Guide for DSPD providers handling sensitive information

This information is for educational and informational purposes only and does not constitute legal advice. Providers should seek their own legal counsel in regards to Health Insurance Portability and Accountability Act (HIPAA) compliance.

The Division of Services for People with Disabilities (DSPD) became a HIPAA-covered entity in 2016. Following HIPAA standards requires organizations to protect people's sensitive health information. It also helps ensure privacy, prevent security risks, and avoid legal consequences. Adherence to HIPAA regulations is a requirement for those contracting with DSPD because they are a business associate of DSPD.

This guide offers information and practical application suggestions to help contracted providers ensure privacy and security of personal identifying information and/or protected health information (PHI) of people they serve.

Section 1: Privacy and security – a provider should develop and implement written policies and procedures that are consistent with federal and state law.

- Your day-to-day practices are important in helping to make sure you are compliant with DHHS/DSPD privacy and security policies. Suggestions include:
    - Be aware of the 18 elements of Protected Health Information (PHI) to fully understand what classifies as PHI.
    - Personally identifiable information may be "used" when known, shared, or analyzed within your day through electronic, written, and spoken form.
    - Arrange monitors away from public view and passersby.
    - Make sure workstations are not accessible by others. Lock the workstation when unattended.

Protected Health Information (PHI)

Is information, including demographic data that relates to:

- The person's past, present or future physical or mental health or condition,
- The provision of health care to the person, or
- The past, present, or future payment for the provision of health care to the person

Identifiable information:

45 CFR 164.514

Outlines the 18 identifiers that must be removed to de-identify data.

- Make sure you double check the email address of anyone you are sharing a document, spreadsheet, or slide show with.
    - Limit access to those who have a need to know.
    - Ask yourself, Is there another way to get this information out? Could I use USTEPS, MySTEPS, or UPI to notify the person?
    - Make sure no sensitive information is used in the subject line of an email, even if using a secure email service.
    - Always use a secure email setting when sending PHI / PII.
    - Double check the "To" and "CC" fields before you send or reply to an email containing PHI / PII.

Section 2: Administrative reporting

- All HIPAA incidents need to be reported to the current DSPD privacy officer through this email address dspddocuments@utah.gov.
- The impact of a breach can be devastating, expensive to repair, and can lose the trust of those whose information you are supposed to protect.
- See something, say something, do something. Create a culture that is open to discussing problems and getting them fixed.
- If you receive an email with PHI / PII that was not intended for you, with PHI / PII information in the subject line, or not sent via secure email, inform the original sender and advise them of a HIPAA incident.

Section 3: Practical applications. The following are suggested applications:

- Support coordinators need to provide a copy of DSPD's NPP to each person they serve.
- Always verify the fax number or email address when sharing PHI / PII.

Helping HIPAA covered entities implement privacy and security protections:

HIPAA regulations are designed to be adaptable so organizations of all types and sizes can be compliant. Because of this, there is no one-size-fits-all training program. Each organization must customize its training approach. This guide outlines DSPD's expectations.

Notice of privacy practices | DSPD (NPP)

- All HIPAA-covered entities are required to have a notice of privacy practices set for their company. The link above is the one for DSPD.
- The Notice of Privacy Practices outlines how a covered entity may use and disclose protected health information (PHI), and it also details a person's rights in regards to their health information.
- The document is presented at the time of intake.
- A notice should be posted in all buildings and treatment areas, as well as on the DSPD website.

- Do not leave any documents around that contain PHI / PII. If you print something while working in an office or shared space, don't let it sit. Take precautions to protect sensitive data from being exposed. Don't leave it unattended.
- When charting, use only factual terms, not opinions or judgments. Always follow documentation guidelines.
- You have no right or ownership to confidential information, even if you created it.
- All documents being uploaded into USTEPS / UPI should be for one consumer at a time. Each document should be clear, readable, and a good representation of the original document.
- Securing all information when leaving your work area. Security is something everyone needs to be aware of.

Applicable regulatory references

- Summary of the HIPAA Privacy Rule | HHS.gov
- HIPAA Guidance Materials
- HIPAA Training and Resources | HHS.gov
- eCFR :: 45 CFR 164.520 -- Notice of privacy practices for protected health information.
- eCFR :: 45 CFR 164.514 -- Other requirements relating to uses and disclosures of protected health information.
- HIPAA Related Links
- Summary of the HIPAA Security Rule
- Security Rule Guidance Material
- HIPAA Breach Notification Rule
- HIPAA Enforcement

Expectations:

- Take privacy and security seriously and make sure PHI is not disclosed in any way.

If an incident happens:

- Don't panic. We know accidents happen, so report incidents per contract requirements, and learn from past mistakes.
- Contact the DSPD privacy officer as soon as possible.
    - Be available and prepared to provide all of the details and documentation of the disclosure.
    - Participate to the extent needed in the resolution of the incident.

Additional information:

For more information or questions, please reach out directly to the DSPD Privacy & Security team at dspddocuments@utah.gov.