Who must comply?

Organizations providing healthcare services or certain administrative services must uphold an individual's right to privacy. This means adhering to requirements set forth by the Centers for Medicare & Medicaid Services (CMS), HIPAA and the HITECH Act, the Gramm-Leach-Bliley Act, the IPA, and the IPA's affiliated health plans.

Under HIPAA, health plans, health care clearinghouses, and health care providers are considered **covered entities**.

Subcontractors that perform activities involving the use or disclosure of protected health information (PHI) are considered **business associates**. These activities include creating, receiving, maintaining, transmitting, processing, accessing, or storing PHI.

A covered entity may be a business associate of another covered entity.

Workforce members are employees, volunteers, trainees, and any other persons under the direct control of a covered entity or business associate, regardless of payment.

Your Responsibilities

As a business associate, the IPA is responsible to fulfill the terms and conditions in our contracts with covered entities, and to meet regulatory requirements for patient privacy and information security. As a subcontractor to the IPA, you are responsible to adhere to these requirements as well. This includes:

- Upholding the Business Associate Agreement (BAA) provisions set forth by the IPA,
- Ensuring your subcontractors also uphold these privacy and security standards.

You must keep evidence of your compliance with these requirements for at least 6 years. This may include employee training records, policies, risk assessments, documentation of privacy/security incidents, or proof of the way you oversee your subcontractors. You may be asked to complete an attestation or audit to verify your adherence to these requirements.

If you or your subcontractors fail to meet privacy and security requirements, it may lead to retraining, corrective actions, or other sanctions. If you discover a privacy or security issue, you must take quick action to fix and report the issue. And, you need to prevent it from happening again.

Privacy/Security Requirements

Offshore Operations

Offshore operations refers to operations conducted outside of the United States or United States Territories. An offshore subcontractor provides services performed by workers located offshore. This includes:

- American-owned companies with operations performed outside of the United States
- Foreign-owned companies with operations performed outside of the United States

If any of your employees or subcontractors perform work offshore, and that offshore work includes receiving, processing, transferring, handling, storing, or accessing PHI on the IPA's behalf, you must notify Physicians DataTrust at compliance@pdtrust.com, or by phone at (562) 860-8771, ext. 114.

Physicians DataTrust may be required to report these operations to the IPA's affiliated health plans. And, Physicians DataTrust may require your organization to develop additional controls to ensure PHI is protected in the course of offshore business.

More information about offshore operations is available at https://pdtrust.com/compliance.

Privacy & Security Training

As a subcontractor to the IPA, your organization must maintain policies and procedures to uphold privacy and security requirements. And, you must train your workforce and business associate subcontractors on these policies and procedures, as necessary and appropriate for them to carry out their assigned duties in compliance with privacy and security requirements.

The policies, procedures, and training materials must include the requirement and the method(s) for workforce members and business associates to report privacy and security concerns. And, your policies and procedures must include a provision to report privacy and security concerns (that impact the IPA) to Physicians DataTrust without delay.

You must conduct this training prior to granting access to PHI, annually thereafter, and when there are changes to privacy and security policies. You must also save proof that you conducted the training. If you use training logs, reports, or sign-in sheets as evidence of completion, they must include names, dates, and training topics.

PDT Privacy/Security Training is available at https://pdtrust.com/compliance. You are not required to use these materials.

Subcontractor Oversight

As a subcontractor to the IPA, you must monitor the compliance of your business associate subcontractors. If you choose to subcontract with other parties for IPA business, you must make sure they abide by all requirements that apply to you as a subcontractor of the IPA. This includes ensuring:

- A written service agreement and BAA are in place prior to involvement with IPA business
- The business associate subcontractor complies with the requirements described in this guide
- The business associate subcontractor complies with all applicable privacy and security standards

PDT's BAA template is available at https://pdtrust.com/compliance. You are not required to use this BAA template.

Not every subcontractor is a business associate. Only subcontractors that create, receive, maintain, transmit, process, store, or access PHI are considered business associates. The following types of subcontractors are not business associates:

- Housekeeping/custodial
- Grounds and maintenance
- Machine repair or servicing

For help identifying which of your subcontractors are business associates, please contact Physicians DataTrust at compliance@pdtrust.com, or by phone at (562) 860-8771, ext. 114.