Compliancy Group

# Compliancy Group Policy Template Starter Kit

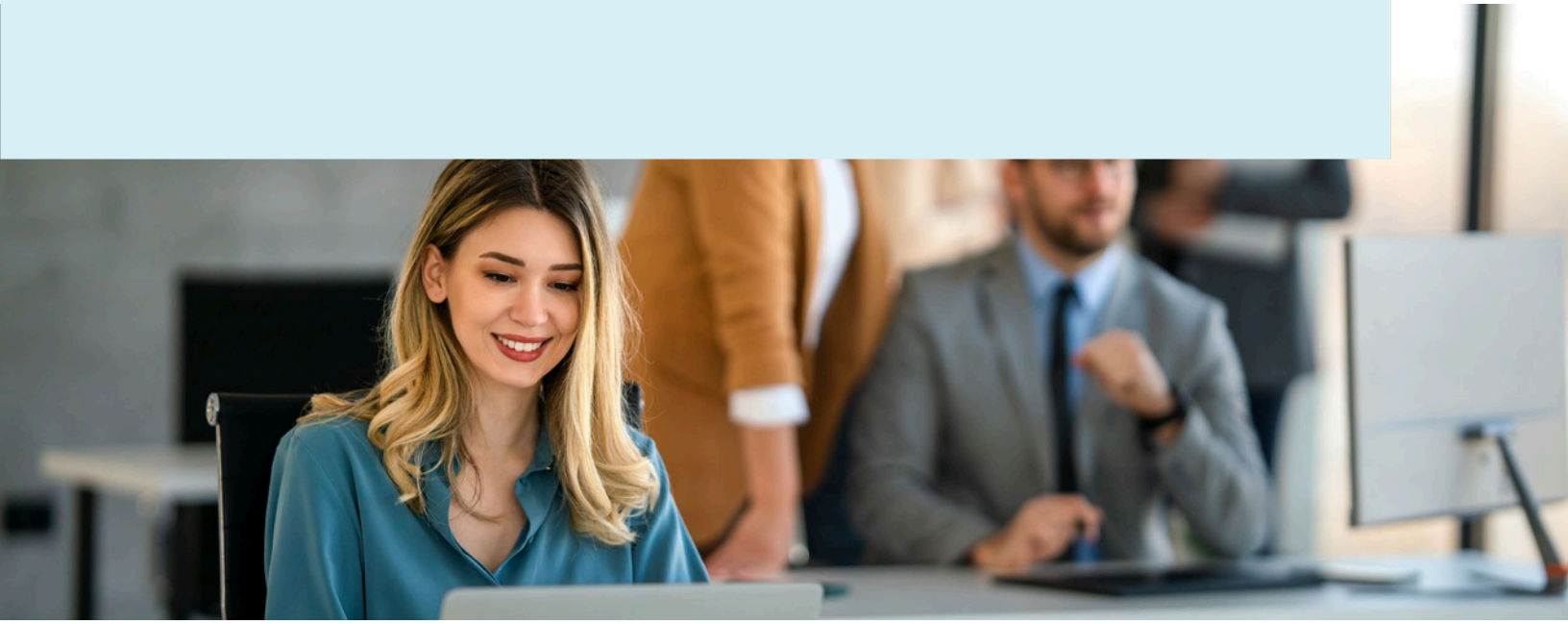
Get policies to prevent the most cited reasons behind HIPAA fines.

# Your Policy Template Pack

Having policies and procedures in place is one of the most critical aspects of building an effective compliance program. Policies and procedures give employees guidelines on best practices in various scenarios that come up in their day-to-day work, and instills a culture of compliance in your organization.

While different regulations apply to different types of healthcare organizations, and each of these comes with unique requirements, every healthcare business must meet the Health Insurance Portability and Accountability Act (HIPAA). To help get you started, we put together policy templates for a few of the most overlooked HIPAA requirements, and most cited in OCR settlements.

- Security Management
- Right of Access
- Breach Notification
- Bonus: Steps to Take if Breached



Roughly

**80%**

HIPAA fines cite missing risk assessment documentation

## HHS Risk Analysis Initiative

In October 2024, the HHS launched the "Risk Analysis Initiative," citing the widespread failure of healthcare organizations to meet the HIPAA Security Rule requirement to conduct an accurate and thorough security risk analysis to identify weaknesses and vulnerabilities to electronic protected health information.

As of August 2025, the OCR has settled 10 cases under the initiative. In the most recent settlement announced on August 18, 2025, BST & Co. CPAs, LLP ("BST"), a New York public accounting, business advisory, and management consulting firm, agreed to pay $175,000 in civil monetary penalties.

OCR Director Paula M. Stannard stated:

> "A HIPAA risk analysis is essential for identifying where ePHI is stored and what security measures are needed to protect it. Completing an accurate and thorough risk analysis that informs a risk management plan is a foundational step to mitigate or prevent cyberattacks and breaches."

https://www.youtube.com/watch?v=3tDGwmW-kO8
https://www.hhs.gov/press-room/hhs-ocr-bst-hipaa-settlement.html

# Data Security Policy – Security Management

**Policy Purpose:** To provide principles and guidelines for managing Organization's information security program and processes.

## Scope

The Security Management Policy will cover Organization's:

- Information Security Management policy and program
- Security program documentation, including creation and retention
- Organizational structure
- Risk management activities, treatment, and assessments
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

## Policy

Organization has defined a security management process that incorporates a risk-based approach, and takes into account the resources, both internal and external, available to the company. Organization considers information security a priority and has established controls and processes to keep sensitive information and protected information, such as ePHI, safe.

In addition to specific processes and controls, Organization's leadership, including senior management and the Board of Directors, are committed to a security-conscious company culture, and information security.

## Procedures

### Information Security Management Program

Organization's information security program defines roles and responsibilities for personnel. Charts, policies, and procedures reflect the responsibilities of the Board of Directors, the independence of the Board, and the expertise available on the Board.

Organization has based its information security program on frameworks and best practices that support its objectives, including relevant accounting standards and the Center for Information Security (CIS). The company's information security program considers the regulatory and compliance standards that need to be included in the program, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Organization's information security program ensures that controls and processes maintain the confidentiality, integrity, and availability (the CIA triad) of sensitive or protected data. When needed, the company separates incompatible duties between different personnel or roles.

***Organization Chart***

Organization has an organization chart that lists personnel and their roles and/or titles and includes reporting lines. The organization chart is reviewed and updated at least annually, or when significant changes occur.

***Compliance Documentation and Retention***

For compliance and analysis purposes, all control activities related to information security are documented. This documentation may need to be provided for audit and assessment purposes. Documentation is a key step in any control activity and should always be completed thoroughly. Electronic documentation, audit logs, ticketing systems, and other IT systems assist with collecting this type of documentation and information. Access to documentation repositories is limited to appropriate personnel only, as it may contain sensitive or protected information.

## Risk Management

Organization applies risk management principles to its information security program in order to better identify, assess, and address risks or threats to the company. Information security risk management involves a cycle of steps:

1. Risk Identification
2. Risk Analysis
3. Risk Treatment and Action Plan
4. Risk Monitoring and Review

Risk assessments are an important part of our risk management program and are performed at least annually. The Guard's data security program is available as one tool in this assessment and includes evidence collection and risk assessment components.
The company's risk register is also reviewed and updated at least annually and includes any findings from completed risk assessments.

***Risk Register***

A risk register is a document or database that contains a listing of the company's risks, including:

- Risk description
- Risk likelihood score
- Risk impact score
- Risk analysis (aggregated score, usually calculated as likelihood score * impact score)
- Risk treatment
- Risk action plan or remediation plan, including an estimated date of completion
- Risk owner
- Other relevant notes or data points

***Risk Committee***

Organization has created a Risk Committee and an accompanying Charter that outlines the Risk Committee's purpose, objectives, and required deliverables or outcomes. The Risk Committee meets at least quarterly, and documents meeting minutes that we retain for compliance purposes. If necessary, the risk register should be updated to reflect updates and changes following the Risk Committee meeting.

## Roles and Responsibilities

Risk Committee: Meets quarterly to review the company's risk posture, including the risk register and any recent risk assessments. Provides cross-functional insights into risk management. Decides the priority of risks as needed.

## Violations

Violations of the information security policy and program may be subject to disciplinary action.

## Forms/Plans/Documents

- Organization Chart
- Risk Committee Charter
- Risk Committee Meeting Minutes
- Risk Assessment Documentation

# The HHS Right of Access Initiative

In 2019, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) launched its "Right of Access Initiative," prioritizing enforcement for providers who failed to provide patients (or their personal representative) timely access to their medical records.

As of March 2025, the HHS OCR has settled 53 cases under the initiative. In the most recent Right of Access settlement announced on March 6, 2025, Oregon Health & Science University agreed to pay $200,000 to settle the matter.

> **"The HIPAA Privacy Rule requires that individuals and their personal representatives receive timely access to their medical records. A covered entity's responsibility to provide timely access continues, even when a covered entity contracts with a business associate to respond to HIPAA right of access requests," said then OCR Acting Director Anthony Archeval.**

https://www.hhs.gov/press-room/penalty-against-or-health-science-university.html

# Privacy Policy - Individual Right: Access to Protected Health Information

**Policy Purpose:** It is the policy of the Organization to honor an individual's right to access, inspect, and obtain a copy of their PHI contained in the designated record set and to charge only allowable fees for such access.

## Policy

This policy describes Organization's responsibility for providing access to a designated record set to individuals for as long as the record is maintained and the procedures for ensuring individuals' timely rights to access, inspect and copy their protected health information and seek review of some denials of access. Additionally, the policy establishes the requirements for determining and charging reasonable fees related to access requests by individuals.

## Procedures

### Accessing and Inspecting PHI Timing and Process

1. An individual must make a request to a member of the workforce to access and inspect their PHI. Whenever possible, this request shall be made in writing and documented on either an "Authorization for Disclosure" form or in the notes of the individual's health record.

2. The workforce member who receives the request should direct it to the individual designated to handle such requests. If no such person is available and the workforce member is unsure of whether access is appropriate, they should contact their supervisor or the Privacy Officer to help make that determination prior to allowing or denying access.

3. When access is granted, the Organization will provide access to the requested PHI and furnish a copy if requested within a reasonable time but no later than 30 days from the date of the request unless the Organization is not able to provide access within 30 days. See below for the requirements on the form and fees for copies.

4. Where it cannot provide access within the 30-day time limit, before the 30 days expire, Organization will provide the individual a written notice of the reasons for the delay and include a date when access will be available. Organization will respond to all requests for access within 60 days of the individual's request. A second extension beyond 60 days is not available.

5. The Organization must document and retain the Designated record sets containing the PHI that is subject to access. The Organization must document and retain the titles of persons or offices responsible for receiving and processing requests for access. These records must be maintained for a minimum of six years form the date of creation or the date it was last in effect.

## When Access, Inspection and/or Copy Request is Granted

1. Individual and the Organization will arrange a mutually convenient time and place for the individual to inspect and/or obtain a copy of the requested PHI within the designated record set. Inspection and/or copying will be carried out on site at the Organization with staff assistance if necessary.

2. The patient may choose to inspect the PHI, copy it, or both, in the form or format requested. If the PHI is not readily producible in the requested form or format, the Organization must provide the patient with a readable hard copy form, or other form or format as agreed to by the Organization and the individual.

- If the individual chooses to receive a copy of the PHI, the Organization may offer to provide copying services. The patient may request that this copy be mailed.
- If the individual chooses to copy their own information, the Organization may supervise the process to ensure that the integrity of the patient record is maintained.

3. Whenever the PHI in the designated record set is maintained electronically, if the individual requests an electronic copy, Organization will provide access in the electronic form and format requested unless it is not readily producible that way. If it is not readily producible in the requested format, Organization and the individual will agree to a different readable electronic format for production.

4. Upon prior approval by the patient, the Organization may provide a summary of the requested PHI and charge an agreed upon fee (must not exceed the fees allowed – see fee section below).

5. If, upon inspection of the PHI, the patient believes the PHI is inaccurate or incomplete, the patient has the right to request an amendment to the PHI. The Organization shall process requests for amendment as outlined in Privacy Policy - Individual Right: Request Amendment to Designated Record Set.

## Fees

Organization may charge a reasonable cost-based fee for the production of copies (including electronic copies) or a summary of PHI pursuant to the request of an individual (or their personal representative) for their own personal use. Organization may decide to waive such fees. For electronic record requests, Organization may decide to charge a flat fee in lieu of a cost-based fee.

Such fees may only include the actual or average cost of:

1. Labor for copying the protected health information, whether in paper or electronic form;
2. Supplies for creating the paper copy if paper is requested;
3. Electronic media if the individual requests an electronic copy be provided on portable media;
4. Postage when the individual requests that the phi or summary be mailed; and
5. Preparation of a Summary or Explanation of the PHI when the individual was informed in advance and agreed to the stated fee.

If Organization, unless charging the flat fee for electronic records, elects to utilize the actual **cost** associated with the requests rather than determining average or per page costs in determining fees, such fees **may *not* include**:

1. costs associated with verification; documentation; searching for, handling, or retrieving the PHI; processing the request; maintaining systems; or recouping capital for data access, storage, or infrastructure, even if such costs are authorized by State law.
2. Fees established by state law where such fees are in excess of that allowed under HIPAA. State laws typically permit providers to charge a per-page copy fee, of up to a certain dollar value, or to charge a flat fee of up to a certain amount for the entire medical record. These fees are untethered to the actual costs of reproduction and can be in excess of that allowed under HIPAA.
3. Costs for providing, releasing, or delivering medical records or copies of medical records, where the request is for the purpose of supporting the application, claim, or appeal for any government benefit or program requested by the relevant government entity or at the individual's request.

*Flat Fee*
Organization, in its discretion, may charge individuals a flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage. Organization may charge this fee in lieu of going through the process of calculating actual or average allowable costs for requests for electronic copies of PHI.

## When Access, Inspection, and/or Copy Request is Denied in Whole or in Part

The Organization will deny access to any PHI without the opportunity for review if it contains:

1. Psychotherapy notes (See Privacy Policy - Psychotherapy notes for further details); or
2. Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative action or proceeding.

If any part of the designated record set is separate from psychotherapy notes or information compiled in anticipation of legal proceedings, Organization shall allow access to that part of the record.

**Organization May Deny Access without Providing Individual an Opportunity for Review in the Following Circumstances**

1. When Organization is acting under the direction of a Correctional Institution and may deny an inmate's request if it were to jeopardize the health, safety, security, custody, or rehabilitation of the individual, other inmates, or any other person at the correctional institution.
2. When PHI is created in the course of research that is still in progress, provided the individual has agreed to the denial of access when consenting to participating in the research that includes treatment, and the covered health care provider had informed the individual that the right of access would be reinstated upon completion of the research.
3. When PHI in the designated record set was obtained under promise of confidentiality from someone other than a healthcare provider and giving access would reveal the source of the information.
4. An individual's access to PHI that is contained in records that are subject to the Privacy Act (also known as the Freedom of Information Act) may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

**Organization May Deny Access but will Provide the Opportunity for Review of Denials in the Following Circumstances**

1. When a licensed healthcare professional (exercising their professional judgment) has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
2. When the PHI makes reference to another person (unless that person is a healthcare provider) and a licensed healthcare professional has determined in exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the person.
3. When request for access is made by a personal representative of an individual and a licensed healthcare professional has determined in exercise of professional judgment that providing access to that representative can reasonably be expected to cause substantial harm to the individual or another person.

## Denials of Access: Timing, Form and Review

If the Organization *denies* access in whole or in part in any of the circumstances described above, the following requirements will apply to the denial:

Making Other information Accessible: The Organization will give the individual access to the protected health information that is not excluded under the denial to the extent that it is possible to separate the information for which the Organization has a basis for denial.

Denials will be in writing:

The Organization must provide a written denial in plain language to the individual. The denial will contain the following elements:

1. The basis for the denial;
2. A statement of the individual's review rights for reviewable denials; and
3. A description of how the individual may complain to the Organization or to the Secretary of Health and Human Services (HHS) including at a minimum the title and telephone number of the individual designated to handle complaints for the Organization.

Other Responsibilities When Access is Denied:

1. If access is denied because the Organization does not maintain the PHI that is the subject of the request, and the Organization knows where that PHI is maintained, the Organization must inform the individual where to direct the request for access.
2. If access is denied under a situation where that denial may be reviewed, an individual has the right to have the denial reviewed by a licensed healthcare professional who is designated by the Organization to act as a reviewing official. Organization will designate a licensed professional to review the original access decision. The reviewing professional must be someone who did not participate in the original decision to deny access.
3. The patient must initiate the review of a denial by making a request for review to the Organization. If the patient has requested a review, the Organization must provide or deny access in accordance with the determination of the reviewing professional, who will make the determination within a reasonable period of time
4. The Organization will promptly provide written notice to the individual of the determination of the reviewing professional and also act promptly on the reviewer's decision if they have granted access.

# Breach Notification

Healthcare organizations that experience a breach, whether it's due to hacking, unauthorized access to patient information, theft, or loss, have an obligation to report the incident.

The incident must be reported to the Department of Health and Human Service (HHS) Office for Civil Rights (OCR) and affected patients.

According to the HHS:

> **"HIPAA breach notification to affected individuals is essential for providing transparency about what caused the breach, when the breach occurred, what PHI was disclosed, what steps affected individuals should take to protect themselves, and information about what the HIPAA regulated entity is doing to investigate the breach, mitigate harm to affected individuals, and protect against further breaches."**

# Privacy Policy - Breach Notification

## Policy Purpose

Organization takes the privacy and integrity of an individual's personal health information seriously. Organization also has legal responsibilities to protect PHI under HIPAA, to determine when there is a reportable breach of an individual's PHI and to make appropriate and timely notifications following a breach.

The purpose of this Breach Notification Policy is to meet Organization's responsibilities and to provide guidance to Organization workforce members regarding making required notifications when a Breach determination has been made under Privacy Policy - Breach Determination.

This policy establishes guidelines for Organization to

- Make, or assure the appropriate Covered entity or Business associate makes, appropriate notifications to individuals impacted by a Breach;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate notifications to federal and state authorities if required by the details of the Breach determination;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate notifications to media if the findings of the Breach determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and
- Document compliance with the requirements of Breach notifications.

## Policy

This policy establishes guidelines for Organization to:

- Make, or assure the appropriate Covered entity or Business associate makes, appropriate timely notifications to individuals impacted by a Breach;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate timely notifications to federal and state authorities if required by the details of the Breach determination including reporting of breaches involving less than 500 individuals in a single state or geographic region to HHS electronically on an annual basis by March 1 (or February 29th in a Leap year) of the year following the Breach;
- Make, or assure the appropriate Covered entity or Business associate makes, appropriate timely notifications to media if the findings of the Breach determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice if required or desired;
- Ascertain and meet any more stringent applicable contractual notification requirements; and
- Document compliance with the requirements of this policy.

Following the determination of a breach under Privacy Policy - HIPAA incident Reporting and Response and Breach Determination Organization will determine what external notifications are required or should be made (i.e., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.), develop appropriate content for the notices, reports and postings, and communicate each notification, report or positing according to the procedures and requirements set forth below.

# Procedures

### Privacy and Security Officers Shall Direct all Notifications but may Appropriately Delegate Activities

With input from the Compliance Officer and others at their discretion, Organization's Privacy and Security Officers will direct all activities required under this policy including the wording of any Individual Notices, HHS filings, communications required by contract, Media notices, and scripts (including escalation processes) for any telephone inquiries. Legal representation will be utilized if desired by the Privacy or Security Officer or at the direction of anyone on the senior leadership team of the Organization. The Privacy and Security Officer may delegate responsibilities as appropriate but remain responsible for the implementation of Breach Notification Policy requirements. This delegation includes allowing either another responsible Covered entity or a responsible Business associate to make the notifications. Organization remains responsible for assuring all requirements have been met by the delegated entity or individual. For responsibilities of Business associates, please refer to Privacy Policy - Business Associates for more information.

Organization will Determine Notification Requirements based on the findings of the Breach Incident Investigation.

Organization will use the Number of Individuals Involved to Determine Appropriate Notifications and Timing.

**Individual Notification:** If the number of individuals impacted by a breach is known to be less than 500, Organization will follow the notification Procedures set forth below for the timing and content of Individual Notification and Notification to HHS.

**500 or More:** If the number of individuals affected by the Breach is known to be 500 residents of a State or jurisdiction, Organization will provide notification to Prominent media outlets serving the State and regional area where the impacted individuals reside and follow the notification Procedures set forth below for the timing and content of Media Notice, HHS and Notification for Breaches Affecting more than 500 individuals.

If the number of individuals is uncertain, Organization must use reasonable efforts to estimate the number of affected individuals and document its methods. Organization shall use this estimate to determine the number of individuals affected for determining appropriate notification procedures. Should further information or investigation prove the estimate to be incorrect, Organization must update any previous notifications or reports made using that estimate if the method or content of the Notice is materially different due to the change.

See Chart below for Summary of Requirements. Details of Appropriate Notice, Timing, Content and Means appear below the summary chart.

*Subject to Law Enforcement requests for delay

**Substitute notice may be used in some situations for individuals, see policy for details.

## Timing

1. Organization will provide Individual notice without unreasonable delay and in no case later than 60 days following the discovery of a Breach. The Organization may also provide additional notice in urgent situations because of possible imminent misuse of the PHI.
2. Organization will provide Media Notice, when required, without unreasonable delay and in no case later than 60 days following the discovery of a Breach.
3. Organization will provide HHS notice by completing a web report form on the following timeline:
    - If 500 or more individual residents of a State or jurisdiction are affected, Organization will complete the HHS notification without unreasonable delay and in no case later than 60 days following the discovery of a Breach.
    - If fewer than 500 individuals are affected, Organization will notify HHS of each Breach no later than 60 days after the end of the calendar year in which the Breaches were discovered (March 1 or February 29th in a leap year).

## Discovery of Breach

A breach of PHI shall be treated as "discovered" as of the first day the breach is known to the Organization, or, by exercising reasonable diligence would have been known to the Organization (includes breaches by Organization's Business associates). The Organization shall be deemed to have knowledge of a breach if such breach is known or if by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or an agent of the Organization (i.e., a Business associate acting as an agent of the Organization).

## Delays in Timing Permitted: Law Enforcement Delay

When Organization is notified by a law enforcement official that a notification, notice or posting required for a Breach would either impede a criminal investigation or damage national security, Organization may delay the notification, notice or posting for a) a period of time specified by the law enforcement official in writing or b) for the requested amount of time not to exceed 30 days from the date of an oral request for delay from a law enforcement official. Organization will extend the original 30-day delay imposed by an oral request if a law enforcement official makes a later request in writing prior to the expiration of the initial delay request. Any such oral or written request must be documented by Organization and the record preserved.

Workforce members should also refer to Privacy Policy - Verification of Identity and Authority when processing any law enforcement request for delay.

## Content and Means of Notifications and Postings

At a minimum the content of reports, notifications and notices required by law for breaches of the privacy or security of PHI in any form must include the information set forth below and must be communicated by the means indicated:

***Individual Notice: Means of Communication***

In writing by first class mail or by email if the affected individual has consented to such notice. Reference the Sample Breach Notification format for all Individual Notice. If the Organization desires to send additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice but not as a substitute for it.

***Substitute Individual Notice***

When Organization has insufficient contact information for ten or greater affected individuals, Organization will give notice by posting notice for 90 days on the company website or by publication in major print or broadcast media in the area where the affected individuals likely reside.

When Organization has insufficient contact information for fewer than ten affected individuals it may give notice to those individuals by alternative written notice, by telephone or other reasonable means.

***Individual Notice: Content***

1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
2. A description of the types of unsecured PHI that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the individual should take to protect themselves from potential harm resulting from the Breach;
4. A brief description of what the Organization is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

***Media Notice Means of Communication and Content***

For Media Notices the following information should be included and the Notice must include enough information for an individual to determine whether their information may have been disclosed, what they should do if it was and who to contact for more information:

1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
2. A description of the types of unsecured PHI that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the individual should take to protect themselves from potential harm resulting from the Breach;

4. A brief description of what the Organization is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

***Means of Notifying HHS***

For a Breach Affecting 500 or More individuals Organization will timely complete a Notice utilizing the form on the HHS website ( https://OCRportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true ).
For a Breach Affecting less than 500 Individuals Organization will timely file (within 60 days of the end of the calendar year in which the Breach occurred) a Notice utilizing the form on the HHS website ( https://OCRportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true).

## Reliance on Others to Provide Notification

Organization will determine any contractual obligations related to the PHI. If allowable, Organization may choose to rely upon notifications given by a business associate for the Breach notifications required. Organization will request copies of any notifications to its individuals, the public and HHS if Organization's individual's information was breached.

## Recordkeeping

Organization must keep records concerning all notifications, notices and postings made separately for each Breach reported. This includes any reports, notices or postings made by any other party on which Organization relied for its own notice to individuals, agencies, authorities, or media. These records must be kept for a minimum of six years following the provision of the notice, report or posting. If desired, utilize the Breach Notification Documentation Job Aid to record the details for recordkeeping.

# Steps to Take if Your Organization is Breached

What to do in the event you've made an initial determination that a breach has occurred



**Notify** key individuals, departments, and businesses of your finding that a breach has occurred, and work with these groups as needed. These can include (but is not limited to compliance officers, public relations, HR, legal counsel, and insurance carriers.

**If the breach is ongoing,** take steps to terminate the breach immediately, such as securing the area or system where the breach occurred.

**Consider** performing a forensic investigation, to determine the scope of the breach and how it occurred. Document all findings.

**Risk analysis:** Once you have made the initial determination that the breach occurred using a breach-specific risk assessment, update the assessment as needed. For example, one item to assess is the nature and types of PHI identifiers involved in the breach. If initially, you discover that the breach contained social security numbers, and note this in your risk assessment, and then later discover that the breach also includes diagnoses and treatment information, update the assessment to include this information. Updates to the assessment may also be required depending on the results of the forensic investigation. For example, if you initially conclude 200 people were affected by the breach, but the forensic investigation reveals that 1000 people were affected, you would want to update the assessment accordingly.

**Send required notifications and file required reports.** Provide updated notifications and reports if additional information becomes available that requires an update. Work with business associates as necessary to obtain breach detail information. Observe all filing and notification deadlines.

# Steps to Take if Your Organization is Breached

What to do in the event you've made an initial determination that a breach has occurred



**Take mitigation measures.** These can include (but are not limited to): (a) Taking appropriate sanctions against workforce members whose actions were not consistent with your policies and procedures; (b) retraining of workforce members; (c) replacement or repair of affected systems; (d) Developing new or different workflow safeguards (for example, if a breach occurred because an employee inadvertently faxed a message to the a patient at an old fax number, review your Administrative, Technical, and Physical Safeguards of PHI policy to determine whether it contains language about ensuring that you have the correct, up-to-date fax number before a fax is sent. If you don't have the correct number, consider adding language to your policy requiring workforce members to ensure that they only send a fax after they've confirmed the fax number is the most current one on file).



**Enhance** administrative, technical, or physical safeguards, as needed.

**Update** policies and procedures, as needed.



**Review and adhere** to business associate agreement language about breach determination and breach notification obligations.

**Determine** whether re-evaluation of a business associate relationship is needed.

**If criminal activity is suspected,** inform and coordinate with law enforcement. Delay notifications if instructed to do so by law enforcement as specified in the breach notification rule.

**Update** incident reporting and response plan, as needed.

**Document** all assessment, containment, notification, and mitigation measures, and all other post-breach activities.

**Maintain** breach documentation for at least 6 years.

# Steps to Take if Your Organization is Breached

What to do in the event you've made an initial determination that a breach has occurred

| | |
|---|---|
| 1 | **Notify** key individuals, departments, and businesses of your finding that a breach has occurred, and work with these groups as needed. These can include (but is not limited to compliance officers, public relations, HR, legal counsel, and insurance carriers. |
| 2 | **If the breach is ongoing,** take steps to terminate the breach immediately, such as securing the area or system where the breach occurred. |
| 3 | **Consider** performing a forensic investigation, to determine the scope of the breach and how it occurred. Document all findings. |
| 4 | **Risk analysis:** Once you have made the initial determination that the breach occurred using a breach-specific risk assessment, update the assessment as needed. For example, one item to assess is the nature and types of PHI identifiers involved in the breach. If initially, you discover that the breach contained social security numbers, and note this in your risk assessment, and then later discover that the breach also includes diagnoses and treatment information, update the assessment to include this information. Updates to the assessment may also be required depending on the results of the forensic investigation. For example, if you initially conclude 200 people were affected by the breach, but the forensic investigation reveals that 1000 people were affected, you would want to update the assessment accordingly. |
| 5 | **Send required notifications and file required reports.** Provide updated notifications and reports if additional information becomes available that requires an update. Work with business associates as necessary to obtain breach detail information. Observe all filing and notification deadlines. |

# Steps to Take if Your Organization is Breached

What to do in the event you've made an initial determination that a breach has occurred

| | |
|---|---|
| 6 | **Take mitigation measures.** These can include (but are not limited to): (a) Taking appropriate sanctions against workforce members whose actions were not consistent with your policies and procedures; (b) retraining of workforce members; (c) replacement or repair of affected systems; (d) Developing new or different workflow safeguards (for example, if a breach occurred because an employee inadvertently faxed a message to the a patient at an old fax number, review your Administrative, Technical, and Physical Safeguards of PHI policy to determine whether it contains language about ensuring that you have the correct, up-to-date fax number before a fax is sent. If you don't have the correct number, consider adding language to your policy requiring workforce members to ensure that they only send a fax after they've confirmed the fax number is the most current one on file). |
| 7 | **Enhance** administrative, technical, or physical safeguards, as needed. |
| 8 | **Update** policies and procedures, as needed. |
| 9 | **Review and adhere** to business associate agreement language about breach determination and breach notification obligations. |
| 10 | **Determine** whether re-evaluation of a business associate relationship is needed. |
| 11 | **If criminal activity is suspected,** inform and coordinate with law enforcement. Delay notifications if instructed to do so by law enforcement as specified in the breach notification rule. |
| 12 | **Update** incident reporting and response plan, as needed. |
| 13 | **Document** all assessment, containment, notification, and mitigation measures, and all other post-breach activities. |
| 14 | **Maintain** breach documentation for at least 6 years. |

# Conclusion

Clive Wilby, Compliance Officer and long-time Compliancy Group client, comments on the policies in our software, The Guard:

> **“ There are privacy and security policy and procedure manuals – let me read them. And I did, and I went. This is exactly the answer to everything I need, and will save me at least three years of work.”**

With a structured, confident approach, healthcare organizations can use the policy module to its full potential—with access to HIPAA, OSHA, FWA, and HR policy templates, you can be confident in your compliance program.

**Book A Demo →**

# About Compliancy Group

Compliancy Group’s compliance software makes implementing policies and procedures a breeze. Get templated policies and procedures and only adopt those that apply to your organization. You can even customize them and track when changes were made and by whom. The software allows you to assign policies for individual review and attestation, and allows employees to access them right from their personalized employee portal. Our software takes it even further and includes training, risk assessments, and more. Learn how our software can help with policy management!

sales@compliancygroup.com

compliancygroup.com

Compliancy Group