all employees and other staff
- General security awareness and responsibility
    - Password protection
    - Virus prevention
    - Data backup procedures
    - Remote access
    - Proper authorization and consent to release procedures
    - Workstation acceptable use policies and practices
    - Client rights and responsibilities regarding medical records
    - Procedures to follow in case of a suspected breach of security or privacy
    - Disaster plan and emergency procedures

Basic privacy and security awareness training is offered to employees and staff upon hire and annually. Any training completed is documented by the acknowledgement of training receipt form or sign-in sheet. At least every 12 months, the Information Technology Department publishes a privacy and security reminder via email to all staff.

Disciplinary Actions

All supervisors are responsible for enforcing the Policies and Procedures outlined in the *Guide*. Any person who violates these policies is subject to discipline up to and including termination of employment/contract.

False Claims

Under the provisions of the federal and state false claims acts (FCAs), employees and other staff have the right to report violations of federal and state law. Child & Family Center is committed to combatting fraud, waste and abuse and understands the remedies and fines for violations that can result from certain types of fraudulent activities.

Reporting Fraud, Waste and Abuse

All employees, contractors, and agents of Child & Family Center must immediately report to the Privacy Officer any suspicion of fraud, waste, or abuse in connection with the business of Child & Family Center. The state and federal FCA imposes civil and criminal penalties on people and entities that knowingly submit a false claim, or act in deliberate ignorance of the claim's truth or falsity or act in reckless disregard of its truth or falsity or conspire to defraud the government by getting a false or fraudulent claim paid. Specific intent to defraud Medicare, Medicaid or other government programs is not required. Individuals or entities that commit fraud against the state or federal government, by false claims or statement, can be assessed money penalties in addition to the penalties of the FCA.

The FCA includes an important provision that allows private citizens to initiate a lawsuit on behalf of the federal government and request the government to join in the suit. In return, that citizen may share a percentage of any recovery or settlements. The FCA is not confined to healthcare claims, but extends to any payment requested of the federal government. The FCA applies to billing and claims sent from Child & Family Center any government payer program, including Medicare and Medicaid. It is the policy of Child & Family Center that an employee, contractor or agent who knowingly submits a false claim will be reported to the necessary authorities.

Examples of potential false claims include, but are not limited to: (a) billing of items or services that were never rendered by the health care provider; (b) billing for services that are medically unnecessary; (c) up coding (practice of billing for Medicare/Medi-Cal using a billing code providing a higher payment rate than the billing code intended to be used for the service or item furnished to the client); (d) billing separately for services that should be bundled; (e) billing for a discharge in lieu of a transfer.

Whistleblower Protection

The FCA protects employees who are discharged, demoted, suspended, harassed, or in any manner discriminated against by their employer because of their participation or assistance (e.g., testimony, initiation of investigation) in a false claim action. The Act entitles employees to relief to "make them whole," including restatement with the same seniority status they would have had but for the discrimination, twice the back pay, interest on back pay, and compensation for any special damages sustained as a result of the discrimination including litigation costs and reasonable attorney fees.

Business Associates

Business Associates are people or entities who perform a function or activity for or on behalf of Child & Family Center in a manner that requires the use or disclosure of PHI. The HIPAA Privacy Regulations require all covered entities to enter into special contracts with Business Associates called a “Business Associate Agreement (BAA).” The BAA imposes certain privacy and security obligations upon the Business Associate and provides Child & Family Center with certain rights and remedies if the Business Associate breaches the BAA. The federal HITECH Act imposes certain privacy and security obligations directly upon Business Associates. The BAA contains certain provisions whereby the Business Associate agrees to comply with those obligations.

At least annually, C&FC takes an inventory of all vendors and contractors and determine which of them qualify as Business Associates. Every Business Associate is required to execute the BAA with Child & Family Center. The Controller (or designee) takes an inventory of all vendors and contractors of Child & Family Center and determines which are Business Associates. The Controller (or designee) ensures that each Business Associate has executed the “Business Associate Agreement” and retains all BAAs on file.

REFERENCES

1. California Hospital Association. Chapter 10. Use and Disclosure of PHI: Substance Abuse (2012). Available at: http://www.dhcs.ca.gov/provgovpart/Documents/Duals/Workgroups/Behavioral%20Health/Meeting%202/UseandDisclosure%20of%20PHI-SubstanceAbuse.pdf
2. California Office of Privacy Protection. A California Business Privacy Handbook (2008).
3. Easter Seals. Compliance, Privacy & Security Policies and Procedures (2014).
4. The Joint Commission. Behavioral Health Standards Manual (2016).
5. Los Angeles County Department of Mental Health. RESPONDING TO BREACH OF PROTECTED HEALTH INFORMATION POLICY NO.506.03, Effective May 3, 2011.
6. The Office of the National Coordinator for Health Information Technology. Guide to Privacy and Security of Electronic Health Information, Version 2.0 (2015).
7. Substance Abuse and Mental Health Services Administration. Applying the Substance Abuse Confidentiality Regulations 42 CFR Part 2 (REVISED-December 14, 2011). Available at: http://lac.org/wp-content/uploads/2014/12/SAMHSA_42CFRPART2FAQII_Revised.pdf

APPENDIX A. DESCRIPTION OF RELATED C&FC FORMS

Request for Correction/Amendment of Health Information

Access to Records Request form

Business Associate Agreement

Notice of Privacy Practices

Authorization for Use or Disclosure of Protected Health Information

Confidentiality Notice

Consent to Use of Email/Text Form

Onsite Inspection Checklist