

MEDCURITY

# CONTINUITY PLANNING AND HIPAA

Preparing for and responding to natural  
disasters and other emergencies



# TABLE OF CONTENTS



## **Section 1:**

What is a Business Contingency Plan?	3
How Can You Follow HIPAA During a Disaster or Emergency?	3
What Provisions of HIPAA Can be Waived During an Emergency?	4
When and to Whom do These Waivers Apply to?	5

## **Section 2:**

What Are You Required to Include in Your BCP?	6
What are Addressable Aspects?	7
How Should I Create a BCP?	8
When Should I Activate my BCP?	8

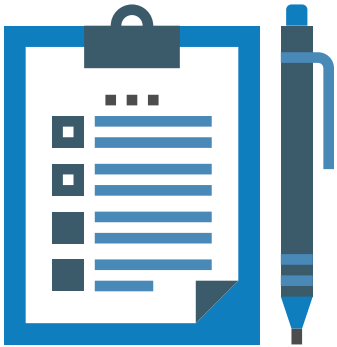
## **Section 3**

What if Your Hospital Was Hit by a Hurricane?	9
What You Should Do and Plan For if You Lose Access to Your Building	9
What You Should Do and Plan For if You Lose Access to Your Workforce	10
What You Should Do and Plan For if You Lose Access to Your IT Systems	11
What You Should Do and Plan For if You Lose Access to Your Supply Chain	12

## **Checklist**

Seven Steps to Take for a Successful BCP	
--	--

## Section 1 | **What is a Business Contingency Plan (BCP)?**



A Business Contingency, or Continuity Plan is a well-coordinated plan that outlines how to continue vital operations after a disaster or disruption to your organization. The goal of a BCP is to reduce the risk of financial loss to your hospital and increase the ability to quickly recover from a disaster.

## **How Can You Follow HIPAA During a Disaster or Emergency?**

HIPAA may not be the first thing on your mind during a natural disaster, but it's still a crucial element that health officials must follow amidst an emergency situation. Through staff education and proper preparation, health care organizations can navigate emergency situations while avoiding HIPAA breaches.

Many questions regarding compliance arise during a disaster, such as how covered entities will follow HIPAA regulations on sharing and protecting personal health information.

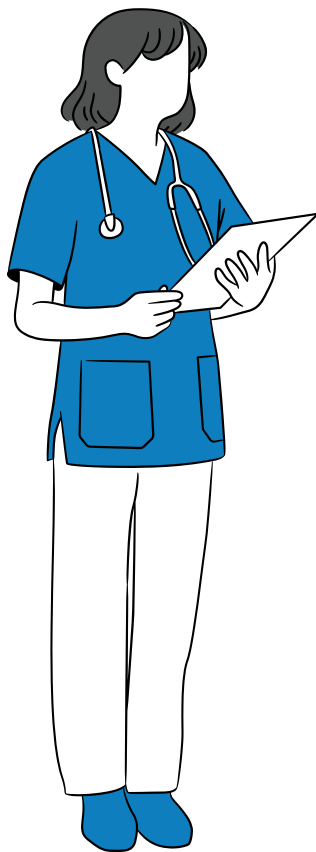
This section will address the compliance standards covered entities must meet during a disaster. The HIPAA Privacy Rule details how patient information can be shared, and how patients can receive the care they need in an emergency situation while still following compliance regulations.

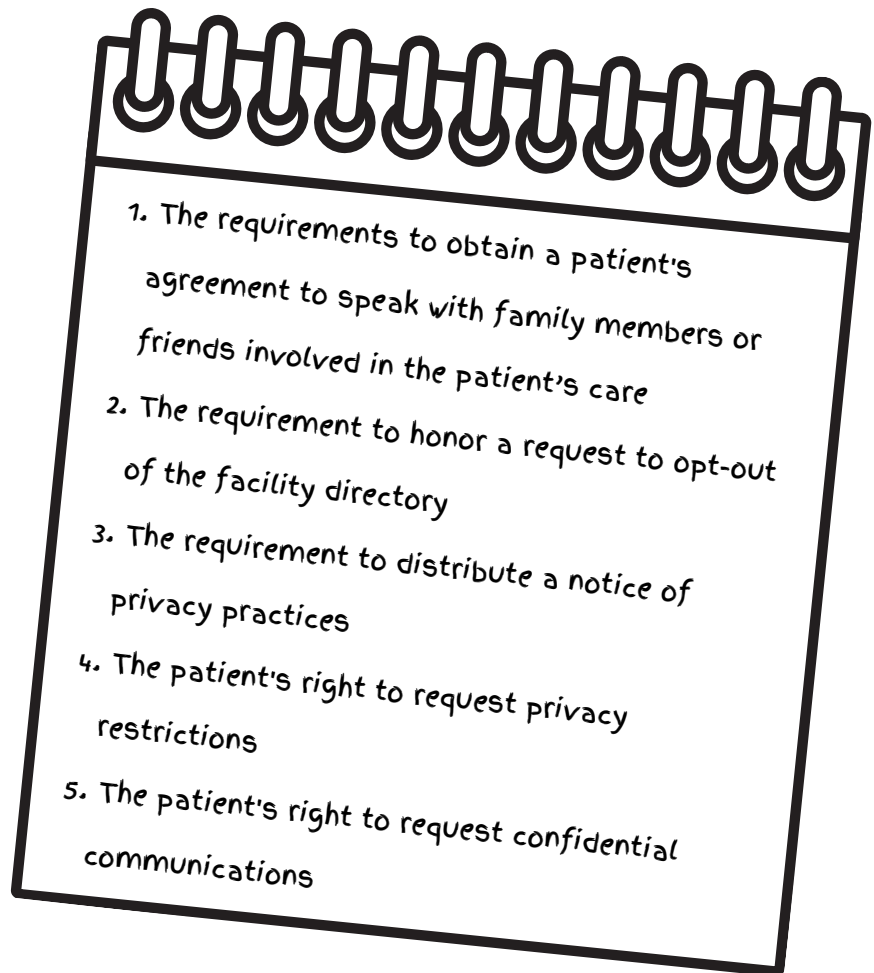
# What Provisions of HIPAA can be Waived During an Emergency?



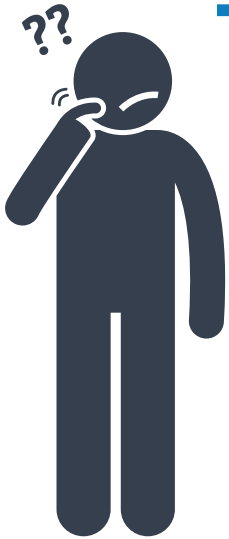
If the U.S. President declares an emergency or disaster or the Secretary of State declares a public health emergency, then the Secretary may waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the HIPAA Privacy Rule.

## The Provisions That May be Waived Include:



- 
1. The requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care
  2. The requirement to honor a request to opt-out of the facility directory
  3. The requirement to distribute a notice of privacy practices
  4. The patient's right to request privacy restrictions
  5. The patient's right to request confidential communications

# When and to Whom do These Waivers Apply to?



## **Whatever the Secretary chooses to waive only applies:**

- To the emergency area and for the period of time as identified by the public health emergency declaration
- To hospitals that have instituted a disaster protocol and,
- For up to 72 hours from the time the hospital implements its disaster protocol.

As soon as the President or Secretary of State terminates the emergency declaration, a hospital must then return to complying with all aspects of the Privacy Rule, even if 72 hours has not passed since the start of their disaster protocol.

Regardless of the activation of an emergency waiver, the HIPAA Privacy Rule permits disclosures for treatment purposes and certain disclosures to disaster relief organizations. For instance, the Privacy Rule allows covered entities to share patient information with the American Red Cross so it can notify family members of the patient's location.





## Section 2 | **What Are you Required to Include in Your BCP?**

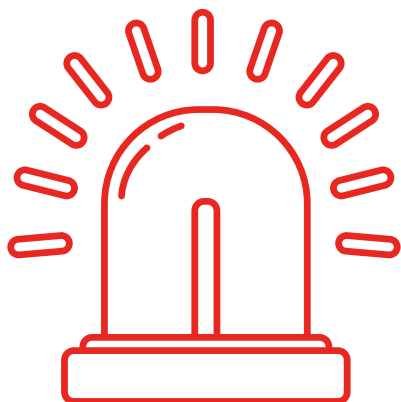


### **Data Backup Plan:**

A documented and routinely updated plan designed to help you retrieve exact copies of electronic Protected Health Information (e-PHI) for a designated period of time.

### **Disaster Recovery Plan:**

An IT plan focused on defining the resources, actions and data that are needed to reinstate essential business functions that have been damaged due to a disaster. It should include an inventory of all the critical data and vital systems as well as procedures detailing how to recover these systems at an alternate location.

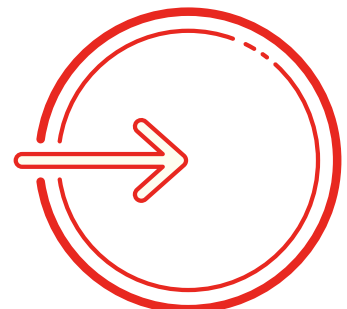


### **Emergency Mode Operation Plan:**

A plan that details how to continue operations in the event of a fire, vandalism, natural disaster, or system failure. The goal is to document the critical resources that will protect your hospital's essential functions if you lose access to all or part of your computer systems and/or electronic equipment due to a disastrous event.

### **Emergency Access Procedure:**

A document that details the procedures needed to gain or maintain access to e-PHI in the middle of an emergency. The goal is to reduce the risk of e-PHI being leaked or accidentally accessed by an unauthorized individual.



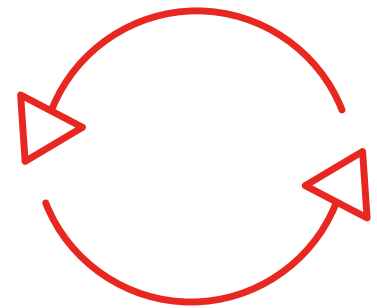
# What are “Addressable Aspects”?

Addressable aspects of a BCP are certain regulations that your organization may have to implement if they are deemed as reasonable necessities to protect PHI.

To determine whether you need these addressable specifications, your organization must perform an assessment to see if they are reasonable and appropriate precautions to take. Addressable aspects include:

## Testing and Revision Procedures

The process of periodically testing and revising your contingency plan to assess its strengths and weaknesses, allowing you to make any necessary changes.

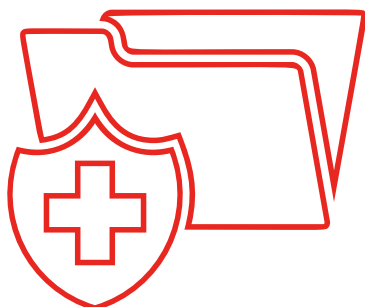


## Applications and Data Criticality Analysis

A formal assessment of the sensitivities, vulnerabilities, and security of your organization's programs and information it receives, manipulates, stores, and/or transmits.

## Contingency Operations:

Procedures that allow access to your facility with the goal of restoring lost data in the event of a disaster or emergency.



## Data Backup and Storage:

The process of creating a retrievable and exact copy of e-PHI, upon request before moving equipment. Backing up accurate data and having it stored in a safe place is an important aspect of this addressable requirement.



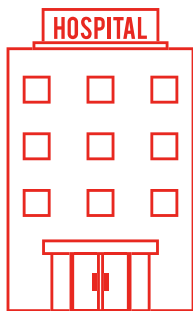
## How Should I Create a BCP?

A lot of people create BCPs by trying to prepare for all the possible things that could go wrong. Instead of focusing on the response plan, they focus on endless “what if” scenarios, causing unnecessary stress.

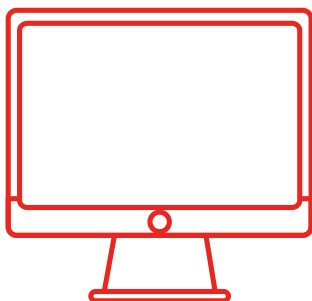
We recommend that you create a BCP that will help you recover from any potential problem. Pay attention to areas of your organization that would affect your critical business function if they were lost. By focusing on what you could lose rather than what kind of disaster could occur, you’re able to create a more solid plan that will be useful in various scenarios regardless of the problem.

## When Should I Activate My BCP?

You should activate your BCP if you lose access to any of the following:



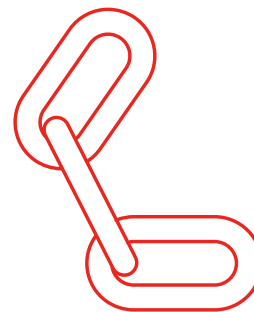
**BUILDING**



**IT SYSTEMS**



**STAFF**



**SUPPLY CHAIN**



## Section 3 | **What if your Hospital Was Hit by a Hurricane?**



Each of the following is a separate scenario showing what your plan should be if your hospital lost access to these areas of your organization.

### **What You Should Do and Plan For if You Lose Access to Your...**

#### BUILDING

**Problem:** The hurricane has led to flooding in your hospital, causing you to lose access to most of the rooms that are needed for essential patient care.

**Solution:**

- Discharge as many patients as safely possible to allow them to get to a proper shelter. This will keep your hospital from being overrun by patients and others seeking shelter and will allow you to care for chronically ill patients who need immediate attention.
- Give the few rooms left to the patients who need it most. Prioritize patient care in order of life-threatening importance with those who had scheduled appointments.
- Plan to reschedule appointments with those who are able to wait until the effects of the storm have subsided.
- Plan to reroute patients to another hospital, facility or resource if they need immediate emergency care that you cannot provide due to a shortage of rooms.
- Plan to evacuate your entire building if the hurricane is causing immediate danger to everyone in the hospital. Go to one of the predetermined locations laid out in your BCP plan.

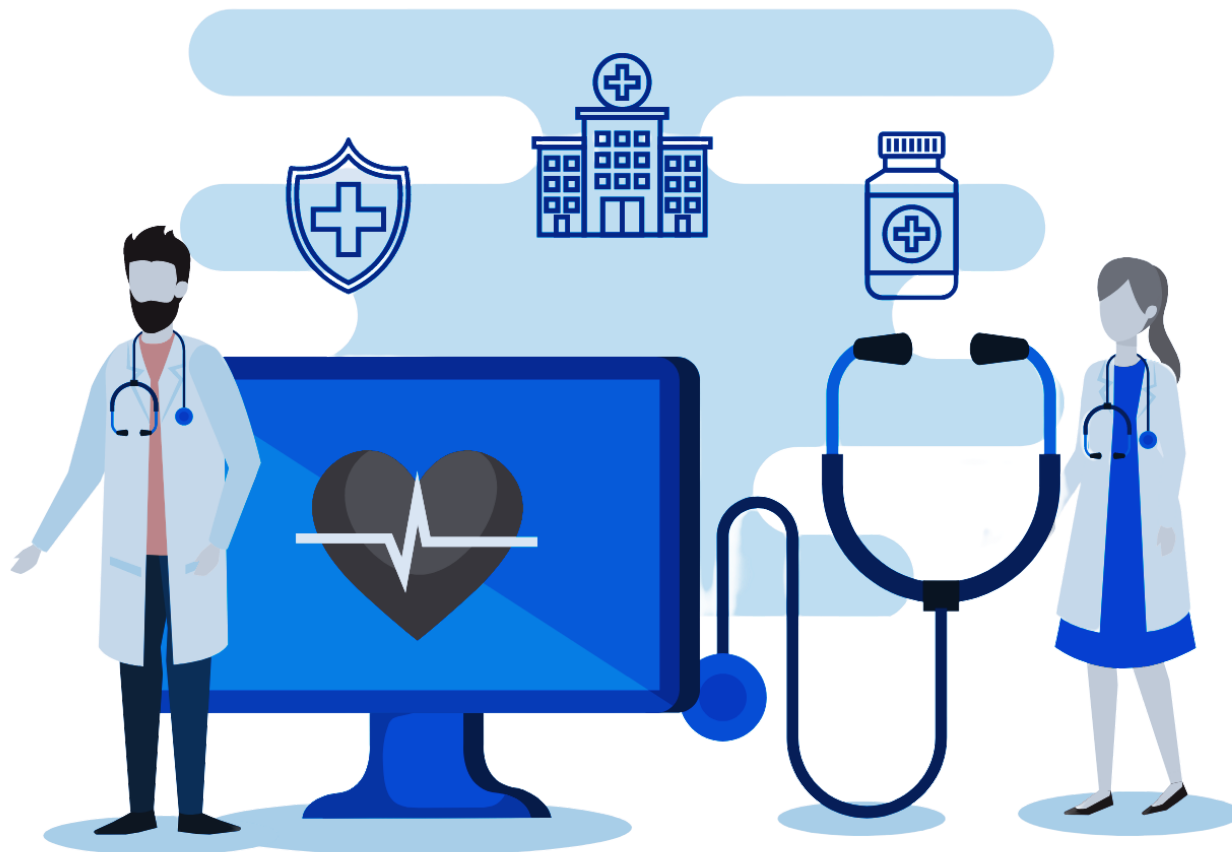


## WORKFORCE

**Problem:** Nearly half of your staff are unable to get to work due to severe flooding on main roads.

**Solution:**

- Plan to be able to maintain basic operations with less than half of your staff. To accomplish this, train all staff members who can work from home to be able to do so. This should be done beforehand and practiced throughout the year.
- Create solid BYOD (Bring Your Own Device) policies so that employees can use their own laptops, cell phones, etc. from home during a disaster scenario when they are unable to make it to the hospital.
- Train non-IT staff periodically throughout the year to be able to assist primary staff members, such as doctors and nurses, to be able to help them keep basic operations going. This way, even if the hospital is understaffed, you will still be able to maintain essential functions with the help of properly trained individuals.



## IT SYSTEMS

**Problem:** The high winds from the hurricane have caused the power to go out in your hospital. You have lost access to all major computer systems and electronic equipment. The hospital generator has powered all the essential equipment needed for urgent patient care, however not all computer systems are up and running.

### **Solution:**

- Have hard drive backups for all important electronic data, especially e-PHI, so that data can be retrieved later if it is lost from a system crash.
- Train your staff to be able to use paper records to maintain basic and essential operations.
- Create strong BYOD policies that focus on encryption so that employees can use their own phones to help with the continuation of essential work in the hospital.
- Create a procedure explaining how to enter information into EMRs once the system is up again, as that will ensure the information is secure.



## SUPPLY CHAIN

**Problem:** The hurricane is causing travel issues for several delivery trucks in your area, including the trucks that are carrying essential supplies your hospital needs to maintain basic operations.

**Solution:**

- Maintain on-site backup supplies your hospital needs to perform life-saving treatments for your chronically ill patients.
- Only conduct the most important and time-sensitive surgeries, and reschedule the rest for a date when your stock has been replenished.
- If you do not have enough supplies in storage, have a plan to re-route your most at-risk patients to hospitals that you have predetermined in your BCP.

# 7 STEPS TO TAKE

for a successful BCP as recommended by the NIST

1

## **DEVELOP A CONTINGENCY PLANNING POLICY STATEMENT**

A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

2

## **CONDUCT THE BUSINESS IMPACT ANALYSIS (BIA)**

The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business functions.

3

## **IDENTIFY PREVENTIVE CONTROLS**

Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

4

## **CREATE CONTINGENCY STRATEGIES**

Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

5

## **DEVELOP AN INFORMATION SYSTEM CONTINGENCY PLAN**

The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

6

## **ENSURE PLAN TESTING, TRAINING, AND EXERCISES**

Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

7

## **ENSURE PLAN MAINTENANCE**

The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.