HIPAA ASSOCIATES

# WHAT TO DO AFTER A BREACH

## *A Crisis Management Toolkit*

# *You're in the right place.*

If you've experienced a breach, time is of the essence. The US Department of Health and Human Services will expect a thoroughly prepared report on how it happened, and what you're doing to prevent it from happening again. If you've already received a letter from HHS Office for Civil Rights (OCR), you'll have 10 days to 2 weeks to respond to them.

This can be a very stressful process , and you may not even be sure where to start. That's why we've created this toolkit. We've detailed all the steps you'll need to take so you can get your report - **and your peace of mind** - on track as soon as possible. This toolkit will enable you to work effectively with your team, and get all all the information HHS is expecting from you gathered in one place.

You've taken a great first step by getting this toolkit and making yourself a plan of action. Breach reporting is our top service - we've helped countless organizations, large and small. If at any time during the process you start to feel overwhelmed, unsure, or just need some hand-holding, don't hesitate to give us a call.

Your partners in protecting your patients,

Mary + Al Lopez

## WHERE TO FIND US

hipaa-associates.org

hipaasupport@hipaa-associates.org

/hipaa-associates

## LEGAL

# Table of *Contents*


**IMMEDIATE HELPERS**

5 Important Numbers

6 To Do Checklist

**PART 1 : BREACH INCIDENT, INCIDENCE RESPONSE, AND MITIGATION PLAN**

8 About: Breach Incident, Incidence Response, and Mitigation Plan

10 Breach Incident worksheet

11 Response Team worksheet

12 Mitigation Plan worksheet

**PART 2 : NOTIFYING THE PUBLIC**

13 About: Notifying the Public + Those Affected

15 Notification worksheet

**PART 3 : NOTIFYING HEALTH & HUMAN SERVICES, ROOT ANALYSIS + FOLLOW-UP**

16 About: Notifying HHS (how, and when)

18 About: Root Cause Analysis + Follow-up

# Important Contacts

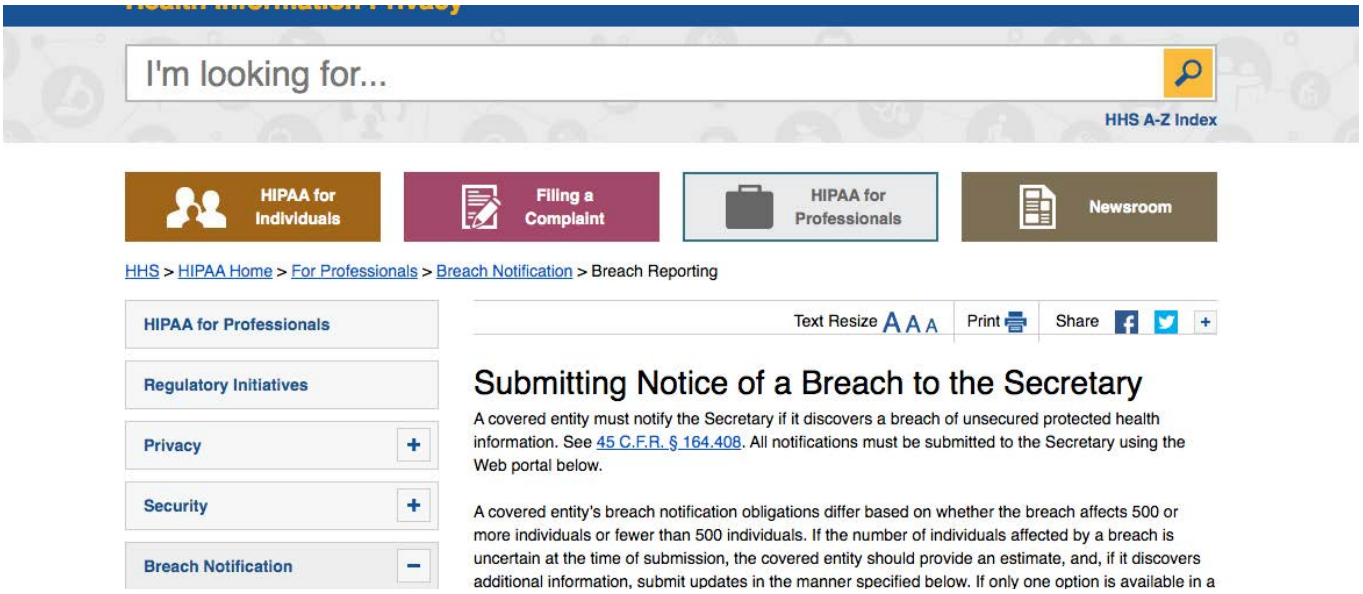
## Office of Civil Rights

800.368.1019

ocrprivacy@hhs.gov

hhs.gov (click to visit)

hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index/html



# To Do List

Each one of these items must be completed after a breach. Detailed explanations follow, but you can track what you've done (and what needs to be done) right here.

## Breach Incident

- ☐ Date of Determination
- ☐ Deadline for notice to individuals affected
- ☐ Actual or estimated number of individuals affected determined
- ☐ Form Incident Response Team
- ☐ Mitigation plan
- ☐ Security or credit monitoring at no cost set up

## Notification of the Public/Individuals Affected

- ☐ Notification posted on website
- ☐ Toll-free number established + made public
- ☐ PR Statement written/distributed to media
- ☐ Notice letter sent to all affected individuals
- ☐ Alternate forms of delivery/substitute notice

## Notice to HHS, Root Cause Analysis + Follow-ups

- ☐ breach report submitted to HHS (date of report:_____)
- ☐ company hired and/or strategy for root cause analysis
- ☐ follow-up planned (re-training of staff, etc.)

# Notes

# SECTION 1

*Breach Incident, Incidence Response + Mitigation Plan*

# About: *Breach Incident Incidence Response + Mitigation Plans*

**In a breach, the first step is determining when the breach occurred**, or the date of determination (also called "discovery date"). This date begins a countdown to the date by which you must issue a mandatory report to the US Department of Health & Human Services, Office of Civil Rights (OCR). There is more about discovery dates on pages 16-17.

The next important step is figuring out how many people have been affected, because the number of individuals involved determines how your organization will submit the breach report and notify them. Here are the OCR Guidelines on breach reporting:

- for breaches of 1-499 individuals, breach must be reported to OCR on an annual basis no later than 60 days after the end of the calendar year.
- for breaches of more than 500 individuals, breach report must be submitted to OCR no later than 6o days following a breach.

## Then, it's time to assemble your response team. It should include:

**Information Security Officer:** It's essential to have an information security officer as part of your response team, someone to analyze the breach of information and develop corrective actions. This privacy officer will have the responsibility of collecting all information and formulating a re-sponse for the breach.

**Legal:** In addition to an information security officer, asking a member of the legal team to participate is advisable to interpret the intricacies of the law regarding the breach reporting process.

**Risk management** is often of great help as your organization attempts to determine the implications of the breach.

**Public Relations:** You'll need a PR professional as the breach becomes public. It will be important for your organization to be transparent and show you're are doing everything possible to mitigate the breach. You'll also need someone who can calmly, professionally answer calls + questions from the press, the public, and other stakeholders.

**Others:** There may be other groups in your system that could be part of your incident response team depending on the circumstances of the breach. Consult with the team members above to see who else you should bring into the fold. Or, feel free to call us and we can advise who else you might need.

## Mitigation

OCR will expect you to mitigate the damage the breach has caused. In most cases, credit monitoring should be offered at no cost to the individuals who've been affected by the breach. Other measures may also need to be considered. Speak with your team about this - each of them can offer a different perspectives that will help your organization as a whole.

# Breach Incident Worksheet

**Use this page to keep track of information you'll need for your own records, and for breach reporting purposes.**

Date of Determination: _____

Deadline for notice to individuals affected: _____

## *Notes*

# Incident Response Team

## Information Security Officer

Name _____

Phone Number_____Email _____

## Privacy Officer

Name _____

Phone Number_____Email _____

## Legal

Name _____

Phone Number_____Email _____

## Risk Management

Name _____

Phone Number_____Email _____

## Public Relations

Name _____

Phone Number_____Email _____

## Others/Notes

# Mitigation Plan

Will security or credit monitoring be provided at no cost? ☐ Yes ☐ No

If yes, name of provider: _____

Contact person for provider: _____

phone: _____ email: _____

## *Notes*

# SECTION TWO

*Notification of the Public + Those Affected*

# Notifying the Public

Notifying the public - so that they can take appropriate steps - is a vital part of maintaining trust in your organization. It's also a requirement: HHS-OCR will expect you to have taken specific steps, and to be able to report exactly how and when you took those steps. Let's take a look at them.

## Notice Letter

You'll need to create and send a notice letter by US mail (or via email, if they've asked to be notified that way vs. paper) to anyone who's been affected by the breach. It's critical to note the date you sent this letter, because OCR will ask for it. In some cases - because people move around - an alternate form of delivery must be used to notify people of the breach. This could include phone calls or other means. You'll need to keep a record of each instance you've used an alternate form of delivery. If contact information for 10 or more individuals is out of date, you'll have to complete what's called a substitute notice. This could be notice by major print or broadcast media in the area(s) where these people likely live, or a notice on the home page of your site. All of the data around the substitute notice (who got one, when, and how) has to be recorded as well.

This is a point at which many people become overwhelmed. The Office of Civil Rights is looking for specific language around specific steps they will expect you to take. In short, they want to be assured that you're doing right by the patients affected by the breach. If you're starting to feel lost, give us a call. We've helped countless organizations through this process, and speak this language. We'll make sure you're on track, and that OCR has what they need to keep your organization in good standing.

## Website

You'll need have a dedicated space on your site where people can access information about the breach, and learn that it's occured. The primary location for a notice should be your home page, and the notice should be active for at least 90 days. And, you guessed it - you'll need to document where, how and when you did it.

## Toll-free number

You'll be required to set up a toll-free number that people can call and get information about the breach, and learn if they've been affected. It will need to be active for at least 90 days. If you need help on exactly how you do this, call or email us - we have several vendors and methods we can recommend for getting this number up and running.

## Media Notice

This is where your PR professional will come in. You'll need for a notice to be written and distributed to the media - especially if your case involves more than 500 individuals. As with everything else, all of the details surrounding the notice - what, when, how - must be recorded in accordance with OCR rules.

# Notification Worksheet

**Notice Letter Status:** ☐ draft ☐ in review ☐ published/ready

Date notice letter mailed: _____

Was notice delivered by other means? If so, list here: _____

_____

_____

**Substitute Notice** (if insufficient or out of date contact information for 10 or more individuals)

Date: _____

Method(s): _____

## Website Notice

Date posted: _____ URL: _____

Method (screen takeover? home page? etc.): _____

## Media Notice

Contact person: _____

Phone: _____ Email: _____

Sent date: _____

## Toll-Free Number

Name of provider/service for number: _____

Contact person for this vendor: _____

And what is the toll-free number? _____

# SECTION THREE

*Reporting to HHS,*
*Root Cause Analysis*
*+*
*Follow-ups*

# Reporting to Health & Human Services

## Timing is everything

Under HIPAA, a breach is considered "discovered" by a covered entity (that's you) on the first day a breach is known, or would have been known, by the covered entity (you). Further, the dates of an investigation, and/or its completion have no bearing on the HHS reporting clock. Keep in mind also that a breach can be discovered by anyone within your organization, and as far as HHS is concerned, whether upper management knows or not does NOT factor into the calculation of when you must report to HHS.

**Let's look at a hypothetical scenario** to illustrate what we're talking about. Say you have an IT employee - Jack - who's making a routine check on January 1, 2019. During his check, Jack discovers his organization has had a breach. He emails his boss, Bob, but Bob is on vacation (it's New Year's, after all). Jack tries calling, but gets Bob's voicemail. Bob finally gets the message the next day, on January 2. Bob sends it up the chain of command, and the CEO doesn't know about the breach until January 3. An investigation is immediately launched. By around January 8, it's learned how the breach happened, and how many were affected. As far as HHS is concerned, the most important date is: January 1, 2019. That's the day the clock started ticking.

There are different timelines for different scenarios, which we cover next.

## For Breaches of 1 to 499 Individuals

If a breach of unsecured protected health information affects fewer than 500 individuals, you must notify the Secretary of Health and Human Services (HHS) of the breach within 60 days of the end of the calendar year in which the breach was discovered (not occured).

**Example:** if your breach is discovered on January 1, 2019, you have at the latest until March 2, 2020, to report your breach to HHS.

However, you don't have to wait.

You can report breaches immediately (and this is what we recommend). The sooner you report, the easier it is to restrict the damage to those affected.

(cont'd)

## For Breaches of 1 to 499 Individuals (cont'd)

You can also report multiple breaches at one time, but each incidence requires a separate report (they can't all be lumped together).

**Example:** you have a breach (A) on January 1, 2019, then another (B) on March 2, 2019, then nothing else for the rest of the year. You can report both of them together as late as March 2, 2020, but have to file a report for A and B separately.

Click here to access the HHS reporting portal for a breach of fewer than 500 individuals.

## For Breaches of Over 500 Individuals

If a breach of unsecured protected health information affects 500 or more individuals, a covered entity (again, that's you) must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach.

**For example**, if you discover a breach on January 1, 2019, you must submit your report no later than March 2, 2019.

Click here to to access HHS reporting portal for a breach of more than 500 individuals.

What does "unreasonable delay" mean? It depends on a variety of factors and is somewhat subjective. In some cases, even reporting at the 60-day mark could be considered "unreasonable." That's why - aside from protecting the people who've been affected - you should make the report as soon as possible. This is also why it's important to have legal counsel with expertise in HIPAA law on your team. They'll be able to tell you what your time limits may be, among other things.

## For All Breaches

Reporting to Health and Human Services Office for Civil Rights is submitted electronically.

Click here to access the HHS reporting portal for a breach of fewer than 500 individuals.

Click here to to access HHS reporting portal for a breach of more than 500 individuals.

**Don't forget:** you must also keep track of what date you've reported your breach(es) to HHS.

**How did this happen?** This will be the question everyone will want answered, followed quickly by: How can we prevent this in the future?

This is why you must complete one of the most important steps of this process:

## Root Cause Analysis

A root cause analysis will look at the breach from lots of different angles, and answer questions such as:

- what are internal policies and procedures? Where are the weaknesses?
- who accessed, used, or received the PHI (protected health information)?
- what was the nature of the PHI?
- who were the staff involved? What were the events surrounding the breach?

This is also a point at which we recommend you hire a professional. This will protect you in multiple ways:

- the company you hire is independent, able to see things with fresh eyes, and free from internal politics.
- failure to adequately address the breach can result in enormous fines - hundreds of thousands of dollars, or in some cases, millions.
- professionals who deal with HIPAA compliance know the pitfalls and blind spots. Without a professional, you may have additional HIPAA violations waiting to happen (or in process), that you never even considered.

In short, an independent, contracted company can act as a “red team” by auditing what you did, what you’re doing, and what you’re planning to do.

## Follow Up

Depending on how bad the breach was, you may have follow-up action items such as paying penalties, or re-training your staff to prevent future violations.

If you’re in need of help with training, root cause analysis, or anything else HIPAA-related, we’d love to work with you - just give us a call or shoot us an email.

# You did it. *Now what?*

You've made it through the breach.

Or maybe you're thumbing through this packet, assessing everything you need to do.

## Either way, we'd love to help you.

Mary is a former nurse and a lawyer. Al is a pulmonary critical care specialist, anesthesiologist, and medical coding specialist. They both have decades of experience as compliance officers, and with HIPAA security+ operational issues.

As people who've worked on both sides of HIPAA – as care givers and compliance officers – we're well positioned to create individualized programs to fit your needs. Both large multi-hospital organizations and smaller companies seek our services, and since the advent of HIPAA we've trained thousands of healthcare providers in person or through our web-based platform. We can even add your company's branding to our customizable training modules, if you like, and we also offer HIPAA training for Spanish speaking associates.

We've helped numerous organizations and individuals with:

- HIPAA Consulting on the HIPAA Rules
- HIPAA Gap Analysis - what are your weaknesses? Find out and prevent future breaches.
- Breach Reporting, investigation, analysis, individual notification and Office for Civil Rights reporting
- HIPAA compliance training
- Privacy and security policies and procedures for HIPAA
- HIPAA Security Analysis
- Investigation and response to HIPAA complaints
- On-site HIPAA audits
- Response to Office for Civil Rights investigations
- Business Associate Agreements

We've been doing this since HIPAA became law, and can help you protect your organization and your patients.

Call us, email us, or explore our site for additional information.

hipaa-associates.org

hipaasupport@hipaa-associates.org