

Organizations that meet the definition of a covered entity under HIPAA must comply with HIPAA requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

First Question: Is your PHO a covered entity?

There are three criteria needed for an entity to be covered under HIPAA. You must:

- Be a health care provider (if you offer medical services and have a medical director, you likely are);
- Engage in a covered transaction (you bill insurance or Medicaid) and
- You send information electronically (true FAX is not considered electronic transmission).

Most Pregnancy Medical Centers do not bill for services and are not likely Covered Entities.

If you are not a covered entity, you may not be able to offer the federal protections HIPAA grants your patients, so you should consider removing references to HIPAA from your materials.

Check your state laws!

Some states have laws similar to HIPAA, some have other health information laws that apply, and some states have no additional laws.

HIPAA is a federal law. It includes rules and regulations, but it also extends rights to patients of covered entities. A state can mimic HIPAA's rules and requirements, but the state can not grant federal rights to the patient of an organization that is not a covered entity under federal law. Find and follow your state law, understanding that the presence of a state law does not require an organization to comply with HIPAA federal law.

Check Terms of your Partners!

Grants and State Funding Agreements can also impose requirements, some similar to HIPAA. It is best to have a local attorney review agreements with these organizations.

BAAs may not be required if your center is not a covered entity.

Even if you are a HIPAA Covered Entity, you probably won't need a Business Associate Agreement to make referrals to other providers. "The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. See [45 CFR 164.502\(e\)\(1\)](#). Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract."*

Confidentiality is always required

Although most PHOs aren't HIPAA Covered Entities, as a matter of good practice, every PHO should have a Confidentiality Policy that includes the following:

1. Employees should be bound by an Employee Confidentiality Agreement that requires that Confidential Information should be shared on a need-to-know basis only.
2. Automatic lock screens should be on computers, paper records maintained in locked cabinets in a locked office/storage room, separate from the waiting rooms or consulting rooms.
3. A Client Confidentiality Statement that applies to all clients, regardless of the services they are receiving, that outlines the safeguards the PHO agrees to follow should be given to each client, regardless of the services they receive. It is wise to have the client acknowledge receipt of this statement. Exceptions to confidentiality that are required by your state's laws or your center's policies should be disclosed to the patient.
4. The requirements of state laws, grants and state funding agreements should be incorporated into the internal policies and the Confidentiality Statement referenced in #3 above. Remember that how well you conform to your written policies and procedures is often a way that external authorities will judge your organization.
5. Review the [Commitment of Care and Competence](#) often. Your policies should align with it.

