A picture containing bird

Description automatically generated

****<CompanyLong>****

[Insert Policy Name]

[Add Client Logo and Branding Here]

Table of Contents

[Revision History 3](#_Toc58146985)

[Definitions 3](#_Toc58146986)

[Purpose 3](#_Toc58146987)

[Applies To 3](#_Toc58146988)

[Policy Statements 4](#_Toc58146989)

[Emergency Numbers and Resources 5](#_Toc58146990)

[Methods to Communicate Essential Information to Partners 5](#_Toc58146991)

[Methods to share protected patient information 6](#_Toc58146992)

[Primary and alternate means of communication 7](#_Toc58146993)

[Contact Information 8](#_Toc58146994)

[Messages 9](#_Toc58146995)

[Resources for Crisis Communications Center 10](#_Toc58146996)

[HIPAA in Emergency Situations: Preparedness, Planning, and Response 11](#_Toc58146997)

[Compliance 12](#_Toc58146998)

[Exceptions 12](#_Toc58146999)

[Appendix – Contact Grids 13](#_Toc58147000)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description of Change |
| 0.01 |  |  | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Definitions

|  |  |
| --- | --- |
| Term/ Acronym | Definition |
|  |  |
|  |  |
|  |  |
|  |  |

Purpose

The purpose of the Emergency Crisis Communication Plan is to establish policies, procedures, and guidelines for responding to a crisis or emergency that could threaten the health, safety, business objectives and mission of a health center. This may include crises or emergencies that are unpredictable and have unforeseeable consequences (i.e. physical and mental health emergencies; accidents; social, physical, or emotional distress; environmental events - severe weather or natural disasters, fires or explosions, extended power outages, cyber-attacks, terrorism, or acts of violence.)

The plan is the application of strategies designed to help an organization deal with these types of events, and helps to ensure quick resolution in efforts to minimize any disruption, damages, or consequences.

**Nothing in this plan should limit the exercise of good judgment and common sense in matters not covered or foreseen by the Emergency and Crisis Communication Plan.**

Applies To

This policy applies to anyone that has access to <CompanyLong> assets, systems, networks or devices.

Policy Statements

The Communication Plan associated with Emergency Preparedness and IRP should incorporate the following:

* Develop an emergency preparedness communication plan that complies with federal, state, and local laws
* Include:
  + Contact information – for relevant partners
  + Methods to communicate essential information with relevant partners
  + Methods to share protected patient information
  + Primary and alternate means of communication

## Contact information

### The communication plan should include:

Contact information (name and contact) for internal needs:

* Residents
* Staff
* Resident physicians
* Volunteers
* Service and resource entities under arrangement
* Over health care providers
* Local, state, regional and federal emergency preparedness staff
* State Department of Health and Human Services
* Local authorities
* Transfer entities
* Transportation entities
* Vendors and service providers
* ISP provider
* Cloud Provider

Information should be current, accessible and readily available

Emergency Numbers and Resources

## Local Numbers

* 911 - Emergency Medical Services (EMS)
* (More Local Numbers)

## National Numbers

* 911 - Emergency Medical Services (EMS)
* 211 - Resources and Assistance, a 24/7 free and confidential service that helps people find local resources they need
* 1-800-799-SAFE (7233) - National Domestic Violence Hotline - Trained advocates are available to take calls through 24/7 hotline
* 1-800-273-TALK (8255) Veteran's Crisis Line / National Suicide Prevention Lifeline
* 1-800-SUICIDE (784-2433) I’m Alive- National Suicide Hotline
* 1-800-662- HELP (4357) National Helpline
* 1-800-985-5990 Disaster Distress Helpline
* 1-800-442-HOPE (442-4673) National Hope line Network, Suicide & Crisis Hotline
* 1-877-Vet2Vet (838-2838) Veterans Peer Support Line
* 1-800-SUICIDA (784-2432) Spanish Speaking Suicide Hotline
* 1-800-WORKPLACE (967-5752) Drug-Free Workplace

# Methods to Communicate Essential Information to Partners

The facility communication plan needs to include primary and alternative means for communicating. Included in the plan should be contact information related to **local, state, regional and federal emergency authorities** as well as contact information and corresponding agreements with other partners (providers, agency staffing organizations, vendors) who are part of the facility’s emergency preparedness plan. Additionally, the facility should ensure that the secondary or alternate methods of communication is compatible with the communication systems of those on their contact list.

# Methods to share protected patient information

The facility communication plan should include methods for medical and financial information sharing requirements. The facility should include in the plan the primary and alternative methods, in case of loss or failure, in which resident medical information and records are shared with agreed upon entities. These processes need to be in alignment with HIPAA and HITECH requirements.

Review of the facility HIPAA compliant policies and procedures should include interventions of sharing information in case of an emergency as well as evacuation. The facility policies should be reviewed and revised to include the required transfer notice and documentation processes per the requirements of participation.

See the HIPAA Decision Flow process, per CMS,. <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/decision-tool/index.html>

Facility communication plan should include a process for providing facility specific information, which is readily accessible for emergency management authorities, including:

* Occupancy/Census
* Resident population demographics
* Specialty programs and special needs of residents including specialty equipment if applicable
* Assistance with evacuation needs
* Supply and pharmaceutical contingency
* Transportation needs
* Other

Facilities should share the overview of the emergency plan with residents, resident representatives and stakeholders so that they are informed of the plan and emergency processes. The facility may develop a fact sheet outlining key components of the plan and the roles/responsibilities of staff as well as communication processes including how to contact the facility during an emergency.

# Primary and alternate means of communication

The facility communication plan needs to include primary and alternative means for communicating. Additionally, the facility should ensure that the secondary or alternate methods of communication is compatible with the communication systems of those on their contact list.

# Contact Information

Contact information for each audience should be compiled and immediately accessible during an incident.

* **Residents and Their Family Members**
* **Suppliers**
* **Management**
* **Government Official and Regulators**
* **Employees, Victims, and Their Families**
* **The Community**
* **News Media**
* **Social Media**

# Messages

During and following an incident, each audience will seek information that is specific to them. These questions need to be answered when communicating with each audience.

Pre-scripted messages should be prepared using information developed during the risk assessment. The risk assessment process should identify scenarios that would require communications with stakeholders.

* + Accidents that injure employees or others
  + Property damage to facilities
  + Service outages due to cyber attacks
  + Liability associated injury to or damage sustained by others
  + Service interruptions in general
  + Chemical spills or releases with potential off-site consequences, including environmental

Care quality issues

Messages should be scripted to address the specific needs of each audience, which may include:

* + **Resident/Resident Representative** - “Is it safe?”
  + **Employee** – “When should I report to work?” “Will I have a job?” “Will I get paid during the shutdown or can I collect unemployment?” “Will overtime be mandated?” “What happened to my co-worker?” “What are you going to do to address my safety? My family’s safety?” “Is it safe to go back to work?”
  + **Government Regulator** – “When did it happen?” What happened (details about the incident)?” “What are the impacts (injuries, deaths, environmental contamination, safety of residents, etc.)?”
  + **Elected Official** – “What is the impact on the community (hazards and economy)?” “How many employees will be affected?” “When will you be back up and running?”
  + **Suppliers** – “When should we resume deliveries and where should we ship them?” “How many and how soon do you need emergencies supplies?”
  + **Management** – “What happened?” “When did it happen?” “Was anyone injured?” “How bad is the property damage?” “How long do you think service will be down?”
  + **Neighbors in the Community** – “How can I be sure it’s safe to go outside?” “What are you going to do to prevent this from happening again?” “How do I get paid for the loss I incurred?”
  + **News Media** - “What happened?” “Who was injured?” “What is the estimated loss?” “What caused the incident?” “What are you going to do to prevent it from happening again?” “Who is responsible?”

Messages can be pre-scripted as templates with blanks to be filled in when needed. Pre-scripted messages can be developed, approved by the management team and stored on a remotely accessible server for quick editing and release when needed.

Resources for Crisis Communications Center

Resources should be available within the primary business site and provisions should be made to set up similar capabilities within an alternate site in case the primary site cannot be occupied.

* Telephones with dedicated or addressable lines for incoming calls and separate lines for outgoing calls
* Access to any electronic notification system used to inform residents and/or employees
* Email address
* Fax machine (preferably one for sending and one for receiving)
* Access to company website to post updates
* Access to social media accounts
* Access to local area network, secure remote server, message template library and printers
* Hard copies of Incident response plan, business continuity, and crisis communications plan
* Site and building diagrams, information related to business processes and loss prevention programs (*e.g.,* safety and health, property loss prevention, physical and information/cyber security, fleet safety, environmental management, and care quality)
* Copiers
* Forms for documenting events as they unfold
* Message boards (flipcharts, white boards, etc.
* Pens, pencils, paper, clipboards, and other stationery supplies

# HIPAA in Emergency Situations: Preparedness, Planning, and Response

The Privacy Rule protects individually identifiable health information from uses and disclosures that unnecessarily compromise the privacy of an individual.

The process chart on the following page addresses the release of protected health information for planning or response activities in emergency situations.  Additional information can be obtained at <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/decision-tool-overview/index.html>.

Additional information addresses the following:

* Who is the source of the information to be disclosed?
  + A covered entity
  + The individual consumer
  + Other agency or organization that is not a covered entity
* To whom is the information being disclosed?
  + Public Health Authority
  + A health care provider for treatment
  + Other agency for public health purposes
  + Other person(s)/agency
* Has the individual consumer signed an authorization permitting disclose?
  + Yes
  + No

## Waivers

If the President declares an emergency or disaster and the Secretary of HHS declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the Privacy Rule.  The Privacy Rule remains in effect.  The waivers are limited and apply only for limited periods of time.

Additional information regarding waivers can be obtained at

<https://www.hhs.gov/hipaa/for-professionals/faq/incidental-uses-and-disclosures/index.html>

<https://www.hhs.gov/hipaa/for-professionals/faq/1068/is-hipaa-suspended-during-a-national-or-public-health-emergency/index.html>

CMS Resource: <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Downloads/OCR-Emergency-Prep-HIPPA-Disclose.pdf>

<https://www.hhs.gov/hipaa/for-professionals/faq/1068/is-hipaa-suspended-during-a-national-or-public-health-emergency/index.html>.

Compliance

The <Responsible Group or Individual> will employ multiple methods, tools, and audit processes to monitor and assess whether security controls and measures have been implemented and are being followed.

Non-compliance with this policy will result in notifications to the employee and management. Further consequences may include disciplinary action up to and including termination of employment (with cause) and/or legal proceedings to recover any loss or damage to <CompanyLong>, and possibly third parties affected.

Exceptions

While business needs may occasionally appear to require variance from established policy and standards, no exceptions are permitted unless granted by <CompanyLong>’s . For example, a particular business function may not be able to be performed effectively, reasonably, or cost-effectively if the Policy is followed.

Exceptions require the completion of a Risk Exception Form that includes a description and justification for the non-compliance. Once completed, the form is sent to <Responsible Group or Individual> ([security@<COMPANY>.com](mailto:security@%3cCOMPANY%3e.com)) for review and processing. The <Responsible Group or Individual> will accept or reject the request based on the results of a risk assessment. If a variance is granted, the affected Security policies will be updated and communicated.

Exceptions will be reviewed annually.

Appendix – Contact Grids

**Primary and Alternate Communication System Grid**

| **Communications System** | | | | |
| --- | --- | --- | --- | --- |
| **Type** | **Location** | **Vendor or Supporting Service** | **Back Up Redundant Service** | **Staff Responsible** |
| Business Phone |  |  |  |  |
| Business Cell Phone |  |  |  |  |
| Radio Communication |  |  |  |  |
| Alert System |  |  |  |  |
| Weather Radio |  |  |  |  |
| Internet Access |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Primary and Alternate Communication Process for Key Contacts**

|  |  |  |
| --- | --- | --- |
| **Primary and Alternate Communication Process for Key Contacts** | | |
| **Contact** | **Primary Method** | **Secondary Method** |
| Residents |  |  |
| Resident Representatives |  |  |
| Physicians |  |  |
| Medical Director |  |  |
| Key Management Team |  |  |
| Staff |  |  |
| Local EMS |  |  |
| Public Health |  |  |
| State EMS |  |  |
| State Public Health |  |  |
| State DHSS |  |  |
| Federal – CMS |  |  |
| FEMA |  |  |
| ASPR |  |  |
| CIO |  |  |
| IRP Team |  |  |