# PROCEDURE

| | | |
|---|---|---|
| **Series:** | **Operating Procedures** | **COA: NET 6.03**<br>**CFOP: 175-04** |
| **Procedure Name:** | Privacy and Security Practices | |
| **Procedure Number:** | OP 1217 | |
| **Review Date:** | 12/9/19 | |
| **Revision #/Date:** | 04/21/2020 | |
| **Effective Date:** | 01/17/17 | |
| **Applicable to:** | Brevard Family Partnership Family of Agencies (BFP FOA) Staff | |

PURPOSE:

The purpose of this procedure is to establish privacy and security Practices procedure is to ensure that CBCIH and BFP comply with laws and regulations concerning privacy and the protection of information as well as to protect the rights and privacy of children and families in the process of gathering and disseminating information in accordance with the Sunshine Health Child Welfare Vendor Agreement.

## PROCEDURE:

CBCIH and BFP staff are required to report any real or suspected incidents of privacy disclosures in accordance with the Health Insurance Portability and Accountability Act of 1996 and the Vendor Agreement between Sunshine Health and CBCIH.

### *Cross Reference(s)*

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
State of Florida, Department of Children and Families, CFOP NO. 60-17, Privacy and Management of Protected Health Information
HITECH Act

### *Scope*

This operating procedure applies to all Brevard Family Partnership and its subcontracted agencies who are responsible for children who are enrolled in the Child Welfare Specialty Plan. If any of the responsibilities outlined in this procedure are contracted with an individual or other entity, the contracted provider must ensure compliance with this procedure, and the terms should be incorporated into the contract.

### *Application*

This procedure applies to CBCIH and BFP Staff, and addresses care coordination activities that are provided on behalf of all CWSP plan enrollees.

### *Key Terms*

Child Welfare Specialty Plan Enrollee—a child who is Medicaid eligible and is enrolled in the Sunshine Health, Child Welfare Specialty Plan, or the Sunshine Health Managed Medical Assistance Plan (MMA), due to an active status in the child welfare system of care. This includes

children who have an open child welfare case, those who have been adopted from dependency and those who are receiving extended foster care or independent living services.

Community Based Care Lead Agency—an "eligible lead community-based provider" as defined in Section 409.1671(1)(e), F.S.

Contracted Service Provider—a private agency that has entered into a contract with the Department of Children and Families (DCF) or with a Community-Based Care Lead Agency to provide supervision of, and services to, dependent children and those children who are at risk of abuse, neglect, or abandonment.

Integrate®—a web-based information system designed to integrate physical health, behavioral health and child welfare data into a single platform of applications.

Medicaid—a program authorized by Title XIX of the Social Security Act. It is a state-administered health insurance program that is jointly funded by the Federal and State governments. Medicaid is an open-ended entitlement program, with states receiving federal reimbursement for every eligible claim they submit. Medicaid, as defined in Rule 59G-1.010, F.A.C., includes eligibility based on income for most groups using Modified Adjusted Gross Income (MAGI).

Electronic Data Exchange or EDI—defines the format of electronic transfers of information between providers and payers to carry out financial or administrative activities related to health care (includes coding, billing and insurance verification).

Protected Health Information (PHI)—individually identifiable health information that relates to the past, present or future physical or mental condition of a Client; the provision of health care to a Client; or the past, present or future payment for the provision of health care to a Client; and identifies the Client; or the information can be used to identify the Client. It is transmitted or maintained in any form (electronic, oral, or paper) by the Department or its business associates.

***Standards***

This procedure acknowledges that CBCIH and BFP subcontractors conduct themselves in a manner that is consistent with the Health Insurance Portability and Accountability Act of 1996 and the requirements set forth within the State of Florida, Department of Children and Families operating procedures. The Health Insurance Portability and Accountability Act of 1996 (HIPAA):

- Protects the privacy of a client's health care data (including genetic information).
- Controls the confidentiality of electronically protected health information or ePHI (including how it is stored and accessed)

BFP adheres to our organization's Privacy and Security policies and procedures related to HIPAA. CBC Lead Agencies are considered "downstream" entities from Sunshine as the main contractor for Medicaid/Medicare, and as a downstream vendor, certain additional requirements are applicable, as indicated within the Florida Managed Medical Assistance Program Services Agreement and in accordance within BFP Annual Contract Compliance Attestation, which includes, but is not limited to, the following:

1. All exchanges of confidential information with all individuals adhere to the parameters established by regulatory and state mandates and privacy policies.
2. Prior to enrollment in the CWSP, no data/information shall be provided to Sunshine Health by CBCIH.

3. Documents, forms and any other materials which contain protected health information (PHI) shall follow federal regulations for protecting and disseminating PHI (e.g., HIPAA, HITECH).
4. PHI shall be kept physically secure within a locked office or file cabinet.
5. Identification of a HIPAA Compliance Officer and IT Security Officer who is responsible for:

- Developing and implementing Privacy and Security Policies and Procedures, including the process and tracking methods for data breaches and PHI disclosures
- Distributing and posting of the Notice of Privacy Practices
- Training of staff and ongoing monitoring efforts, consistent with DCF requirements (i.e., annual HIPAA and Security Awareness Training, http://www.myflfamilies.com/generalinformation/dcf-training)
  - (a) At minimum, HIPAA and Security Awareness Training must occur within thirty (30) days of hire and annually thereafter.
  - (b) Follow up training may be recommended upon the identification of privacy violations, issues or concerns, or as corrective action requested during annual compliance monitoring.
  - (c) BFP is monitored by CBCIH annually, to include a review of privacy practices, policies/procedures, training efforts and internal monitoring processes.
- Maintaining a list of all Subcontractors that receive, create, maintain or transmit PHI on behalf of CBCIH, Sunshine/Centene and the Child Welfare Specialty Plan
- Maintaining a Disclosures Log (via a list or report) for disclosures that have occurred in the last 3 years
- Completing an annual HIPAA Privacy and Security Risk Assessment (e.g.,http://www.hhs.gov/about/news/2014/03/28/hhs-releases-security-risk-assessment-tool-to-help-providers-withhipaa-compliance.html)
- Providing Notification to the Community Based Care Integrated Health, Contract Compliance Manager/Privacy Officer, and, upon request, to the Sunshine Health Compliance Department, regarding:
  1. Potential data breaches and inadvertent disclosures of personal health information (PHI), including documentation and tracking of each instance.
  2. Potential breaches should be reported as soon as reasonably possible, but in no case should they be reported more than fourteen (14) calendar days following discovery of the breach. BFP is required to utilize CBCIH Form 1004A, Data Breach Reporting, to be completed in its entirety to include the following information:
     - Description of the circumstances under which the breach occurred;
     - The date of the breach and the date that the breach was discovered; • Description of the types of PHI involved in the incident;
     - Identification of each Individual whose PHI is known or is reasonably believed by BFP to have been affected;
     - Recommendations that BFP may have, if any, regarding the steps that Individuals may take to protect themselves from harm.
  3. Report privacy concerns to the CBCIH Contract Compliance Manager/HIPAA Privacy Officer CBCIH Compliance Officer:

     at 1-321-207-8330 compliance@cbcih.com

Once CBCIH is notified of a potential data breach, all related correspondence is maintained in a log and the HIPAA Privacy Officer conducts an internal risk assessment of the event, utilizing the CBCIH FHIPAA Four-Factor Risk Assessment Form (Form 1004B) to assess the Follow-up actions may include the provision of additional training and the requesting of additional information, as indicated.

Upon receipt of information related to a potential data breach, CBCIH provides email notification to Sunshine Health (CWSP Notifications CWSP_Notifications@CENTENE.COM). Notification includes identification of the impacted enrollee(s), completed Data Breach Notification Form(s) and additional information related to the event, as applicable.

Further, CBCIH and BFP must comply with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, including without limitation, the Standards for Electronic Transactions and Code Sets (45 CFR Parts 160 and 162), the Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164), the Security Standards for the Protection of Electronic Protected Health Information (45 CFR Parts 160 and 164) and such other regulations that may, from time to time, be promulgated thereunder, and including the amendments thereto pursuant to the Health Information Technology for Economic and Clinical Health Act, part of the American Recovery and Reinvestment Act of 2009, and regulations promulgated thereunder (collectively, "HIPAA"). The Parties agree not to use or further disclose any Protected Health Information or Individually Identifiable Health Information, as defined at 45 CFR § 160.103, other than as permitted by HIPAA.

**Administrative Safeguards**

CBCIH and BFP must comply with all HIPAA Privacy, Security and Breach Notification Rule requirements and must have the following administrative safeguards:

1. Security Management Process 45 C.F.R. §164.308(a)(l)
   a. Risk Analysis [45 C.F.R. §164.308(a){l{ii)(A)] – CBCIH conducts an accurate and thorough assessment of potential risks and vulnerabilities to ePHI through the engagement of a HITRUST assessor.
   b. Risk Management [45 C.F.R. §164.308(a)(l(ii)(B)] – CBCIH implements security measures sufficient to reduce risks and vulnerabilities based on the Security Risk Assessment completed by a third-party HITRUST assessor.
   c. Information System Activity Review [45 C.F.R. §164.308(a)(l)(ii)(D)] – CBCIH has a process to regularly review records of Integrate activity, such as audit logs, access reports and incident reports.
   d. Security Awareness Training [45 C.F.R. §164.308(a)(5)(i)] – CBCIH staff complete Security Awareness Training annually that is provided by the Florida Department of Children and Families.
   e. Password Management [45 C.F.R. §164.308(a)(5)(ii)(D)] – CBCIH utilizes password management procedures provided by Embrace Families via a Management Agreement.
   f. Security Incident Procedures [45 C.F.R. §164.308(a)(6)(i)] – CBCIH utilizes security incident procedures provided by Embrace Families via a Management Agreement
   g. Response and Reporting [45 C.F.R. §164.308(a)(6)(ii)] – CBCIH utilizes procedures to respond to suspected or known security incidents or data breaches, both internally and by business associates
2. Business Associate Agreements [45 C.F.R. § 164.308(b)] – CBCIH has executed business associate agreements with all vendors who receive or have access to ePHI from CBCIH as the

covered entity. a. Subcontractors [45 C.F.R. §164.308(b)(2)] – CBCIH requires all subcontractors to have executed business associate agreements with CBCIH as the covered entity.

**Organizational and Administrative Requirements**

CBCIH and BFP must comply with all HIPAA Privacy, Security and Breach Notification Rule requirements and must have the following organizational requirements:

1. Subcontractors [45 C.F.R. §164.314(a)(2)(iii)] – CBCIH requires all subcontractors to have business associate agreements.
2. Safeguards [45 C.F.R. §164.530(c)] – CBCIH has appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
3. Mitigation [45 C.F.R. §164.530(f)] – CBCIH mitigates, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information in violation of its policies and procedures.
4. Breach Risk Assessment [45 C.F.R. §164.402(2)] – CBCIH performs a four-factor risk assessment to determine if there is a low probability that ePHI has been compromised.
5. Notification to Individuals [45 C.F.R. §164.404] – CBCIH follows the requirements to notify each individual who's unsecured ePHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach. A sample notification form is attached
6. Substitute Notice [45 C.P.R. §164.404(d)(2)] – CBCIH provides a substitute form of notice reasonably calculated to reach the individual In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual.
7. Notification to the Media [45 C.F.R. §164.406] – For a breach of ePHI involving more than 500 members, CBCIH shall notify prominent media outlets.
8. Timeliness of Notification [45 C.F.R. §164.406 (b)] – CBCIH provides the required notification without reasonable delay and in no case later than 60 calendar days after discovery of a breach.

BY DIRECTION OF THE CHIEF EXECUTIVE OFFICER:

PHILIP J. SCARPELLI
Chief Executive OFFICER
Brevard Family Partnership Family of Agencies

APPROVAL DATE: 5/1/2020