HIPAA Best Practices Guide

This HIPAA Best Practices Guide is a Q&A for developing an effective compliance program for implementing privacy policies. It is intended to be a resource for those who are developing their compliance program and privacy policies but should not be the only resource used in the process.

This guide provides educational information on federal laws and regulations. This guide does not provide legal advice. Please consult with your own attorney on federal and state laws applicable to your situation.

The Health Insurance Portability and Accountability Act of 1996 (HIPPA), its Administrative Simplification Regulations (HIPPA Regulations), the Health Information Technology for Economic and Clinical Health Act (HITECH), Chapter 8 of the United States Sentencing Commission's Guidelines (U.S. Sentencing Guidelines), and the U.S. Department of Justice's Evaluation of Corporate Compliance Programs provide a framework for best practices.

Topics Page

Is your organization subject to HIPAA and its regulations?

HIPAA's privacy and security regulations only apply to covered entities and their business associates. Your first step is to determine whether your organization is a covered entity or business associate.

The regulations apply directly to three types of health entities, called "covered entities":

- Health plans
- Health care providers
- Health care clearinghouses

If your organization is one of the entities above, then it would be a covered entity subject to HIPAA's regulations.

If your organization is not one of the entities above, then your organization may still be subject to HIPAA's regulations if your organization is a business associate of a covered entity.

Your organization is a business associate if it creates, receives, maintains, or transmits protected health information for payment, health care operations, or activities (governed by the privacy regulations) of a covered entity.

If your organization has executed a business associate agreement with a covered entity, then it's likely that your organization is a business associate and subject to HIPAA's regulations.

Does your organization handle protected health information?

Protected health information (PHI) is individually identifiable information, including demographic and genetic information, related to the past, present, or future physical or mental health or condition, provision of health care to an individual, or the past, present, or future payment of health care which is created or received by a covered entity.

PHI does not include certain records covered under the Family Educational Rights and Privacy Act of 1974 (FERPA) and does not include employment records maintained by a covered entity in its capacity as an employer.

This means that if your organization is a covered entity or business associate that handles PHI, then your organization is subject to HIPAA's regulations.

Does your organization need a business associate agreement?

If your organization is a covered entity that has a business associate, then your organization must have a contract called a business associate agreement (BAA) with the business associate. The BAA limits the business associate's uses and disclosures of PHI to those workforce members permitted by the contract. The BAA also imposes security, inspection, and reporting requirements.

Under HITECH, a business associate must enter into a BAA with each of its subcontractor business associates who create, receive, maintain, or transmit PHI on behalf of the business associate. The BAA must meet all of

HIPAA's privacy and security requirements and must be at least as stringent as the BAA that the business associate has with its covered entity.

Among the BAA's required terms, the covered entity must have the authority to terminate the services contract and BAA if it determines that the business associate violated a material term of the BAA.

Also, a business associate must take reasonable steps to stop violations if the business associate knows that its subcontractor is violating its obligations under the BAA or has a pattern of activity that is a material breach of the BAA. If the business associate is unsuccessful in stopping the violations, then the business associate must terminate the contract, if possible.

For which HIPAA violations can a business associate be directly liable?

Business associates are directly liable for the following HIPAA violations:

1. Failure to provide the U.S. Department of Health and Human Services' Secretary (Secretary) with records and compliance reports, failure to cooperate with complaint investigations and compliance reviews, and failure permit access by the Secretary to information, including PHI, pertinent to determining compliance.
2. Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under HIPAA's regulations.
3. Failure to comply with the requirements of HIPAA's security regulations.
4. Failure to provide breach notification to a covered entity or another business associate.
5. Impermissible uses and disclosures of PHI.
6. Failure to disclose a copy of electronic PHI (ePHI) to either the covered entity, the individual, or the individual's designee (as specified in the business associate agreement) to satisfy a covered entity's obligations.
7. Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
8. Failure, in certain circumstances, to provide an accounting of disclosures.
9. Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for those business associate agreements.
10. Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.

What should your organization have in place for an effective compliance program?

The U.S. Sentencing Guidelines and the Office of Inspector General's Guideline Manual provide the elements of an effective compliance program:

1. Develop policies and procedures.
2. Assign oversight for compliance, including designating a compliance officer.
3. Conduct training and education.
4. Develop open lines of communication.
5. Conduct internal monitoring and auditing.
6. Respond promptly to detected offenses and take corrective action.
7. Enforce standards through well-publicized disciplinary guidelines.
8. Conduct periodic risk assessments.

What are some tips for drafting a written privacy policy?

If your organization needs to draft a privacy policy or is reviewing its current policy, it's helpful to involve your attorney in the process. HIPAA and its regulations can be complex so legal counsel can help determine which regulations apply to your organization so that the policy accurately reflects your business practices.

At the same time, it's critical to get buy-in from senior management and from workforce members who use PHI in their work. Forming a committee that consists of key stakeholders can be helpful to the success of drafting or revising a privacy policy. Your committee members can also provide feedback on the privacy policy training methods that may be most effective for your organization.

Keep in mind that there are multiple audiences for your written privacy policy. Your internal audiences will include your employees and Board of Directors (Board). Your external audiences may include business associates, shareholders, vendors, accrediting agencies, and members of the regulatory and legal community.

This means that the policies will serve several purposes. The policies will reflect the organization's character upon its Board and senior management. Managers will need to operate under the policies with the understanding that they are accountable for complying with and enforcing the policies throughout the organization. Employees will also be accountable for complying with the policies. Even if the policies are not explicitly incorporated into employees' terms of employment, the policies' enforcement, including employee discipline, will play a role in employment actions.

Further, the policies serve broader purposes to external audiences. The policies provide the business community with an indication of your organization's good corporate citizenship and a standard by which to judge your organization's actions. The policies also provide a framework for your organization's agents who agree to abide by the policies and who understand that a breach of the policies could lead to agency relationship termination.

The final audience for your policies is the government. For example, if there is a breach that triggers the breach notification process, then several regulatory agencies (for example, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR), the state Attorneys General, or accrediting agencies) and the court system may become involved.

In the past, having a written policy was a mitigating factor when regulatory agencies investigated and settled a breach. However, because of extensive education by the government about privacy compliance since HITECH was enacted in 2009, regulatory agencies now expect covered entities and business associates to have policies in place. This means that having a written policy is no longer a mitigating factor when negotiating a resolution agreement with the government.

While having a privacy policy is essentially expected by the government, having no policy is better than having one that your employees don't follow. This means that when your organization adopts a policy, your organization must provide annual training for its employees and business associates, training within a reasonable amount of time after new employees start work with your organization, specific training for employees who handle PHI on a routine basis, and retraining for employees who your organization identifies as needing additional education.

Think of the written privacy policy as a work in progress. As your employees and their duties change, your organization will need to update the policy to reflect those duties that are within the minimum necessary standard for your employees' job duties. Also, as your business grows, you may need to address those lines of business. Finally, as privacy laws and regulatory agencies' enforcement criteria change, your organization will need to amend its policy to reflect the changes.

What is the difference between a policy and a procedure?

In the context of privacy compliance programs, a policy is a written document that is developed by the organization's privacy officer and approved by the organization's Board. It is the framework by which the employees and business associates handle PHI.

Procedures are the daily checklists or how-to manuals that project teams develop to train their staff and ensure that all team members handle PHI consistently, within the organization's adopted privacy policy and within any applicable business associate agreement.

Team members modify procedures as needed to help with their work. Procedures are not usually reviewed or formally approved by an organization's Board. Even though procedures do not go through formal Board approval, all procedures must be consistent with the organization's privacy policy.

How should your organization communicate the policy?

Your organization should provide the policy to *all* employees (regardless of their role in your organization) so that the policy is in immediate reach. If your organization maintains a website that is regularly used by employees as part of their jobs, then posting the policy on your website may be a cost-effective way of making the policy immediately accessible and easily updated.

In addition to training employees on the policy, your organization should document its compliance efforts. After your employees have an opportunity to read and ask questions about the policy, your organization should require each person to sign an acknowledgement that they read the policy, received training on the policy, and abides by the policy.

What should the privacy officer's role be within the organization?

If your organization is a covered entity, then it must designate a privacy officer who is responsible for developing and implementing your organization's privacy policies and procedures.

The privacy officer may report to the organization's Chief Compliance Officer (CCO) if the organization has a CCO. The CCO, or privacy officer (if the organization does not have a CCO), should report to – or at least have a dotted line to – the organization's Chief Executive Officer (CEO) and the Board.

The privacy officer and CCO should have independence from the organization's legal, financial, and business departments. The government has indicated that, to avoid conflicts of interest, the CCO role should be separate from legal counsel's role.

Legal counsel's role is to defend the best interests of the company. A Chief Compliance Officer's role or privacy officer's role is different.

The CCO's and compliance department's role is to advise senior management and Board of how to best comply with the laws, monitor activities, investigate complaints and potential breaches, communicate with the U.S. Department of Health and Human Services (HHS) when breach reporting is triggered, and provide recommendations on implementing compliance policies and training.

The compliance staff prevents problems from occurring and helps mitigate damage if problems occur. In the toughest situations, the CCO may be your organization's one senior officer who enforces policy and takes all necessary steps to prevent the organization from violating the law.

What reporting system should your organization have?

Your organization has discretion to determine the best reporting system for its culture and needs. Systems vary; an organization may offer a hotline, email, drop-box or post office box, a monitor, or a combination of these options.

When your organization decides on a reporting system and implements it, your organization should develop policies regarding confidentiality and anonymity, non-retaliation, investigation process, and publicizing the reporting system.

As a best practice, your organization's employees and agents should have a way to make anonymous reports.

In publicizing the reporting system, your organization should make it clear that callers' identities may be revealed during the investigation process. Some organizations develop a confidentiality policy summary, with assistance of legal counsel, that hotline staff read at the start of a call to explain the organization's confidentiality policy and its limits.

Compliance department staff must document hotline calls, their investigation, and follow-up actions. Further, compliance department staff should secure hotline records. Electronic files should be password protected and paper records should be locked and accessible to only compliance department staff who receive reporting confidentiality training. Hotline staff should only receive calls when and where their calls cannot be overheard.

One of the most important aspects of the reporting system is your organization's non-retaliation policy. Your organization should explain its non-retaliation policy within its written privacy policy to assure employees that your organization, including management, will not take any adverse employment actions against an employee who makes a good faith report to the compliance department.

When publicizing a reporting system, an initial letter or email from your organization's CEO announcing the reporting system can meet several goals. The letter or email can demonstrate your CEO's commitment to the compliance program, encourage employees to report, set the expectation that employees must report violations, and reassure employees of your organization's non-retaliation policy.

What is the difference between monitoring and auditing?

The U.S. Sentencing Guidelines state that an organization shall take reasonable steps "to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct."

Monitoring and auditing are methods that an organization should use to identify real or potential issues before they become larger compliance risks. As a best practice, an organization should regularly monitor and audit its activities.

Monitoring is generally defined as contemporaneous review of activities either by self-review within the department or outside the department by the compliance department or another part of the organization. In contrast, auditing is a formal review of activities that is independent of the activity that is being audited.

Your organization's review process should include sample selection, data review, data collection, data analysis, and reporting. The review process can involve many techniques, including on-site visits, testing of staff knowledge, mock audits and investigations, staff interviews, questionnaires, and document review. After a baseline review, compliance department staff should analyze its data to develop regular or trend reports for your organization's Board.

As a best practice, your organization should perform an annual audit of its compliance risk areas. The auditing team should be different than the individuals who perform ongoing monitoring reviews. It can be valuable to select an auditor from an outside firm that is independent from your organization and that has subject matter expertise in each area being audited.

While the audit format will be similar to most compliance reviews (sample selection, data review, data collection, data analysis, reporting, follow-up), the audit methodology must be structured and consistent so that valid comparisons can be made between audits.

The auditor should present its reports to the CEO and Board on a regular basis, or at least annually. The report should include the CCO's recommendations for corrective actions to address weaknesses identified by the audit. The organization, specifically its management, should be prepared to act promptly on any unfavorable audit findings to mitigate the organization's potential liability for criminal and civil penalties.

How should policy enforcement and discipline be handled?

Your organization should have a written policy that describes the procedures for handling disciplinary problems, including how investigations will be handled and who will be responsible for taking appropriate action.

Your organization must advise employees of the disciplinary policy, including potential sanctions, and that sanctions will be enforced. The sanctions should include progressive discipline that your organization will impose on its officers, managers, and other employees for policy non-compliance.

The U.S. Sentencing Guidelines do not provide specific sanctions for violations. However, per Office of Inspector General (OIG) guidance, sanctions can include oral warnings, suspension, termination, or financial penalties, as appropriate.

Further, the OIG advises organizations to "make the promotion of and adherence to compliance an element in evaluating the performance of managers, supervisors and other employees" and to "inform all supervised personnel that strict compliance with these policies and procedures is a condition of employment, and . . . take disciplinary action up to and including termination."

This means that your organization should not only follow through with its disciplinary policy, but it should take all direct discipline into account when evaluating an employee for a promotion or pay raise.

Your organization should also apply sanctions against managers and supervisors who fail to investigate a problem. This accountability is expressed by the OIG when it states that a compliance plan should include a "policy that managers and supervisors may be sanctioned for failure to adequately instruct subordinates or for failing to detect non-compliance with applicable policies and legal requirements, where reasonable due diligence on the part of the manager or supervisor would have led to the discovery of any problems or violations."

Further, in OIG's self-disclosure protocol, an organization that self-reports violations to the government must also identify the corporate officers, employees, or agents who should have known of, but failed to detect, the incident or practice based on their job responsibilities. If your organization self-reports, then it should be prepared to explain what sanctions it imposed on management for failing to detect or adequately address the violation.

Your organization should consult with its attorney and Human Resources department when developing a disciplinary policy to ensure that it reflects federal and state employment laws. Further, the policy should explicitly reflect any applicable whistleblower laws.

In addition to documenting the disciplinary procedures, range of sanctions, and factors used when applying sanctions, your organization should document the protocols that it will use during investigations. The OIG

recommends that organizations document the alleged violation, the investigative process, copies of interview notes and documents, log of witnesses interviewed and documents reviewed, and the investigation results when conducting an investigation.

What is your organization's potential liability, including your Board's liability?

Potential liability can include court injunctions, reputational harm, criminal penalties (up to $250,000, or imprisonment for up to 10 years, or both), and civil monetary penalties (described below).

Civil Monetary Penalties (for civil penalties assessed on or after March 17, 2022)

Tier	Penalty
1. Did Not Know: Covered entity or business associate did not know (and by exercising reasonable diligence would not have known) that it violated the provision of the Administrative Simplification regulations. "Reasonable diligence" means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.	$127 - $63,973 for each violation, up to a maximum of $1,919,173 for identical provisions during a calendar year.
2. Reasonable Cause: The violation was due to reasonable cause and not to willful neglect. "Reasonable cause" means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated a provision of the Administrative Simplification regulations, but in which the covered entity or business associate did not act with willful neglect.	$1,280 - $63,973 for each violation, up to a maximum of $1,919,173 for identical provisions during a calendar year.
3. Willful Neglect – Corrected: The violation was due to willful neglect, but the violation is corrected during the 30-day period beginning on the first date the liable person knew (or by exercising reasonable diligence would have known) of the failure to comply. "Willful neglect" means conscious, intentional failure or reckless indifference to the obligation to comply with a provision violated.	$12,794 - $63,973 for each violation, up to a maximum of $1,919,173 for identical provisions during a calendar year.
4. Willful Neglect – Not Corrected: The violation was due to willful neglect and the violation is not corrected as described in Tier 3.	$63,973 minimum for each violation, up to a maximum of $1,919,173 for identical provisions during a calendar year.

Criminal Penalties: The maximum criminal penalty for a HIPAA violation by an individual is $250,000. Restitution may be required to be paid to the victims. Additionally, a potential jail sentence may be imposed, as reflected below.

Tier	Potential jail sentence
Reasonable cause or no knowledge of violation	Up to one year
Committed under false pretenses	Up to five years
Committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm	Up to ten years

State law penalties may also apply.

Under the court case In re Caremark, a Board member can be held liable for losses caused by non-compliance with legal standards if the Board member failed "to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists."

Under the U.S. Department of Justice's Yates Memo, the U.S. Department of Justice (DOJ) expressed its intent to focus on individual accountability for corporate wrongdoing. To be eligible for cooperation credit, the corporation must provide relevant facts regarding individuals involved in corporate misconduct to the DOJ. Further, both criminal and civil investigations will focus on individuals at an investigation's inception and the DOJ's evaluation of whether to sue an individual will be based on factors beyond the individual's ability to pay.

This means that your Board members should receive training on their duty to exercise oversight of your organization's activities. Your organization should have a system of reporting compliance issues to the Board so it can oversee the organization's efforts to prevent, detect, and address corporate misconduct.

How can your organization encourage compliance?

1. There must be buy-in at the top. The Board and senior management must follow your HIPAA policies.
2. Your organization should encourage employees to establish personal work goals that include measurable compliance objectives.
3. Your organization can recognize and reward workforce members for their promotion of compliance, contributions to compliance-related activities, and actions that are consistent with your compliance program's goals.

Updated 10/20/2023