Health Insurance Portability and Accountability Act (HIPAA)

What Is HIPAA?

- The HIPAA *Privacy Rule* sets standards for how information can be accessed, used and disclosed at WRC and defines Clients' rights regarding their health information.

- The HIPAA ***Security Rule*** requires that WRC/ Vendor implement and maintain physical and electronic safeguards to protect the integrity of data and the confidentially of protected health information. Examples are door locks, email end to end encryption, key cards. Not taking client files out of WRC or vendor site.

The Lanterman Act and Confidentiality

Welfare and Institutions Code – WIC DIVISION 4.5. SERVICES FOR THE DEVELOPMENTALLY DISABLED [4500 - 4885]

Title 17 California Code of Regulation §4514. (For Regional Centers)

All information and records obtained in the course of providing intake, assessment, and services under Division 4.1 (commencing with Section 4400), Division 4.5 (commencing with Section 4500), Division 6 (commencing with Section 6000), or Division 7 (commencing with Section 7100) to persons with developmental disabilities shall be confidential. Information and records obtained in the course of providing similar services to either voluntary or involuntary recipients prior to 1969 shall also be confidential…

Terms - PHI

- Information that identifies a Client in any form, collected, created, maintained or received
- "Protected health information" - any individually identifiable patient information, which includes name, address, birthday, phone number, email, fax, SSN, UCI number, photograph, names of family members, or any number or code that can uniquely identify and individual
- Can be electronic, written or oral
- Including personal, financial and medical information
- That pertains to:
  - Past, present, or future physical or mental conditions
  - Past, present, or future treatment

PHI Individual Identifiers

- Names;
- Addresses – all geographic subdivisions smaller than state, including 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 publicly 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; and
- The initial three digits of a zip code for all such geographic units containing 20,000 or fewer is changed to 000.
- All elements (except year) for dates directly related to an individual (including birth date, admission date, discharge date, date of death
and all ages over 89);
- Telephone numbers;
- FAX numbers;
- Electronic mail (email) addresses

PHI Individual Identifiers

- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Online account username or email address, in combination with a password or security question and answer;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;

Web URL's;

- IP addresses;
- Biometric identifiers e.g., finger and voice prints, retinal scans, etc.;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (e.g., UCI)

WRC/ Vendor Responsibilities

- Obtain a signed consent whenever we seek to obtain ***or*** release PHI to someone outside our agency
- May not use or further disclose info other than as permitted by contract or consent
- Use appropriate safeguards to protect PHI
  - Administrative – e.g., assigned roles/access
  - Physical – e.g., locked rooms/filing cabinets
  - Technical – e.g., electronic encryption

WRC/ Vendor Responsibilities

- Report to DDS any unlawful use or disclosure of PHI as soon as we become aware of it – e.g., break-ins, stolen laptops and email or other Data Breaches
- Ensure that agents to/from whom we disclose/receive PHI follow the same rules we are required to follow
- Allow individuals to whom PHI refer access to their own PHI
- Allow individuals to amend PHI

WRC/ Vendor Responsibilities

- Allow individuals to receive an accounting of disclosures of PHI – so records of consents are very important
- Make records relating to PHI available to the CA Secretary of Health and Human Services
- Return or destroy all PHI upon termination of contract
- Authorize termination of contract if a violation occurs

Penalties

- HIPAA provides for civil and criminal fines for wrongful use and disclosure of PHI
- California Law has additional fines and penalties
- HIPAA requires that employers apply sanctions up to and including termination of employment for violations of privacy

Penalties

- When a person knowingly & in violation of HIPAA releases information:
  - Fines: Not more than $50,000
  - Imprisonment: Not more than 1 year
- When committed under false pretenses:
  - Fines: Not more than $100,000
  - Imprisonment: Not more than 5 years
- When committed with intent for gain:
  - Fines: Not more than $250,000
  - Imprisonment: Not more than 10 years

How Can I Protect PHI?

- Model best practice with providers, vendors/ others. Use encryption and remind them to also use encryption.
- Do not speak in the community or in public areas of the office about a specific Client by using his/her complete name
- Do not throw away any information containing Client identifiers including names, UCI or social security numbers or addresses; shred it!
- Do not take charts or electronic devices out of the office and leave them where someone can view the Clients name or any information

How Can I Protect PHI?

- Do not leave a voice mail that includes PHI on a message unless the Client has specifically authorized it
- Do not leave a fax or printed document that includes PHI in an unsecured area
- When you find unattended PHI, place it in a lost and found box or forward it to the HIPAA Compliance Officer

How Can I Protect PHI?

- Do not share your electronic login information with others or leave it in exposed areas
- Logout completely from your computer or electronic device whenever you are away from it

Minimum Necessary

- HIPAA requires that a release of PHI be limited to the ***minimum necessary*** to accomplish the request.
- For example, if you assist a parent to request a WRC psychological evaluation be sent to the school. ONLY the psychological evaluation will be sent (not other medical records, etc).

Access To Health Records

- A Client or their legal representative may request access to inspect and copy their PHI upon presentation of written request.
- Lanterman (4725) and Early Start (303.402) regulations also gives Clients the right to inspect, review and obtain an accurate copy of any records obtained in the course of providing services.
- Provider must allow inspection in a timely manner, but in no event more that five (5) working days after receiving written request.
- Provider must make photocopies available in a timely manner, and in any event must transmit copies within fifteen (15) calendar days after receiving written request.

Amendment of Health Records

- Clients may request an amendment of their records if they feel PHI is incorrect or incomplete by submitting written request.
- WRC does not have to agree to amend the record, but if we deny the request we will do so in writing
- WRC has sixty (60) calendar days after receipt to decide to accept or deny the amendment request.

Request for Restrictions

- Client may request restrictions on how WRC uses or discloses PHI.
- For example, an adult Client may request that information not be shared with a sibling.
- WRC does not have to agree with the request.
- WRC must document any restrictions to which it agrees.

Request for Confidential Communications

- A Client may request that WRC contact them in a certain way.
- WRC must accommodate any reasonable or lawful request.
- WRC may not require a Client to explain the reason for the request.
- For example, a Client may ask that they only be contacted at home and not at their workplace.

Vendors/ Providers

- WRC works with many Vendors/ Providers who provide direct services to Clients. Vendors/ Providers are also obligated to comply with HIPAA regulations.

- *Any* breaches of confidentiality that occur with Vendors/ Providers must be reported and will addressed by the HIPAA Privacy Officer. DDS has special reporting requirements if such a breach occurs

- Refer to Centers for Medicare & Medicaid Services for the regulations at: http://hhs.gov/ocr/hipaa/

Encryption

- Vendors/ Providers must use an End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data while it's transferred from one end system or device to another. In E2EE, the data is encrypted on the sender's system or device, and only the intended recipient can decrypt it.
- Vendors/ Providers must have a business associate agreement (BAA) in place with each of their partners to maintain PHI security and overall HIPAA compliance.

HIPAA Compliant Email Encryption Services

- Barracuda
- Egress
- Hushmail
- kIdentillect
- LUXSCI

HIPPA Compliant File Sharing Services

- Box
- Citrix ShareFile
- Microsoft OneDrive
- Google Workspace
- Kiteworks

Recommended Tools for Disk Encryptions

- Bitlocker (Windows)
- FileVault (mac OS)
- Sophos
- TrueCrypt