HIPAA & Business Associates

San Gabriel/Pomona Regional Center

HIPAA and Business Associates Agenda

1. Brief History of HIPAA
2. What is a Business Associate?
3. What changed and why are we here today?

Disclaimer

This Training Is **NOT LEGAL ADVICE**

INFORMATION PROVIDED IS STRICTLY FOR EDUCATIONAL PURPOSES ONLY AND IS NOT, NOR IS IT INTENDED TO BE , CONSIDERED OR INTERPRETED IN ANY MANNER WHATSOEVER AS LEGAL ADVICE.

Please contact an attorney for legal advice.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA passed in **1996** and created two sets of rule.

Privacy Rules established national standards to identify what health information should be protected and how ***protected health information (PHI)*** can be used and disclosed.

Security Rules soon followed to establish national standards to protect ***electronic protected health information (ePHI)***.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Originally Regulated Covered Entities (CE)

- Health Plans
- Health Care Clearinghouses
- Health Care Providers

DDS is a Covered Entity under HIPAA

What is a Business Associate (BA)?

- **Regional Centers qualify as a Business Associate of the DDS**
- A person or entity that creates, receives, maintains, or transmits PHI and/or electronic PHI on behalf of Contractor.
- Originally, Business Associates and sub-contractors were not directly subject to compliance obligations and penalties.
- As a sub-contractor of the Regional Center most of this did not directly apply to vendors through their relationship to the regional center.

What changed?

- **Health Information Technology for Economic and Clinical Health Act (HITECH)**
  - Passed in 2009.
  - Intended to promote the adoption and meaningful use of health information technology.

- **HIPAA Omnibus Rules**
  - Released in 2013
  - Implemented the changes to HIPAA outlined in HITECH.

Significantly changed parts of HIPAA in relation to Business Associates.

What changed?

Some of the biggest changes included in the new HIPAA-HITECH Omnibus rules were:

- Require BA's to comply with the HIPAA Security Rule
- Require BA's to comply with provisions of the Privacy Rule outlined in their Business Associate Agreement (BAA)
- **Sub-contractors of a Business Associate who meet the same definitions are now also covered as Business Associates**
- Created a Breach Notification Standard

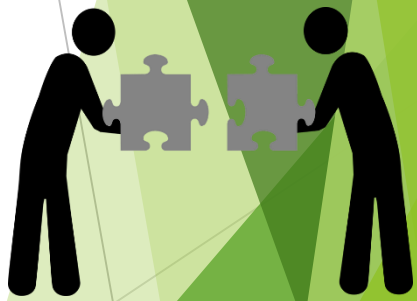
Fast Forward To Today

- **Contract between Regional Centers and the DDS has been updated effective Fiscal Year 17/18.**

- It now includes the required Business Associate language between Regional Centers and the DDS.

- Specifically requires Regional Centers to implement Business Associate Agreements with all sub-contractors (Vendors) who create, maintain, receive, or transmit PHI and/or electronic PHI on behalf of the Regional Center.

- Includes requirements on Breach Reporting for the Regional Center and all Vendors.



Where to Start?

- Policies and Procedures
- Engage legal counsel or consultants to help
- Review your existing contracts to determine if you need to establish a Business Agreement yourself (i.e. Email Encryption Services, Cloud Backups, etc).
- Read the HIPAA Rules (or at least the HHS Summary)

In addition you will need to…

Designate a Privacy Officer

- Regional Centers and Vendors must identify a **Privacy Officer** who is responsible for:
  - Receiving complaints/notices pertaining to breaches, and processing them according to the BAA, HIPAA and State Breach Reporting requirements.
  - Be the point of contact for communication on privacy matters with the Regional Center and the DDS.
  - Provide annual training to all employees on how to handle records; and
  - Keep paperwork including employee name, date and signature for each employee trained that documents the yearly training

Designate a Security Officer

- Regional Centers and Vendors must identify a **Security Officer** who is responsible for:
  - Overseeing the agencies data security program
  - Carry out the requirements outlined in the BAA and HIPAA Security Rules
  - Be the point of contact for communication on security matters with the Regional Center and the DDS

This is usually, but not always, an IT person.

The Privacy Officer and Security Officer may be the same person and/or may be contracted out.

Training and Information

- There is a lot of decent free training out there for yourself and your staff.

- Training on Privacy and Security is required annually for all staff.
- **HHS.gov**
  Various training videos, presentation slides and Q&A's on HIPAA topics.

- **HealthIT.gov**
  Great site. They have a Privacy and Security section specifically focused on providing help and materials to get started with HIPAA.

- **HIPAACOW.ORG**
  Site out of Wisconsin that provides a lot of material. Including guides, presentations and training.

Perform a Risk Analysis

- A written assessment required for Security Rule compliance.
- "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information" held by your agency. 45 CFR § 164.308(a)(1)(ii)(A).
- Should be re-done periodically and when any system containing ePHI changes.
- You can do this yourself or contract it out.
- **HealthIT.gov** has a risk assessment tool to help walk you through doing one.

Encryption

- Under California Civil Code §1798.82, “encrypted” means:
- “rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.”

- Recommend using software based on the Federal AES-256 Standard (most are now days).

- Windows and Mac have built in encryption options.
  - Bitlocker (Windows)
  - FileVault (Mac)

- **Using a Password by itself is NOT encryption!**

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29

What is Personally Identifiable Information (PII)?

- **Personally Identifiable Information (PII)** is any information about an individual that can be used to distinguish or trace an individual's identity; and any other information that is linked or linkable to an individual.

What is Protected Health Information?

- **Protected Health Information (PHI)** is any information in a medical record or designated record set that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment.

What is Protected Health Information?

Examples of some of the HIPAA PHI Identifiers:

- Electronic mail addresses;
- Medical record numbers;
- Health plan beneficiary numbers;
- Full face photographic images and any comparable images; and
- Any other **unique identifying number,** characteristic, or code

Administrative Safeguards

- **Administrative Safeguards**
- Administrative actions, and policies and procedures to protect ePHI and to manage the entity's workforce in relation to the protection of that ePHI.
- **Examples:**
- Policies and Procedures
  - Sanction Policy (Required)
  - Clear Desk Policy
  - Working with information in the field
- Risk Analysis
- Risk Management

Technical Safeguards

- **Technical Safeguards**
- The technology and the policy and procedures for it's use that protect ePHI and control access to it.
- **Examples:**
- Policies and Procedures
  - Password Policy
  - Data Access
  - Remote Access
  - Handling of portable media
- **Encryption**

Physical Safeguards

- **Physical Safeguards**
- The physical measures, policies, and procedures to protect ePHI and related buildings and equipment, form natural and environmental hazards, and unauthorized intrusion.
- **Examples:**
- Policies and Procedures
  - Building Access
  - Workstation Use/Location
    (i.e. Not facing monitors towards windows, Privacy Screens, etc)
- **Door Locks**
- **Alarm Systems**
- **Data Backups**

Minimum Necessary Requirement

- Make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- Evaluate practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.
- Does not apply when:
  - Dealing directly with the individual
  - The individual has authorized the disclosure
  - Disclosure to or requests by health care providers for treatment purposes

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html

Business Associate Agreement

- SG/PRC has dedicated a webpage on the SG/PRC with regards to the Business Associate Agreement, including the memo to service providers dated 10/27/17, Instructions for completing the BAA and this Powerpoint presentation. This information is located at:

  http://www.sgprc.org/service-providers/business-associate-agreement
- The BAA is an electronic pdf document, which can be filled out, signed and submitted electronically.
- The deadline to complete and submit the BAA is December 31, 2017
- Service Providers must complete a BAA for each tax identification number, vendored with SG/PRC (on page 9 of the BAA indicate all the applicable vendor numbers under the tax id for the BAA being completed)
- Failure to complete the BAA with SG/PRC will result in termination of vendorization
- If you have any questions, please email us at commsrvs@sgprc.org.

Questions?