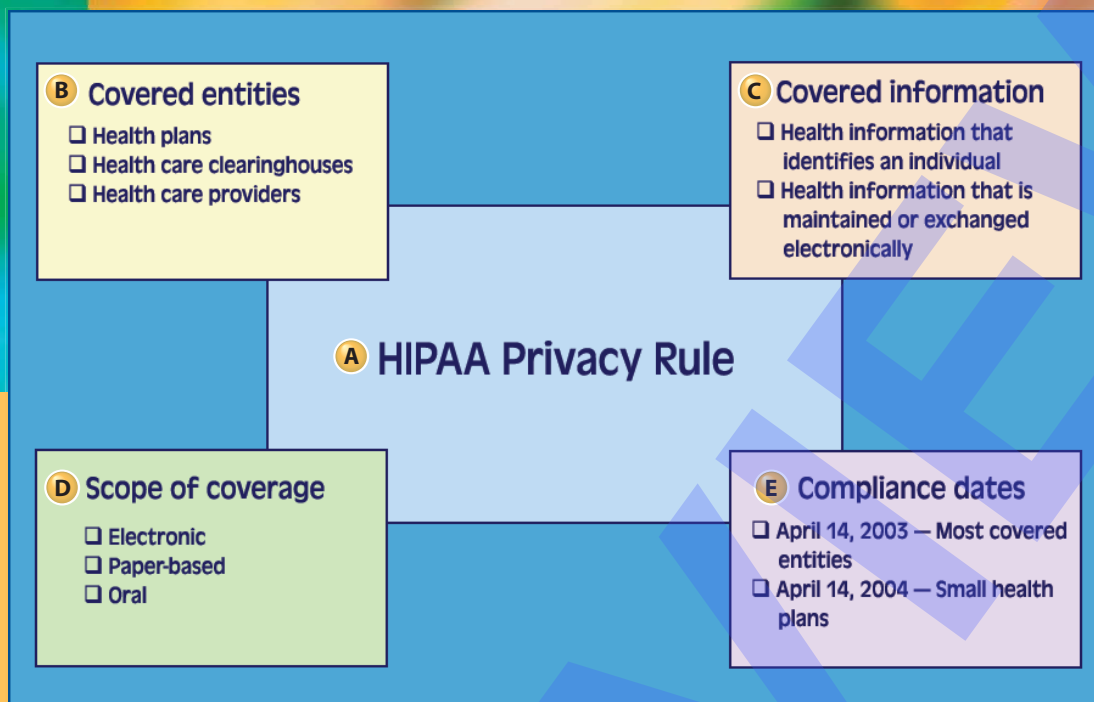


# HIPAA Privacy Rule



## Privacy Basics

Key terms and an overview of the Privacy Rule



- Key terms
- Notice (required)
- Authorization (required)
- Policies and procedures
- Flow of PHI/PII
- Releasing PHI
- Minimum necessary

## PHI Use and Disclosure

PHI activities



- Individuals' (patients') rights
- Fax requirements
- Limited data set
- Business associates
- Business associate contracts (BACs)
- Data use agreements

## Privacy Solutions

Key steps for complying with the Privacy Rule



- Administrative requirements
- Organizational assessment
- Site assessment
- Gap analysis
- Remediation and evaluation

## Top Productivity Tips and Solutions

Hints on reaching compliance



- Costs involved in working toward compliance
- Incoming PHI
- Key privacy documents
- Developing Privacy Rule Plans
- Record keeping

- A HIPAA Privacy Rule**  
A rule that creates national standards to protect people's personal health information. This rule also gives patients increased access to their medical records.
- B Covered entities**  
Health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions (such as enrollment, billing, and eligibility verification) electronically. A *health plan* is an individual or group plan that provides, or pays the cost of, medical care. A *health care clearinghouse* is an organization that processes health care transactions on behalf of providers and insurers. A *health care provider* is a person who is trained and licensed to give health care. A health care provider can also be a place licensed to give health care.
- C Covered information**  
The key information covered by the Privacy Rule, which is *protected health information* (PHI). The Privacy Rule protects health information that identifies an individual and is maintained or exchanged electronically.
- D Scope of coverage**  
Medical records and other individually identifiable health information (IIHI) that's used or disclosed electronically, via paper, or orally by a covered entity. Thus, if you print any electronic information, that information (in paper form) retains its coverage.
- E Compliance dates**  
The latest dates by which covered entities must comply with the Privacy Rule. Most covered entities must comply with the Privacy Rule by April 14, 2003. Small health plans must comply by April 14, 2004.

## Key terms

### Individually identifiable health information (IIHI)

Individually identifiable health information (IIHI) is information, including demographic data, that:

- Is created or received by a health care provider, health plan, employer, or clearinghouse.
- Relates to an individual's past, present, or future physical or mental health or condition, or relates to health care provided to an individual, or relates to payment for that health care.
- Identifies the individual (or there is a reasonable basis to believe that the information can be used to identify the individual).

### Protected health information (PHI)

Any patient-identifiable information is now protected health information (PHI) regardless of the media form it is or was in. Data can be at rest or in transit. At rest can mean data that is accessed, stored, processed, or maintained.

### Treatment, payment, or health care operations (TPO)

- **Treatment** — Organizations can use or disclose information to health care providers who are involved in your health care. For example, information can be shared to create and carry out a plan for your treatment.
- **Payment** — Organizations can use or disclose information to get payment or to pay for the health care services you receive. For example, an organization can provide PHI to bill your health plan for health care you received.
- **Health care operations** — Organizations can use or disclose information in order to manage their programs and activities. For example, an organization can use PHI to review the quality of services you receive.

### Patient-identifiable information (PII)

PII is a subset of PHI that contains identifiers (such as name, address, Social Security number) that could be used to identify an individual.

### De-identified information (DII)

Once the personal identifiers have been removed from a data set, the information is not individually identifiable and can be disclosed without an individual's Authorization.

### Use and disclosure

Use and disclosure are two fundamental concepts in the HIPAA Privacy Rule. *Use* limits the sharing of information within a covered entity. *Disclosure* restricts the sharing of information outside the covered entity.

- **Use** refers to doing any of the following to individually identifiable health information (IIHI) by employees or other members of an organization's workforce:
  - Sharing
  - Employing
  - Applying
  - Utilizing
  - Examining
  - Analyzing

Information is used when it moves within an organization.

- **Disclosure** is defined as doing any of the following by the entity holding the information so that the information is outside the entity:
  - Release
  - Transfer
  - Provision of access to
  - Divulging in any manner

Information is disclosed when it's transmitted between or among organizations.

## Notice (required)

### Create a Notice

The Privacy Rule requires covered entities to provide a Notice that summarizes their privacy practices to individuals. A Notice must:

- Be written in plain, simple language.
- Include a header that reads:  
**This Notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review carefully.**
- Describe the covered entity's uses and disclosures of PHI.
- Describe an individual's rights under the Privacy Rule. These include the right of the individual to:
  - Request restrictions on certain uses and disclosures.
  - Receive confidential communication of PHI.
  - Inspect, copy, and amend PHI.
  - Obtain an accounting of disclosures of PHI.
- Describe the covered entity's duties.
- Describe how to register complaints concerning suspected privacy violations.
- Specify a point of contact.
- Specify an effective date.
- State that the entity reserves the right to change its privacy practices.

## Authorization (required)

### Create an Authorization

The Privacy Rule requires covered entities to provide an Authorization that allows use and disclosure of PHI for purposes other than treatment, payment, or health care operations (TPO).

- An Authorization must be written in specific terms.
- An Authorization can allow PHI to be used and disclosed by the covered entity seeking the Authorization or by a third party.
- Covered entities must obtain an individual's Authorization for uses or disclosures not covered by the Notice.

### Core elements of an Authorization

An Authorization must:

- Give a specific and meaningful description of the authorized information.
- List the persons authorized to use or disclose PHI.
- List the persons to whom the covered entity may make the requested use or disclosure.
- Describe the purpose(s) of the requested use or disclosure.
- Give an expiration date or an expiration event for the use or disclosure of an individual's PHI.
- State the individual's right to revoke the Authorization in writing, and state the exceptions to the right to revoke.
- Detail the ability or inability to conduct treatment, collect payment, manage enrollment, or determine eligibility for benefits based on the Authorization.
- State that information used or disclosed in accordance with the Authorization might be subject to re-disclosure by the recipient and might no longer be protected by this rule.
- Have the individual's signature and the date.

*NOTE: If an Authorization is signed by a personal representative of the individual, the Authorization must have a description of the representative's authority to act for the individual.*

- Be written in plain language.

## Policies and procedures

Every HIPAA-regulated practice must keep key audit documents and forms—including a Policies and Procedures manual—that the HHS's Office for Civil Rights HIPAA Agents will look for.

### Examples of privacy policies

- Uses and Disclosures of Patient, Client, or Participant Information
- Uses and Disclosures for Research Purposes and Waivers
- Enforcement, Sanctions, and Penalties for Violation of Individual Privacy
- Patient (or Client) Rights
- Minimum Necessary
- De-identification and Use of Limited Data Sets
- Administrative, Technical, and Physical Safeguards
- General Privacy Policy

## Flow of PHI/PII

### Define patient-identifiable information (PII)

Define how the information will be handled.

### Track the flow of PII

- How is new information created?
- What information is reviewed and modified?
- What information is transferred within the organization?
- What information is received from within or outside the organization?
- From what other sources is information received?
- To what sources is information disclosed outside the organization?
- What information is maintained by the organization?

### De-identified or aggregate patient data

Does the organization handle aggregate patient data (which does not identify individual patients) in any of the following ways?

- Creating or reviewing aggregate data
- Transferring data within the organization
- Receiving data within the organization
- Receiving aggregate data from outside the organization
- Disclosing aggregate data to anyone outside the organization

## Releasing PHI to third parties

Before releasing PHI to third parties, assuming that the information requested is not for TPO, follow these steps:

1. **Verify the request.** Upon receiving a request for PHI, verify the identity and authority of the requestor.
2. **Obtain the patient's permission.** Make sure the patient has given the appropriate permissions for disclosing the information.
3. **Review the requested information.** Make sure the information disclosed is limited to the minimum necessary information required for the third party to perform the task.
4. **Prepare the requested information.** Make sure disclosures are not made to unauthorized individuals or organizations, and that information will be disclosed only to the extent necessary, and only to the permitted recipient.
5. **Send the requested information.** Make sure you document each disclosure sent.

## Minimum necessary

Under HIPAA, *minimum necessary* means that the entity should disclose just enough information to get the job (treatment) done. This information can be the entire medical record if it's needed for TPO.

### Exceptions

Minimum necessary does not apply to:

- Health care providers (for treatment purposes)
- The individual who is the subject of the information
- Uses or disclosures made in carrying out an Authorization requested by the individual
- Uses or disclosures required for compliance with standardized HIPAA transactions
- Disclosures to the Department of HHS when disclosure of information is required under the Privacy Rule for enforcement purposes
- Uses or disclosures that are required by law

### Reasonable reliance

When someone requests disclosure, a covered entity is sometimes allowed to rely on the requestor's judgment about the minimum amount of information needed. This reliance is allowed when the request is made by:

- A public official or agency for a disclosure permitted under the Privacy Rule
- Another covered entity
- A professional who is a workforce member or business associate of the covered entity
- A researcher with documentation from an Institutional Review Board (IRB) or Privacy Board

### Reasonable effort

To make reasonable efforts to limit use of, disclosure of, and requests for PHI to the minimum necessary, a covered entity should:

1. Document all routine PHI communications, focusing first on high-impact communications.
2. Document which PHI is required for each type of communication.
3. Review existing policies, procedures, and training.
4. Document any exceptions for risk analysis and remediation, and send all exceptions to the Privacy Officer.
5. Determine which communications require change, and build a remediation project plan.
6. Execute the initial remediation plan.
7. Evaluate the remediation plan.
8. Repeat this process with lower-impact communications.

### Policies and procedures

Develop policies and procedures to restrict the use of PHI to the minimum necessary information for the performance of any task. Policies must include procedures that:

- Identify the persons or classes of persons in the entity's workforce who need access to PHI to carry out their duties.
- Identify the category or categories of PHI to which each person or class of persons needs access.
- Identify conditions for access to PHI.

### Use and disclosure for treatment

HIPAA tries to avoid having a negative impact on treatment activities. For treatment:

- No business associate contract (BAC) is needed between providers.
- Disclosures are allowed with providers who aren't covered entities.
- Minimum necessary does not apply.
- Only direct treatment providers are required to get a signed acknowledgement of receipt of their Notices.

# PHI Use and Disclosure

## Individuals' (patients') rights

Individuals have a right to:

- Access their PHI.
- Ask to amend their PHI.
- Allow, deny, or revoke an Authorization.
- Receive an accounting of disclosures.
- Restrict uses and disclosures of their PHI.
- Receive information from the covered entity by alternate means, such as mail, e-mail, fax, or telephone or at alternate locations.
- File complaints.

## Fax requirements

### Fax requirements and recommendations

PHI can be exchanged via faxes sent to business associates, covered entities, and others. Here are some recommendations to help safeguard information exchanged via fax machines:

- **Fax cover page**—State clearly on the fax cover page that confidential and protected health information is included, and that the information must be protected and must not be shared or disclosed without the appropriate Authorizations from the patient.
- **Location of fax machine**—Keep the fax machine in an area that is not accessible by people who are not authorized to view PHI.
- **Faxes with PHI**—Faxes with PHI that your office receives must be stored promptly in a protected and secured area.
- **Fax numbers**—Always confirm the accuracy of fax numbers to minimize the chances of faxes being sent to unintended recipients.
- **Confirmation**—Program the fax machine to print a confirmation for all faxes sent, and staple the confirmation to each PHI fax sent.
- **Fax storage**—Define processes and systems for tracking and storing PHI that has been faxed.
- **Business associates**—Require your business associates to keep their fax machines and the faxes received in protected areas.
- **Training**—Train all employees to understand the importance of safeguarding PHI sent or received via fax.

## Limited data set

A limited data set can be used for the purposes of research, public health, or other health care operations, as long as the covered entity removes the following fields:

- Name
- Street address
- Telephone and fax numbers
- E-mail address
- Social Security number
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- URLs and IP addresses
- Full-face photos and other comparable images
- Medical record numbers, health plan beneficiary numbers, and account numbers
- Device identifiers and serial numbers
- Biometric identifiers (fingerprints and voiceprints)

## Business associates

A *business associate* is a person or entity who provides certain functions, activities, or services—involving the use and/or disclosure of PHI—for or to a covered entity.

- A business associate is not a member of the health care provider's, health plan's, or other covered entity's workforce.
- A health care provider, health plan, or other covered entity can also be a business associate of another covered entity.
- The Privacy Rule is extended to a covered entity's arrangements with their business associates to prevent covered entities from circumventing the Privacy Rule by contracting out the performance of various functions.

### Examples of business associate services

- Legal
- Actuarial
- Consulting
- Administration accreditation
- Financial or accounting
- Data aggregation

## Business associate contracts (BACs)

A *business associate contract* (BAC) is a document demonstrating that the covered entity has obtained satisfactory assurance that the business associate will appropriately safeguard PHI.

BACs must do two things:

- Specify the PHI to be disclosed and the ways that information can be used.
- Impose security, inspection, and reporting requirements on the business associate.

### Business associate activities

Business associates can be authorized to do the following:

- Use and disclose PHI as necessary for proper management and to meet legal obligations.
- Provide data aggregation services to the covered entity.

*Data aggregation* is the process of combining information from a variety of sources to provide comparative or other management information.

### Exemptions

The following types of organizations are not defined as business associates:

- **Conduits**—Entities that transport information but don't have access to it except on a random or infrequent basis.
- **Financial institutions**—Firms that process consumer-related financial transactions.

## Data use agreements

A *data use agreement* is an agreement between the disclosing covered entity and the recipient of the data. In this agreement, the recipients promise to:

- Limit their use of the limited data set to research, public health, and other health care operations.
- Limit who can use or receive the data.
- Protect, and not re-identify, the data.

# Privacy Solutions

## Key steps

In working to meet the Privacy Rule requirements, a business needs to consider the following key steps:

1. Identify administrative requirements.
2. Assess the organization's current privacy interactions and policies.
3. Analyze the current interactions and policies for compliance gaps.
4. Correct organizational processes so they are in compliance.
5. Negotiate business associate contracts (BACs).
6. Certify that the organization meets HIPAA requirements.

## Administrative requirements

The Privacy Rule specifies the following administrative requirements:

- **Personnel designations**—Assign a Privacy Officer to ensure that the privacy procedures are adopted and followed.
- **Complaints**—Define a process for handling complaints.
- **Policies and procedures**—Develop clear forms, policies, and procedures.
- **Documentation**—Create and maintain documentation related to the HIPAA Privacy Rule.
- **Training**—Train employees so that they understand the following:
  - Privacy and security requirements
  - PHI policies and procedures
- **Safeguards**—Implement administrative, technical, and physical safeguards.
- **Sanctions**—Implement a policy that describes the specific actions to be taken against members of the covered entity's workforce who fail to comply with internal policies and procedures.
- **Mitigation**—Implement a policy that includes steps to remedy any harm caused by a mistake and to prevent that mistake from occurring again.
- **No intimidating or retaliatory acts**—Implement a policy to make sure your organization doesn't intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient for the exercise of any right under the Privacy Rule.
- **No waiver of rights**—Implement a policy to make sure your organization doesn't require, as a condition of TPO, that an individual waive his or her right to make complaints to the Secretary of HHS.

## Organizational assessment

### Assessment areas

- Business scope and objectives
- Business policies, risks, and vulnerabilities
- Infrastructure technology
- Business and technical skills, capabilities, and limitations

### The assessment report

This report typically includes the following information:

- Site assessment
- Review of policies, documents, practices, and procedures
- Flow of PHI
- Review of contracts
- Review of communication programs

## Site assessment

### Gather detailed information about the physician's facilities and operations practices, including:

- Total square footage
- Number of patient rooms
- Sites where diagnostic tests are performed
- Number of computer systems
- Types of software and applications installed

### Perform an audit for the following areas:

- Records storage, transmission, and disposition
- Computer systems (usage and applications)
- Policies and procedures
- Forms and paperwork
- Labs and diagnostic facilities
- Patient privacy
- Reception areas

## Gap analysis

During this phase, the results of the assessment are analyzed and interpreted.

1. Information collected from the physician's office is mapped and compared to the rules defined in HIPAA regulations.
2. The analysis identifies the policies, documents, practices, and procedures that meet, or don't meet, the Privacy Rule requirements.
3. The result is a gap analysis report, which is used to prioritize HIPAA compliance initiatives.

### The gap analysis report

A gap analysis report typically compares the organization's current practices to HIPAA requirements in the following areas:

- Use and disclosure
- Business associates
- Minimum necessary
- Administration, enforcement, and complaint processes
- Individual rights
- Special requirements

The report also identifies compliant and non-compliant policies, documents, practices, and procedures. The report then provides recommendations on:

- Strategic framework
- Priorities
- Implementation challenges

## Remediation and evaluation

### Remediation

Remediation is the process of correcting organizational practices to bring them into compliance.

### Evaluation

1. Perform a final assessment to ensure compliance.
2. Inspect and close all gaps.
3. Evaluate whether the organization has met all HIPAA Privacy Rule requirements. This evaluation can be done by an outside firm or by the organization itself.

# Top Productivity Tips and Solutions

## 1. Get more help with HIPAA Privacy Rule compliance.

The following Web sites provide information and resources related to Privacy Rule compliance:

- HIPAA Academy — [www.HIPAAAcademy.net](http://www.HIPAAAcademy.net)
- Office for Civil Rights — [www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/)
- Department of Health and Human Services — <http://aspe.hhs.gov/admsimp/>

## 2. Costs involved in working toward compliance.

As businesses work toward Privacy Rule compliance, they will incur costs. Cost areas might include:

- Minimum necessary
- Privacy Officer
- Business associates
- Policy development
- Disclosure tracking and history
- Training
- Requirements for research
- De-identification of data
- Authorizations

## 3. Tasks involved in working toward compliance.

To bring your organization into compliance with the Privacy Rule, you'll need to do the following:

1. Identify the Privacy Officer.
2. Identify the individual who will handle complaints.
3. Identify the members of the privacy team.
4. Work with your legal counsel to determine which documents need to be created (both internal documents and contracts), and use any document templates available to get started. Free templates are available at [www.ouwb.ohiou.edu/hipaa/ohic-oucom/pages/documents.htm](http://www.ouwb.ohiou.edu/hipaa/ohic-oucom/pages/documents.htm).
5. Understand and define the PHI that your enterprise collects. Then, determine how this PHI flows through your business and which business associates come in contact with the PHI.
6. Review all BACs and data use agreements, and obtain satisfactory assurance from all business associates and recipients of the limited data set that they will appropriately safeguard the information.
7. Develop HIPAA-related policies, forms, and documents.
8. Determine which safeguards, such as those required for security, you will need to implement for compliance.
9. Develop a policy for receiving, processing, and documenting all complaints.
10. Train your entire staff, and establish an internal knowledge base on HIPAA compliance issues.

## 4. Incoming PHI.

For incoming PHI, review the following information:

- Type of disclosure to practice
- Purpose and description of disclosure
- Specific information received
- HIPAA Rule Permission for Disclosure/Receipt
- Whether the practice or provider requested the PHI
- Where the PHI will be filed or stored
- Whether the PHI will be transferred between groups or departments internally, and if so, which ones

## 5. Key privacy documents.

Privacy Rule compliance will result in the following policies and procedures:

- Notice of Privacy Practices
- Consent for Use or Disclosure for Treatment, Payment, or Health Care Operations (optional as a result of the Final Privacy Rule)
- Authorization for Other Uses and Disclosures
- Privacy Officer Job Description
- Termination Procedure

## 6. Developing Privacy Rule forms.

An organization will need to develop forms that support requirements for the Privacy Rule. These forms include:

- Privacy Compliance Program Statement of Understanding
- Access to Records Request
- Amendment of Health Record Request
- Restriction of Use and Disclosures Request
- Accounting of Disclosures Request
- Disclosure of Protected Health Information (PHI)

## 7. Record keeping.

Covered entities must keep records of:

- Notices of Privacy Practices
- Written acknowledgements of receipt of Notice
- Consents
- Authorizations
- Disclosures

*NOTE: Disclosures that are allowed by the Notice or by an Authorization do not need to be recorded for HIPAA compliance. A covered entity might still want to record these disclosures for its own business purposes, but it would not need to report them to an individual or an HHS auditor. Records must be retained for six years.*

## 8. Oral disclosures.

When orally exchanging PHI, use these safeguards:

- Speak to people in private.
- Step into a room and close the door.
- Lower your voice.
- Use the handset instead of the speakerphone.

## 9. Resource for HIPAA training.

HIPAA Academy delivers highly specialized training solutions for the development of HIPAA skills, knowledge, and certification. HIPAA Academy programs include:

- HIPAA Overview (1 day)
- HIPAA Executive Brief (2 hours)
- HIPAA Privacy Awareness (3 hours)
- HIPAA Security Awareness (3 hours)
- HIPAA Transactions Overview (1 day)
- Certified HIPAA Professional (3 days)
- Certified HIPAA Administrator (1 day)
- Certified HIPAA Security Specialist (2 days)
- HIPAA e-learning solutions — Privacy Awareness, Security Awareness, and HIPAA Overview

For further information about HIPAA Academy training programs, visit [www.HIPAAAcademy.net](http://www.HIPAAAcademy.net) or call 1-877-899-9974, extension 20.

