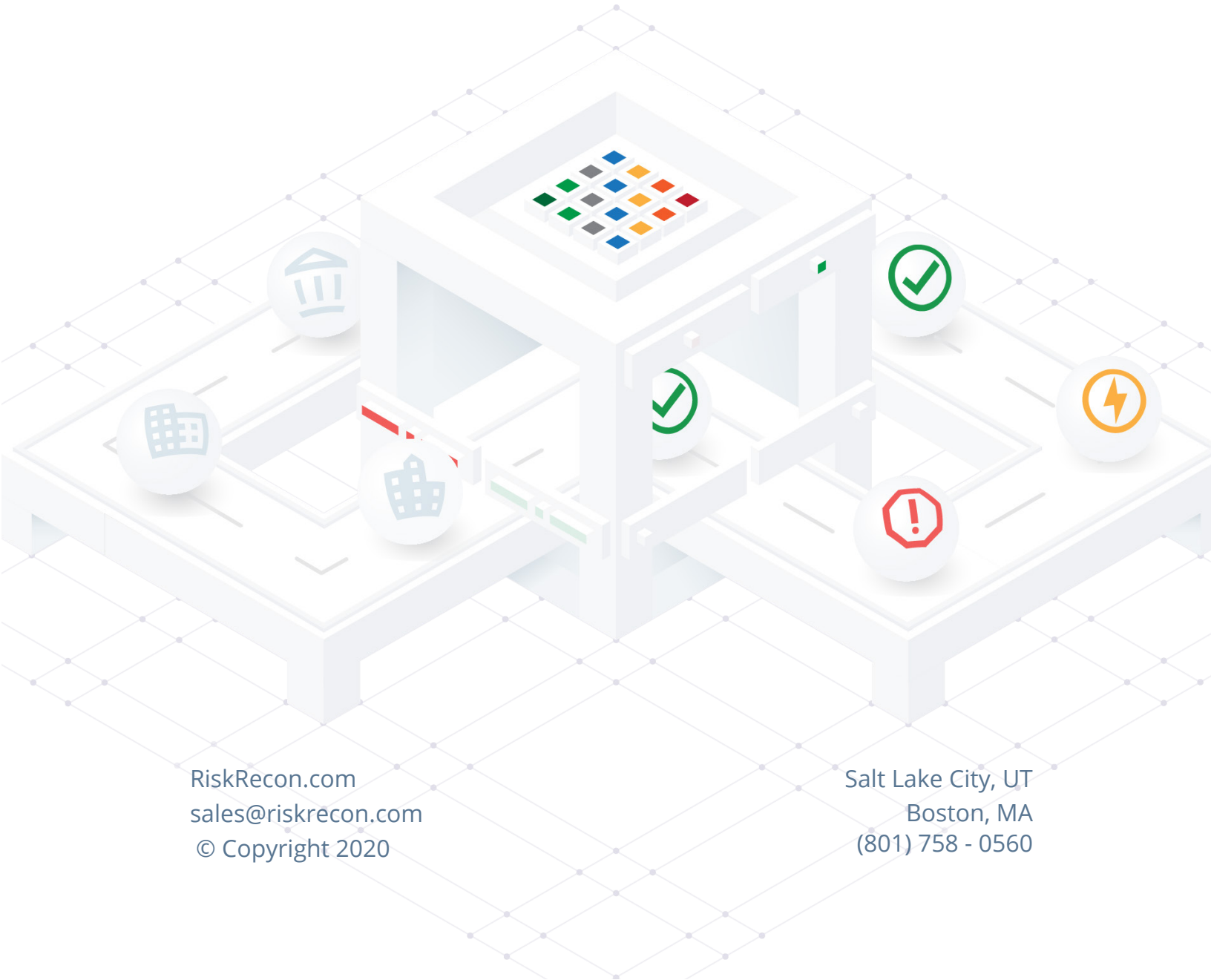




# HIPAA & HITECH: Today's Health Data Privacy Laws

A guide to healthcare data privacy regulations



RiskRecon.com  
sales@riskrecon.com  
© Copyright 2020

Salt Lake City, UT  
Boston, MA  
(801) 758 - 0560

# Table of Contents

---

Healthcare Data Privacy laws: Introduction

3

HIPAA & HITECH: Requirements

5

HIPAA & HITECH: Third-Party Risk Management

13

# Healthcare Data Privacy Laws: Introduction

HIPAA & HITECH are major regulations in the healthcare industry in the United States of America. HIPAA was enacted in 1996 and aimed to provide privacy protections related to individuals' health information. HITECH, on the other hand, was actually part of a much larger piece of legislation (The American Recovery and Reinvestment Act of 2009) that was enacted to stimulate the American economy during the Great Recession. To do this, HITECH provided (and still provides) subsidies for companies that invest in new healthcare technologies that lead to improved patient outcomes.

Notwithstanding its fiscal focus, HITECH did update some of the privacy protections of HIPAA, namely HIPAA's:

- Notification requirements in the event of a breach
- Restrictions on disclosing and selling health information
- Rules related to marketing

Because of this, any discussion of HIPAA is not complete without considering HITECH. Additionally, we want to ensure we provide a complete and accurate picture of these two legislations.

In this guide, we provide an overview of HIPAA and HITECH, which constitute the bulk of health data laws in the United States. Our goal is to enable you to meaningfully contribute to healthcare privacy-related discussions at your organization.



## Rights of Individuals

Under HIPAA, individuals have the following rights:

- Right to opt-out of marketing communications
- Right to access PHI
  - Psychotherapy notes
  - Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action/proceeding
  - PHI maintained by a covered entity that is
    - a. Subject to the Clinical Laboratory Improvement Amendments of 1988, to the extent that providing access of PHI to the individual would be prohibited by law
    - b. Exempt from the Clinical Laboratory Improvement Amendments of 1988
  - Individuals may obtain a copy of their PHI for as long as PHI records are maintained, except for:
- Right to an accounting of disclosures of PHI
  - Individuals may receive an accounting of disclosures of PHI made by a covered entity in the previous six years

# HIPAA & HITECH: Requirements

## Security Requirements

Organizations are to:

- Ensure the confidentiality, integrity, and availability of all electronic PHI, including:
  - Protect against any unpermitted uses or disclosures that can be reasonably anticipated
  - Ensure compliance with this by the organization's workforce
  - Flexibility on implementation is allowed depending on:
    - a. An organization's size, complexity, and capabilities
    - b. Their technical infrastructure, hardware, and software security capabilities
    - c. The costs of the security measures
    - d. The probability and criticality of potential risks to electronic PHI
  - Implement policies & procedures:
    - a. To prevent, detect, contain, and correct security violations, including:
      - 1. Risk analysis
      - 2. Risk management
      - 3. Sanction policy (against noncompliant workforce members)
      - 4. Information system activity review
  - Limiting physical access to electronic information systems and the facilities they're housed in, including:
    - a. Contingency operations
    - b. Facility security plans
    - c. Access control and validation procedures
    - d. Maintain documentation of security-related repairs and modifications to facilities (e.g., hardware, doors, locks, etc.)
  - Which workstations can access electronic PHI
  - Governing identity & access management for systems containing electronic PHI, limiting access to appropriate persons and software programs, including:
    - a. Unique user identification
    - b. Emergency access procedures
    - c. Automatic logoff
    - d. Cryptography
- To record and examine activity in systems containing/using electronic PHI
- As needed to comply with the rest of this Regulation



## Privacy Requirements

Covered entities are allowed to use or disclose PHI as follows:

- To the individual
- For treatment, payment, or health care operations
- Incident to a use or disclosure permitted/required by this part
- When required by the Secretary

Business associates are allowed to use or disclose PHI only as permitted in their contracts with covered entities (or as required by law). That said, associates must disclose PHI:

- When requested by an individual
- When required by the Secretary

Covered entities and business associates cannot sell PHI, except when disclosing PHI:

- For public health purposes
- For research purposes (where the only money received is a reasonable cost-based fee to cover the costs to prepare & transmit the PHI)
- For treatment and payment purposes
- For the sale, transfer, M&A, or consolidation of all (or part) of a covered entity and for related to due diligence
- To/by a business associate for activities it's undertaken on behalf of a covered entity, and the only money received is given by the covered entity for the performance of the activities
- To an individual when requested
- Required by law
- For any other purpose permitted by and in accordance with the applicable requirements of this subpart, so long as the only compensation received is a reasonable, cost-based fee to cover the cost to prepare & transmit the PHI

Health plans may not disclose genetic information for underwriting purposes, except for:

- Determining eligibility for benefits under the plan, coverage, or policy
- Computing the premium or contribution amounts under the plan, coverage, or policy
- Applying any pre-existing condition exclusion under the plan, coverage, or policy
- Other activities related to creating, renewing, or replacing a health insurance/benefits contract
- Underwriting does not include determining medical appropriateness when an individual seeks a benefit under a plan, coverage, or policy

## De-Identifying Health Information

### How to De-identify Health Information

In order to make identifying an individual through health information (reasonably) impossible, organizations may choose to de-identify health information. Health information is deemed to be de-identified only if:

- A person with appropriate knowledge of and experience with generally accepted statistical/scientific principles and methods for rendering information not individually identifiable:
  - Applying such principles/methods determines that the risk is very small that the information could be used (alone or in combination with other reasonably available information) to identify an individual; and
  - Documents the methods and results of the analysis that justify such determination

The steps to de-identify health information are as follows:

The following identifiers of the individual (or their relatives, employers, or household members) are removed:

- The geographic unit formed by combining all zip codes within the same three initial digits contains more than 20,000 people; and
- The initial three digits of a zip code for the areas containing 20,000 or fewer people is changed to 000
- DOB
- Admission date
- Discharge date
- Date of death
- All ages over 89 and all elements of dates (including year) indicative of such age, unless such ages/elements may be aggregated into a single category of 'age 90 or older'





The Secretary of DHHS may audit covered entities and business associates to ensure they are complying with HITECH and HIPAA. Organizations must comply with these audits.

The following identifiers of the individual are removed (continued):

- Names
- All geographic subdivisions smaller than a State (including street address, city, county/precinct, zip code (except for the first three digits) and other equivalent geocodes) if:
- All elements of dates (except for the year) directly related to an individual, including:
- Telephone numbers
- Fax numbers
- Email addresses
- SSNs
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- URLs
- IP address(es)
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code (except as permitted by paragraph (c) of this section)

#### How to Re-identify Health Information

To enable de-identified information to be re-identified, a covered entity may assign a code (or something similar) to a record, so long as the code is not:

- Derived from or related to information about the individual
- Capable of being translated to identify the individual
- Used or disclosed for any other purpose

#### Audits

The Secretary of DHHS may audit covered entities and business associates to ensure they are complying with HITECH and HIPAA. Organizations must comply with these audits.



## Breach Notifications

HITECH expects organization to take reasonable steps to detect breaches. This means an organization can't justifiably claim a notification wasn't made because the breach was undetected if there were reasonable steps the organization could have taken that would have led to the discovery of the breach.

### Circumstances Where Notification is Required

Covered entities or business associates who interact with PHI in the following ways must notify each individual whose PHI has been (or is reasonably believed to be) impacted by a discovered breach within 60 calendar days:



In short, if an organization interacts with PHI and that PHI is involved in a breach, that organization is required to notify the individuals impacted by the breach.

### How to Notify Individuals, the Media, and the Secretary of the US Department of Health and Human Services (DHHS)

In notifying individuals, organizations are to send notification via either first-class mail or if a mailing address is not available for the individual:

- Email
- Phone number
- Easily noticeable statement on the organization's homepage

If a breach involves more than 500 residents in a given State/jurisdiction, the organization must notify prominent media outlets in the affected area.

Organizations are to notify the Secretary of DHHS each year of all breaches involving PHI, unless the breach involves more than 500 individuals. In that situation, the Secretary is to be notified immediately. The Secretary also keeps a list identifying each covered entity involved in these large breaches on the DHHS's website.



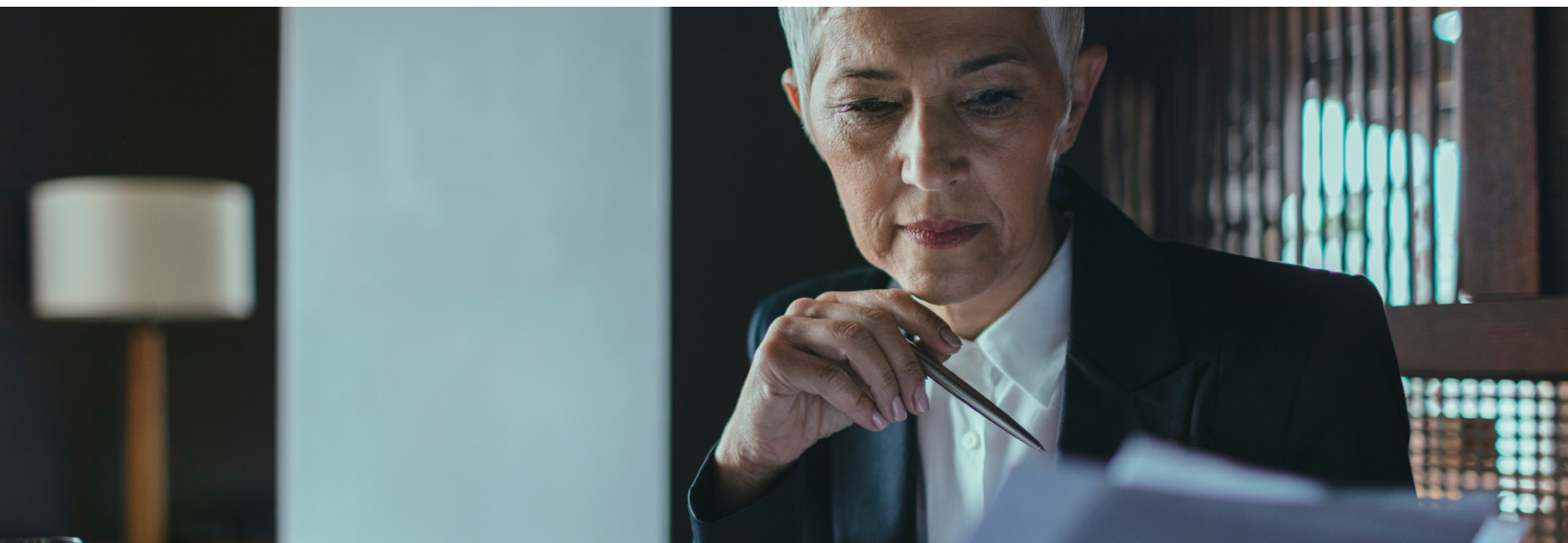
### Information to be Included in a Notification

Regardless of how individuals are notified of a breach, the notification is to include (to the extent possible):

- A brief description of what happened, when it happened, and when it was discovered
- A description of the types of unsecured PHI involved. For example:
  - Full name
  - Social security number
  - Date of birth
  - Home address
  - Account number
  - Disability code
  - Etc.
- The steps individuals should take to protect themselves from potential harm resulting from the breach
- A brief description of what the covered entity is doing to investigate the breach, mitigate losses, and to protect against any further breaches
- Contact information individuals can use to ask questions or learn additional information, which is to include a(n):
  - Toll-free number
  - Email address
  - Website
  - Postal address

### Notifications and Law Enforcement

If a law enforcement official determines that a notification of a breach would impede a criminal investigation or cause damage to nation security, notifications of the breach are to be delayed.



## Fines

### Important Definitions Related to Violations & Fines

As used in this subpart, the following terms have the following meanings:

#### REASONABLE CAUSE

- An act or omission in which a covered entity or business associate knew (or should have known) was in violation of this act, but in which the covered entity or business associate did not act with willful neglect

#### REASONABLE DILIGENCE

- The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances

#### WILLFUL NEGLIGENCE

- Conscious, intentional failure or reckless indifference to the obligation to comply with this act

### When Fines Can be Levied

- If a covered entity or business associate has violated HIPAA, the US Government can impose a monetary fine on the offending organization
- If a violation is committed by more than one covered entity or business associate:
  - Each offending organization can be fined
  - If a covered entity is part of an affiliated covered entity, the affiliates are jointly liable unless it's found that a member of the affiliation was responsible for the violation
- A covered entity will be found in violation of HIPAA even in situations where the violation was committed by any of the following acting within the scope of the covered entity:
  - An agent of the covered entity
  - A workforce member
  - Subcontractor
  - Business associate

## Fine Amounts

Fines can be up to the following amounts:

- For a violation where the covered entity or business associate did not know (and would not have known through reasonable efforts) they were in violation:
  - Between \$100 - \$50,000 per violation
  - No more than \$1,500,000 for identical violations during a calendar year (i.e., January 1 - December 31)
- For a violation stemming from reasonable cause and not willful neglect:
  - Between \$1,000 - \$50,000 per violation
  - No more than \$1,500,000 for identical violations during a calendar year
- For a violation stemming from willful neglect and were corrected within 30 days (from discovery of the issue) or should have known the violation occurred:
  - Less than \$10,000 or more than \$50,000 for each violation
  - No more than \$1,500,000 for identical violations during a calendar year
- For a violation stemming from willful neglect and that was not corrected within 30 days (from discovery of the issue) or should have known:
  - Min. of \$50,000 for each violation
  - No more than \$1,500,000 for identical violations during a calendar year
- If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another provision, a civil money penalty may be imposed for violating only one of the provisions

## What Your Organization Can Do

In order to comply with HIPAA & HITECH, your organization should:

- Consult with the appropriate experts, including your organization's legal counsel, to determine if HIPAA & HITECH applies to your organization
- Assess if your organization is currently handling PHI
- Implement a process so if your organization begins handling PHI, your organization can be HIPAA & HITECH compliant the first day it begins handling that information
- Have your personnel read our compliance articles on HIPAA & HITECH

## HIPAA & HITECH: Third-Party Risk Management



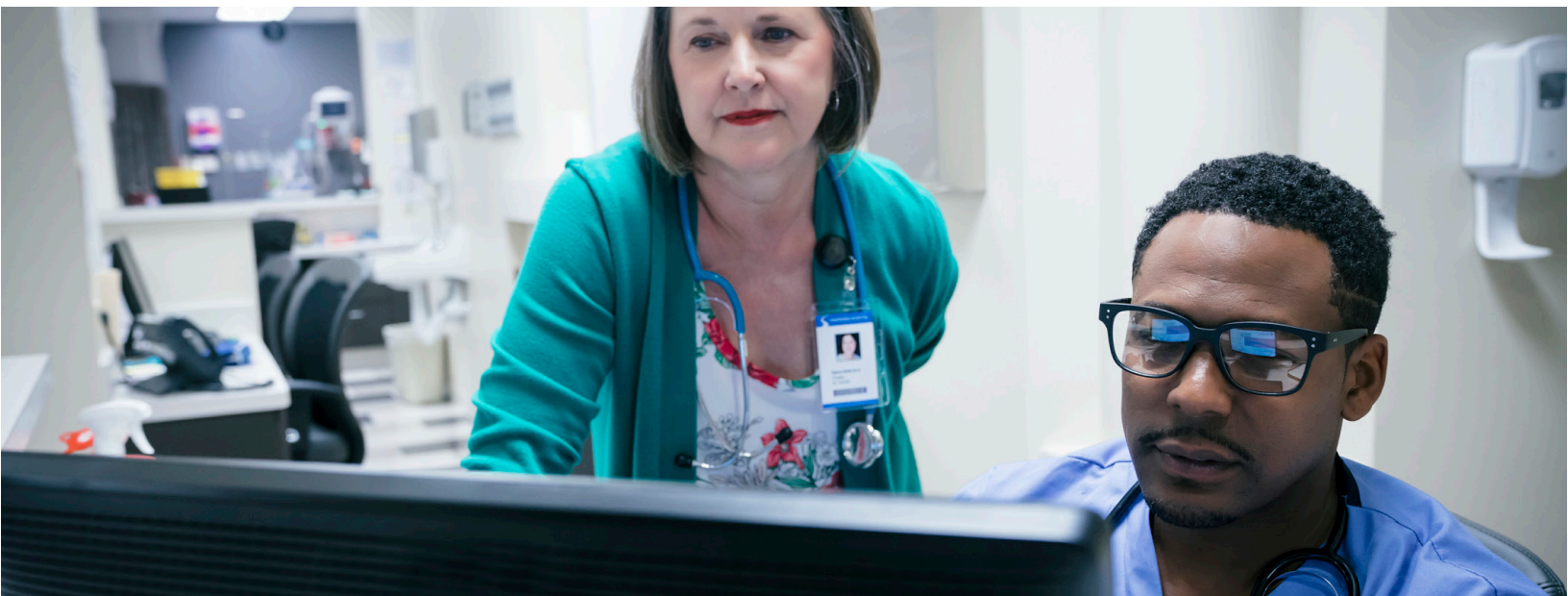
“RiskRecon helps maximize our efficiency with continuous, automated vendor assessment and tracking.”

—NATIONAL HEALTHCARE ORGANIZATION

Health information is regarded as highly private data by many individuals. The unauthorized disclosure of health data can, and has, caused individuals to suffer personal embarrassment, identity theft and worry. In an effort to keep health information private, especially as health records have become digitized, the US government has enacted two laws over the past 25 years: HIPAA and HITECH.

One risk facing organizations' security & privacy programs are their third-parties. Many third-parties have access to sensitive data, including health data, and if these entities don't have good security programs, they can present unnecessary risks to your organization. In this article, we discuss both what HIPAA & HITECH require of third parties and what you can do to proactively protect the health data your organization has been entrusted with.





## Important Definitions

### Covered Entity

A covered entity is any health plan, healthcare provider who transmits any health information in electronic form in connection with a transaction or healthcare clearinghouse (i.e., an organization that processes health care-related transactions or non-standard data).

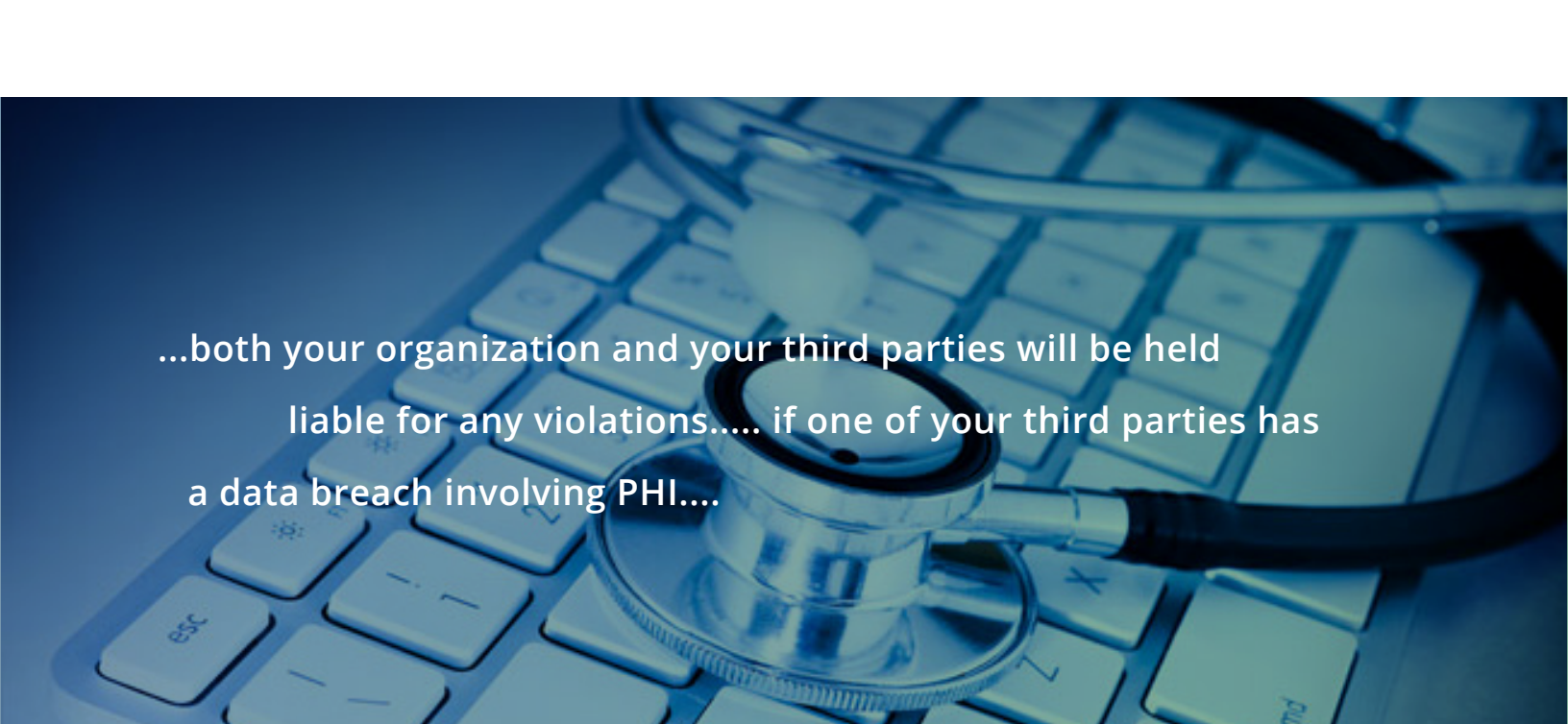
### PHI

PHI stands for “protected health information.” PHI is individually identifiable health information that is transmitted or maintained in any medium, physical or digital; however, PHI is excluded from education records covered by FERPA, in employment records held by a covered entity in its role as an employer and regarding any person who has been deceased for over 50 years.

### What Counts as a Third-party

Under HIPAA & HITECH, a third-party is referred to as a “business associate” (we will use “third-party” and “business associate” synonymously throughout this article).

Under these laws, a business associate is defined as any health information organization, e-prescribing gateway or other person that provides data transmission services involving PHI to a covered entity on a routine basis; a person that offers a personal health record to at least one other individual on behalf of a covered entity; or a subcontractor that creates, receives, maintains or transmits personal health information on behalf of a business associate. A business associate, however, does not include health care providers in regards to disclosures by a covered entity to a health care provider regarding an individual's treatment; a plan sponsor in regards to disclosures to the plan sponsor by the group health plan, health insurance issuer or health maintenance organization; a government agency that determines eligibility for, or enrollment in, a government health plan or the collecting of health information related to determining eligibility for or enrollment in a government health plan; or a covered entity if it participates in an organized health care arrangement that provides a function or services as described above.



...both your organization and your third parties will be held liable for any violations..... if one of your third parties has a data breach involving PHI....

## Requirements

In short, your third-parties must comply with both HIPAA & HITECH if they meet the requirements (as defined above) for a business associate. There are, however, some important requirements to note:

### Violations, Data Breaches and Notifications

Both your organization and your third-parties are required to take reasonable steps to detect breaches. This means an organization can't justifiably claim a notification wasn't made because the breach was undetected if there were reasonable steps the organization could have taken that would have led to the discovery of the breach.

If either your organization or your third party suffers a data breach involving PHI, the organization that suffered the data breach must notify each affected person whose PHI has been (or is reasonably believed to have been) impacted by the breach within 60 calendar days.

Notwithstanding, both your organization and your third-parties will be held liable for any violations (including data breaches) and potentially subject to fines (e.g., if one of your third parties has a data breach involving PHI, both your organization and your third party could be fined).

### Disclosure or Use of PHI by Third Parties

Third-parties are to only disclose or use PHI as is allowed in the contract with your organization and required by law. Law requirements include disclosing PHI when an individual requests their PHI and when the Secretary of the Department of Health and Human Services (who is responsible for enforcing HIPAA and HITECH) requires such disclosure or use.



## The Sale of PHI

Neither your organization nor your third parties may sell PHI, except when disclosing PHI for public health purposes; for research purposes where the only money received is a reasonable cost-based fee to cover the costs to prepare and transmit the PHI used in the research ; for treatment and payment purposes; for the sale, transfer, merger and acquisition or consolidation of all (or part of) a covered entity, including for the purposes of due diligence; either to or by a business associate for activities it's undertaken on behalf of a covered entity and the only money received is given by the covered entity for the performance of those activities; to an individual when requested; as required by law; and for any other purpose permitted by and in accordance with the requirements of HIPAA & HITECH so long as the only compensation received is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI.

## What Your Organization Can Do

There are several things your organization can do to comply with HIPAA & HITECH, including consulting with appropriate legal counsel and other experts to determine how HIPAA & HITECH apply to your organization; ensuring your organization only works with third-parties who are able to adequately protect PHI and comply with both of these regulations; reviewing vendors' security posture on at least an annual basis; for vendors who are critical to your organization in complying with HIPAA and HITECH, conducting more frequent but less-intensive reviews than the annual review (but still doing annual, in-depth reviews) of the third-parties' compliance & security programs such as continuous assessments, quarterly or semi-annually; and partner with your vendors and work together to improve both of your organization's security and compliance programs.