FAQs for Victim Service Programs About HIPAA Privacy, HIPAA Security, & Technology

Victim service providers need technology that provides appropriate privacy protections to help them comply with VAWA, VOCA, and FVPSA confidentiality obligations. Use of the term "HIPAA-Compliant" by technology vendors sometimes causes confusion. The purpose of this handout is to clarify what HIPAA is, what it is *not*, and what a vendor saying "HIPAA-compliant" might mean.

SUMMARY:

There are two distinct and primary rules related to HIPAA: the HIPAA Privacy Rule and the HIPPA Security Rule. (See FAQs for full descriptions of each.)

HIPAA Privacy Rule:

- HIPAA Privacy standards are looser and more permissive than VAWA, VOCA, and FVPSA confidentiality rules. See this chart for a comparison.
- Information sharing that is permissible under the HIPAA Privacy Rule may be prohibited under VAWA, VOCA, FVPSA, or local law.
    - Some programs face pressure from medical facilities and other community partners that claim HIPAA mandates they share information. It's important to clarify - HIPAA never mandates sharing information.
- In general terms, the HIPAA Privacy Rule permits doctors, insurance companies, businesses, and patients to decide when patient health information should be shared.
    - VAWA, VOCA, and FVPSA confidentiality dictate that only violence survivors (not victim service providers) can decide when personally identifying information should be shared.
    - Both HIPAA & VAWA/VOCA/FVPSA recognize an exception when local law explicitly requires a provider to share information for a specific reason.

HIPAA Security Rule:

- HIPAA Security standards offer a roadmap for how healthcare providers and software developers can build & maintain secure electronic information storage and sharing systems.

- When software companies market their products as "HIPAA Compliant", they are referring to HIPAA Security standards. There is no formal certification for "HIPAA-Compliant" products. Rather, it is a popular marketing term used by technology vendors that have determined through self-assessment that the product meets HIPAA Security.

HIPAA & Victim Service Programs:

- If you are NOT covered by HIPAA, the Privacy and Security Rules will not be enforced by the federal government, regardless of whether you signed contracts using the words "business associate" or "HIPAA."

FREQUENTLY ASKED QUESTIONS

What is HIPAA?

- The Health Insurance Portability and Accountability Act (HIPAA) is a federal statute that governs the portability of health insurance and facilitates sharing of patient records between doctors, businesses, insurance companies, and public health agencies.
- HIPAA has two major rules that "covered entities" must follow:
    - HIPAA Privacy Rule
    - HIPAA Security Rule

What is the HIPAA Privacy Rule?

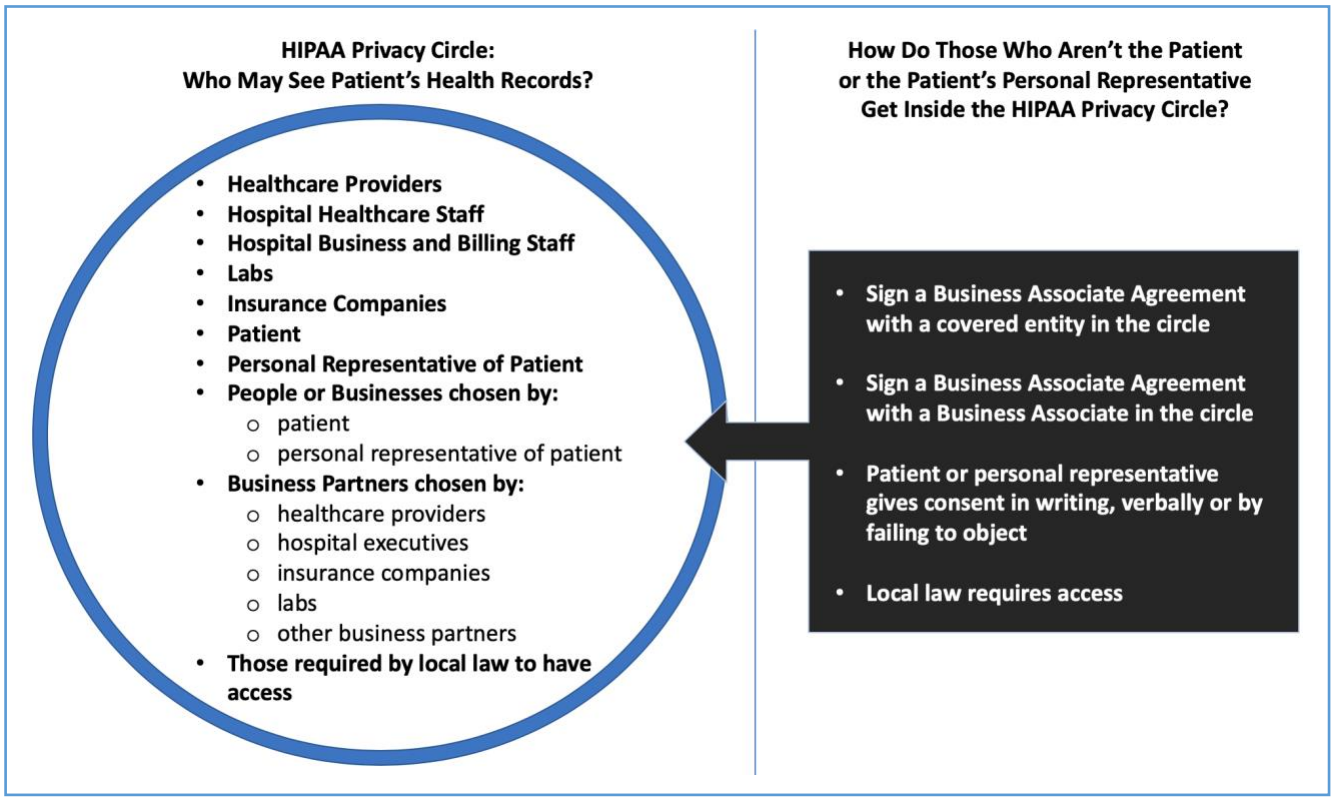
- The HIPAA Privacy Rule explains who is ***permitted*** to see personal health information.
- There are two broad categories of ***permissible*** (not mandated) sharing of information:
    - Sharing to help the business of healthcare work, and
    - Sharing to fulfill the patient's wishes.
- There are exceptions that ***permit*** (but don't mandate) doctors to share patient health information for public health, public safety, and some law enforcement purposes (regardless of whether the patient agrees).
- The HIPAA Privacy Rule allows doctors, health care offices, hospitals, health insurance companies, and health care clearinghouses to exchange patient information without checking with the patient first.

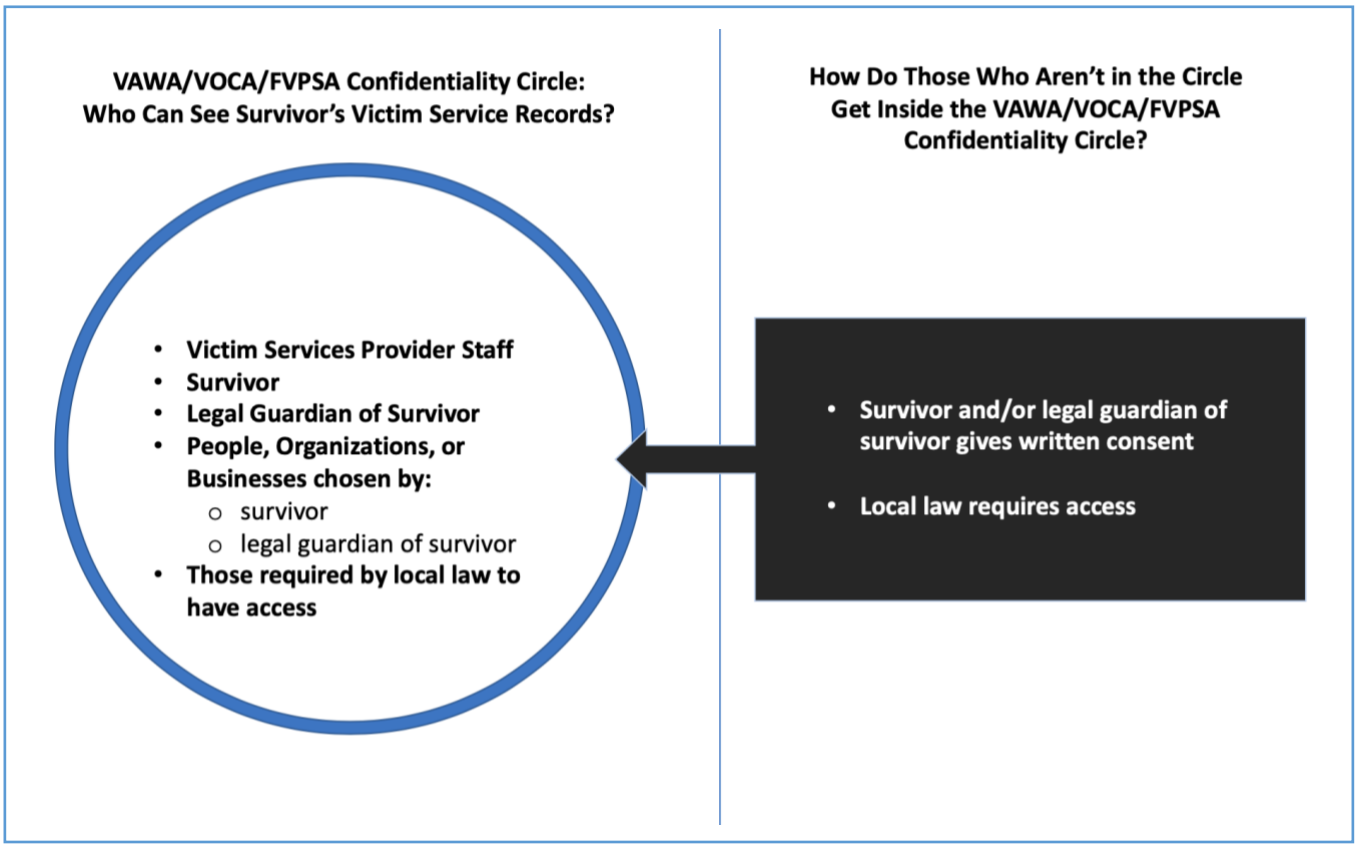
- The Privacy Rule also allows those entities to contract with "business associates" and share necessary patient information with them without checking with the patient first.
    - And those business associates can subsequently contract with *other* business associates of their choosing without checking with the patient first.

- Visit the HHS.gov website for more information about the HIPAA Privacy Rule.

What are the general differences between HIPAA Privacy and VAWA / VOCA / FVPSA Confidentiality?

The graphics below show the broad differences between HIPAA and VAWA/VOCA/FVPSA information rules. For questions about whether specific incidents of sharing would be authorized or prohibited, consult the relevant law directly and reach out for technical assistance or legal advice as needed.





What is the HIPAA Security Rule?

- The Security Rule specifically protects electronic Protected Health Information ("e-PHI") held by covered entities and their business associates.
- The HIPAA Security Rule offers a flexible set of technology and workplace standards that help covered entities and their business associates protect e-PHI from being misused, disclosed without authorization, lost, destroyed, or inappropriately changed.
- Technology vendors that want to sell services to healthcare providers look at the standards in the Security Rule when designing their technology products.
- See the HHS website for more detailed information about the HIPAA Security Rule.

Who is required to follow the HIPAA Privacy & Security Rules?

- Only covered entities and business associates of covered entities are required to follow the HIPAA Privacy & Security Rules.
- Generally, covered entities are:
    1. Healthcare providers that electronically transmit protected health information for purposes related to payment for services;

2. Health insurance companies; and
3. Healthcare clearinghouses.

If unsure see HHS website for more detailed information.

Do HIPAA Privacy & Security Rules apply to victim service providers?

- Usually not. Agencies that offer free mental health care and/or forensic medical exams are typically not considered covered entities (even though they provide "health care").
    - Occasionally, victim service providers are part of health care providers or have become a formal business associate of a covered entity, so HIPAA rules may apply to the Protected Health Information (PHI) that they hold.
    - However, if those victim service providers also receive VAWA, VOCA, or FVPSA funding, they must follow the stricter privacy standard of VAWA, VOCA, and FVPSA.
        - If the information sharing is prohibited by VAWA, VOCA, or FVPSA, the victim service provider cannot share it, even if HIPAA would permit it.
        - A victim service provider will likely hold sensitive, confidential information about survivors that may not be included in the definition of Protected Health Information.
- If an organization is neither a covered entity nor a formal business associate of a covered entity, then the HIPAA rules do not apply and HIPAA rule enforcement is not available through federal agencies.

What are "covered entities" and how do I know if my agency is one?

- HIPAA covered entities include health care providers that engage in electronic transactions (like billing), health insurance plans, and health care clearinghouses.
- The Center for Medicare and Medicaid Services has created a Covered Entity Guidance Tool that organizations can use to help determine if they are considered a covered entity.
    - Is it not a good practice to assume an agency is a covered entity.

- If an agency "voluntarily" follows HIPAA rules, there will not be any enforcement of the rules by the federal government.

Who is a "business associate"?

- Generally, a business associate is a person or organization hired to help a covered entity manage its healthcare business, **and** needs access to protected health information to provide such help.
- A business associate can hire their own business associates and share protected health information with them as needed.
    - In order to have access to protected health information, the business associate must sign a "business associate agreement" (see next question for more details) and agree to have HIPAA Privacy and Security Rules enforced against them by the US Dept of Health and Human Services.

What is a "business associate agreement" under HIPAA?

- A HIPAA business associate agreement:
    1) Describes the ways the business associate is allowed to use the PHI it gets from a covered entity, and
    2) Contains agreements to protect against other uses or disclosures.
- Upon signing a HIPAA business associate agreement, the business associate must follow HIPAA Privacy and Security Rules (with some exceptions).
    - The US Department of Health and Human Services will enforce the rules against the business associate that signed the agreement.

What if a victim service provider that isn't a covered entity enters into a business associate agreement with a technology vendor?

- The US Department of Health and Human Services will <u>not</u> enforce HIPAA Privacy and Security Rules against either the victim service provider or the technology vendor.
- The terms of the contract can be enforced in traditional ways, such as suing a technology vendor that violates the contract.
    - Many technology vendors write contracts that severely limit the amount of damages for which the vendor can be sued.

- Merely using the terms “business associate”, “covered entity”, “HIPAA”, or “Protected Health Information” in a contract will not make the contract covered by HIPAA rules.

What does “HIPAA-compliant” mean?

- Only the vendor using the term knows what it means when they say it.
- There is no formal process for proving or certifying that certain technology and systems are “HIPAA-compliant”.
- If a vendor uses this term, victim service providers should follow-up by asking:
    - “What do you mean by HIPAA-compliant?”
    - “What security features do you offer that protect confidential information?”
    - “Who in your company would be able to access the information we enter into your system?”
    - “Here is information about the laws governing our work. The privacy standards in VAWA, VOCA, and FVPSA do not have an exception for sharing with business associates. How does your system meet these higher standards?”

Can victim service providers use “HIPAA-compliant” technology?

- A technology product that follows HIPAA Security Rule standards *might* be a good option for a victim service provider.
    - But the product must also meet the higher privacy and confidentiality standards of VAWA, VOCA, and FVPSA.
- There are two differences between HIPAA and VAWA/VOCA/FVPSA that might make technology built to be “HIPAA-compliant” a poor fit for victim service providers:
    1) HIPAA allows for greater information sharing without seeking permission from the person who the information belongs to.
    2) Under HIPAA, losing or destroying information is just as bad as having information stolen or misused. However, at appropriate times, victim service providers may genuinely need to destroy information as part of survivor-centered services.

- If the technology provider mishandles survivor information provided by a victim service provider that is not a HIPAA covered entity, the US Department of Health and Human Services will not investigate or punish the technology provider for the mishandling.

PRACTICAL EXAMPLE OF HIPAA-AUTHORIZED INFORMATION SHARING:
I break my leg and go to the local hospital's emergency room. The doctor works for her own practice. The radiologist works for a different practice. HIPAA Privacy Rule authorizes all of the following sharing of information *without notifying me or asking my permission*:

- The local hospital's staff, the doctor, and the radiologist share my health and insurance information.
- They also all share my health information with my medical insurance company.
- All of my health information is stored in a database called Digital Records Deluxe ("DRD"). DRD is a business associate of the hospital and their authorized employees can read my health records as part of providing tech support to the hospital.
- DRD contracts with Giant Server Farm ("GSF") to store my electronic health records in GSF's servers. GSF is a business associate of DRD, and their authorized employees can have access to my health records as needed to run the servers.
- I have a $1,000 bill from my broken leg, but I can't afford to pay it, so it goes to collection at the hospital's billing department. The hospital has a debt collection attorney who is a business associate, and gives the attorney my health information.
- After a year, I still can't pay my bill. The hospital decides to sell my bill to a debt buyer. The debt buyer becomes a business associate who can also see my health records.
    - But, if my lawyer calls the hospital to get my health records, the hospital will not share them unless they get a specific consent from me to share the information.

CONCLUSION:

- The HIPPA Privacy Rule takes a very different approach to professionals sharing personal information than VAWA, VOCA, and FVPSA's approach.
- The HIPAA Security Rule is a set of standards for protecting electronically stored information.
- HIPAA requirements and enforcement protections only apply to organizations that are actually covered by HIPAA, and it is unusual for a victim service provider to be a HIPAA "covered entity".
- Victim service providers should independently assess whether a technology product or an information-sharing practice meets the confidentiality standards of VAWA/VOCA/FVPSA and local laws, even if the product or practice is labelled as "HIPAA-compliant".

Thank you to our grant partner Alicia Aiken, JD, from Danu Center's Confidentiality Institute, for her extensive contributions to the creation of this resource.

Supported by US DOJ-OVW Grant #2019-TA-AX-K003. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.