

Disaster Preparedness Building The Plan

Presented by:
Barbara B. Citarella RN, MS, CHCE, CHS-V (Certified in Homeland Security)
President/CEO
RBC Limited Healthcare & Management Consultants
www.rbclimited.com



Let's Start With The Plan

The regulations clearly define the plan as one that will continue to Provide continuity of patient care in an emergency.

Based on a risk assessment of hazard vulnerability assessment (HVA)



Continuity Of Operations Plan (COOP)

The Purpose of a Continuity Plan

- Provide for continuation of essential functions.
- Enable a rapid response to any emergency situation.
- The continuity plan documents:
 - **What** will occur in a continuity situation.
 - **How** and **how quickly** continuity actions must occur.
 - **Where** continuity operations will occur.
 - **Who** will participate in continuity operations.

Will Your Agency Survive A Disaster?

- According to the Federal Emergency Management Agency (FEMA), **more than 40% of businesses never reopen** after a disaster, and for those that do, **only 29%** were still operating after two years.

And guess what likely becomes of those that lost their information technology for nine days or more after a disaster?

Bankruptcy within a year

Purpose of COOP Plan

**To keep the business operational during crisis
and
provide essential services.**



Four Phases of Continuity of Operations Activation

- **Phase I - Readiness and Preparedness**
- **Phase II - Activation and Relocation: plans, procedures, and schedules to transfer activities, personnel, records, and equipment to alternate facilities are activated**
- **Phase III - Continuity Operations: full execution of essential operations at alternate operating facilities is commenced**
- **Phase IV – Reconstitution: operations at alternate facility are terminated and normal operations resume**

Standards of Care

- Your agency specific plan address crisis standards of care.



1135 Waiver



HIPAA



HIPAA and Disaster Preparedness

- If necessary to treat the patient or a different patient or if the information would help treat a different patient
- To a public health authority, as outlined below
- At the direction of a public health authority, to a foreign agency acting in collaboration with the public health authority
- To persons at risk of contracting or spreading a disease or condition (if authorized by other law)
- With certain people involved with patient's care/ responsible for the patient

When there is imminent threat to public health/ safety

COOP Checklist



Page 11

Executive Summary

- Mission statements, philosophy statements
- Scope of service
- Geographic locations
- Agency Demographics



Page 12

Defining Patient Population

- More than 10% of your census
- English as a second language
- Non-English speaking
- Cultures
- Special programs
- Functional limitations
- Electricity dependent

Persons-At-Risk (CMS Definition used for Regulation)

- Maintaining independence
- Communication
- Transportation
- Supervision
- Medical care
- Non English speaking
- Pharmacological needs
- Children, elderly, pregnant women

Essential Functions

What Is an Essential Function?

Essential functions are those functions that enable an organization to:

- Provide vital services.
- Exercise civil authority.
- Maintain the safety of the general public.
- Sustain the industrial or economic base during an emergency.
- In other words, essential functions are the agency's business functions that must continue with no or minimal interruption.
-

Patient Care is Our Essential Function

Identify Essential Functions

- Continuity of patient care services
- Triage
- People resources
- Supply functions/resources
- *Communication*
- Link to community resources

Page 17

Vital Information

- What databases
- Financial records
- Employee list
- Patient list
- Legal authority list
- Coop plan



Page 18

Alert/Notification Process Succession

- How each person will communicate to each other, team.
- Various offices
- Different states
- List of succession for officers



Page 18

Document List

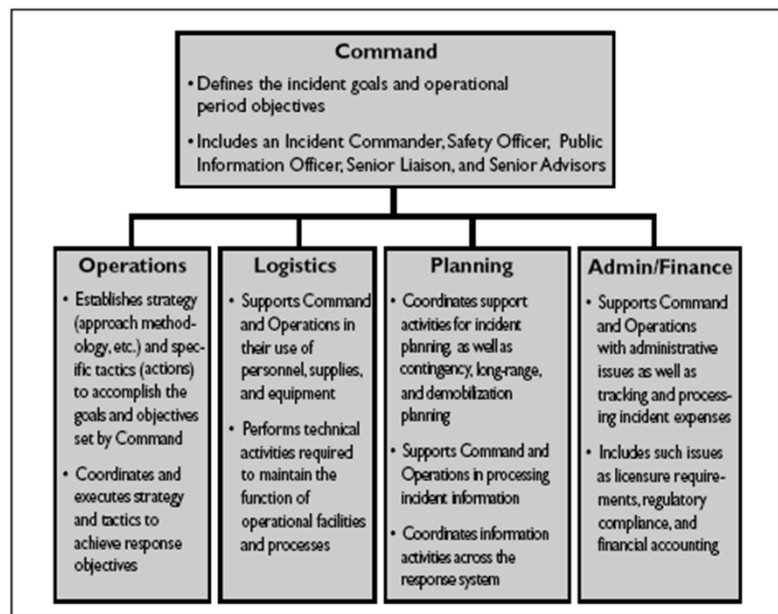
- Contracts- software vendors, licenses, personal protective equipment, independent contractors, health care benefits, recovery contracts
- Organizational chart
- Job descriptions- ICS



Page 19

Name Your Incident Command Structure

- The Incident Command System (ICS) is a standardized, on-scene, all-hazards incident management approach that:
- Allows for the integration of facilities, equipment, personnel, procedures and communications operating within a common organizational structure.
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private.
- Establishes common processes for planning and managing resources.



Public Information

- Who will serve as information officer
- How, what, where, and when for employees and patients
- Cultural diversity



Logistics/Communication

- Redundancy who will get what
- Food, generators
- Interoperable communications
- Use of smart phone technology and the internet
- What will the agency use?




Insurance Review

- Property coverage
- Payroll
- Interruption of power
- Reduced income
- Deductible
- Documentation for insurance

Page 23

Supplies

- Identify your **suppliers, shippers, resources and other businesses** you must interact with on a daily basis.
- Go 5 deep

1. GOWN <ul style="list-style-type: none">• Fully cover torso from neck to knees, arms to end of wrists, and wrap around the back• Fasten in back of neck and waist	
2. MASK OR RESPIRATOR <ul style="list-style-type: none">• Secure ties or elastic bands at middle of head and neck• Fit flexible band to nose bridge• Fit snug to face and below chin• Fit-check respirator	
3. GOGGLES OR FACE SHIELD <ul style="list-style-type: none">• Place over face and eyes and adjust to fit	
4. GLOVES <ul style="list-style-type: none">• Extend to cover wrist of isolation gown	

Page 24

Alert/Notification Process Succession

- How each person of the ICS will communicate to each other, team. Various offices
- List of succession for officers and ICS
- Up and down the tree

Human Resources

- We need human resources to fulfill our mission.
- Make sure we have all contact information
- Have an alternate staffing plan

Family Support Planning

- An organization's ability to respond in a continuity situation depends on the personal readiness of its employees. Individual and family preparedness is important for continuity planning.

All employees should develop:

- A family support plan that ensures family members will be safe and secure during an emergency situation.
- A personal "go kit" that includes the items their families will need if they have to evacuate or shelter in place.

Family Support Planning

The continuity plan addresses family support by providing for:

- An emergency information call-in number.
- An office "go kit" with an employee contact list.
- A communication plan to keep all employees informed.

Succession Planning

- Identification and development of potential successors for key positions in an organization, through a systematic evaluation process and training. Unlike replacement planning (which grades an individual solely on the basis of his or her past performance) **succession planning is largely predictive in judging an individual for a position he or she might never have been in.**

Source: <http://www.businessdictionary.com>

Orders of Succession

Orders of succession provide for the orderly, predetermined assumption of senior agency positions during an emergency in the event that any officials are unavailable or unable to execute their legal duties.

Communications

- Continuity of communications provides the capability to perform essential functions, in conjunction with other agencies, until normal operations can be resumed.

Continuity communications must be:

- Redundant.
- Available immediately because of the mission and requirements of the organization.
- Sustainable for up to 30 days or until normal operations can be resumed.

Alternate Facility Operations

- Locations
- Primary/secondary
- Redundancy
- Plan for that facility

Types of losses

- Human error
- Physical damage to office
- Technology
- Geographical
- Human resources

Page 35

Authorities and References

- Delegation plan
- Names
- Methods of communication

Page 36

Delegations of Authority

- Specify the activities that may be performed by those authorized to act on behalf of the agency head or other key officials.
- Document the legal authority for officials to make key policy decisions during a continuity situation.

Lists/Forms

- Employee roster
- Patient roster
- Vendor roster
- Off site inventory list
- Go kits
- Backup schedule

Who Has Responsibility

- Provide strategic leadership and overarching policy direction for the Continuity program
- Implement the Continuity Plan when necessary or directed
- Update/promulgate Orders of Succession and Delegations of Authority
- Ensure adequate funding is available for emergency operations
- Ensure all components participate in Continuity exercises
- Update Continuity Plan annually

Who Has Responsibility

- Update telephone rosters monthly
- Review status of essential files, records, and databases
- Know role and responsibilities in the event of activation
- Conduct alert and notification tests
- Make sure the plan is updated

Examples of Redundancies

- Copies of the plan
- Contracts, personnel listing
- Methods of communication

Page 11

Devolution/Dissolution

- Plan for when your agency can no longer function
- Information storage

Page 12

Reconstitution

- Surviving and/or replacement agency personnel resume normal agency operations from the original or replacement primary operating facility.
- The reconstitution process involves three broad tasks:
 - Transitioning from continuity status to normal operations after the threat or disruption has passed.
 - Coordinating and planning options for reconstitution, regardless of the level of disruption.
 - Outlining procedures necessary to effect a smooth transition from a relocation site to a new or restored facility.

Reconstitution

- Identification of who will do what
- Time frame estimates
- Damage assessments

How Do You Get The Business
Back Up and Running

Testing, Training, Maintenance of the Plan

- Test vital record restoration
- Compatibility of offsite offices
- Training of teams

Survey Procedures

Interview leadership and ask them to describe the following:

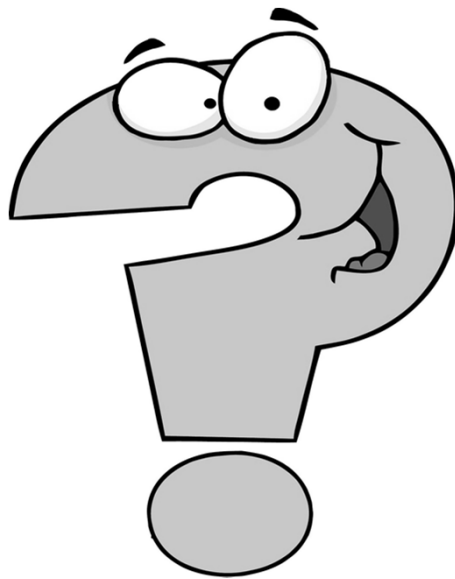
- The patient populations that would be at risk during an emergency event;
- Services the facility would be able to provide during an emergency;
- How the facility plans to continue operations during an emergency;
- Delegations of authority and succession plans.

Verify that all of the above are included in the written emergency plan.

“Chance favors the prepared mind”

- Louis Pasteur

1822-1895



RBC Limited

48 West Pine Road
Staatsburg, NY 12580

T- (845) 889-8128

F- (845) 889-4147

E - rbc@netstep.net

www.rbclimited.com

HIPAA and Disasters: What Emergency Professionals Need to Know

August 31, 2016

Disasters and emergencies can strike at anytime with little or no warning and the local healthcare system in the midst of an emergency response can be rapidly inundated with patients, worried family and friends looking for their loved ones, and media organizations requesting patient information. Knowing what information can be released, to whom, and under what circumstances, is critical for healthcare facilities in disaster response. This guide is designed to answer frequently asked questions regarding the release of information about patients following an incident.

NOTE: This guide does NOT replace the advice of your facility Privacy Officer and/or legal counsel who should be involved in planning for information release prior to an event, developing policy before a disaster that guides staff actions during a disaster, and during an emergency when contemplating disclosures.

This guide does address what information can be disclosed and under what circumstances. Covered entities can disclose needed patients' protected health information (PHI) without individual authorization:

- If necessary to treat the patient or a different patient or if the information would help treat a different patient
- To a public health authority, [as outlined below](#)
- At the direction of a public health authority, to a foreign agency acting in collaboration with the public health authority
- To persons at risk of contracting or spreading a disease or condition (if authorized by other law)
- With certain people involved with patient's care/responsible for the patient
- When there is imminent threat to public health/safety

What is HIPAA and the Privacy Rule?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing regulations, the HIPAA Privacy, Security, and Breach Notification Rules, protect the privacy and

Covered entities:

- Health plans
- Healthcare clearinghouses
- Healthcare providers (e.g. hospitals, clinics, pharmacies, nursing homes) who conduct one or more covered healthcare transactions electronically.

Business associates:

- Persons or entities that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI.
- Subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate.

security of patients' PHI, but is balanced to ensure that appropriate uses and disclosures of the information may still be made when necessary to treat a patient, to protect the nation's public health, and for other critical purposes.

Does HIPAA Apply to Me or My Organization?

The HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity's or business associate's workforce. Covered entities are health plans, healthcare clearinghouses, and those healthcare providers that conduct one or more covered healthcare transactions electronically, such as transmitting healthcare claims to a health plan.

Business associates generally include persons or entities (other than members of the workforce of a covered entity) that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI. Business associates also include subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate.

HIPAA does not apply to disclosures made by those who are not covered entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired).

When Can PHI Be Shared?

Patient health information, or PHI, can be shared under the following circumstances:

Treatment. Under the HIPAA Privacy Rule, covered entities may disclose, without a patient's authorization, PHI about the individual as necessary to treat the patient or to treat a different patient. Treatment includes the coordination or management of healthcare and related services by one or more healthcare providers and others, consultation between providers, providing follow-up information to an initial provider, and the referral of patients for treatment.

Public Health Activities. The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to PHI that is necessary to carry out their public health mission. Therefore, the HIPAA Privacy Rule permits covered entities to disclose needed PHI without individual authorization:

- **To a public health authority** that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, or to a person or entity acting under a grant of authority from or under contract with such public health agency,. This could include, for example: the reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions.
- **At the direction of a public health authority**, to a foreign government agency that is acting in collaboration with the public health authority.

- **To persons at risk** of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations.

Disclosures to Family, Friends, and Others Involved in an Individual’s Care and for Notification.

A covered entity may share PHI with a patient’s family members, relatives, friends, or other persons identified by the patient as involved in the patient’s care. A covered entity may also share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient’s care, of the patient’s location, general condition, or death. This may include—if necessary to notify family members and others—the police, the press, or the public at large.

- The covered entity should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object, when possible; if the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient’s best interest.
- In addition, a covered entity may share PHI with disaster relief organizations such as the American Red Cross, which are authorized by law or by their charters to assist in disaster relief efforts, for the purpose of coordinating the notification of family members or other persons involved in the patient’s care, of the patient’s location, general condition, or death. It is unnecessary to obtain a patient’s permission to share the information in this situation if doing so would interfere with the organization’s ability to respond to the emergency.

Covered entities can disclose needed PHI without individual authorization:

- If necessary to treat the patient or a different patient
- To a public health authority authorized by law to collect or receive such information
- At the direction of a public health authority, to a foreign agency acting in collaboration with the public health authority
- To persons at risk of contracting or spreading a disease or condition (if authorized by other law)
- With certain people involved with patient’s care/responsible for the patient for reunification or when in the patient’s best interest
- When there is imminent threat to public health/safety

Imminent Danger. Healthcare providers may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider’s standards of ethical conduct.

Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification. Upon request for information about a particular patient by name, a hospital or other healthcare

facility may release limited facility directory information to acknowledge an individual is a patient at the facility and provide basic information about the patient's condition in general terms (e.g., critical or stable, deceased, or treated and released) if the patient has not objected to or restricted the release of such information or, if the patient is incapacitated, if the disclosure is believed to be in the best interest of the patient and is consistent with any prior expressed preferences of the patient. Reference 45 CFR 164.510(a). In general, except in the limited circumstances described elsewhere, affirmative reporting to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, may not be done without the patient's written authorization (or the written authorization of a personal representative who is legally authorized to make healthcare decisions for the patient).

General or aggregate information in mass casualty events that does not identify an individual or meets the requirements of the HIPAA Privacy Rule's de-identification provisions is *not* considered PHI (e.g., X number of casualties were received by the hospital with the following types of injuries).

Minimum Necessary. For most disclosures, a covered entity must make reasonable efforts to limit the information disclosed to that which is the "minimum necessary" to accomplish the purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.) Covered entities may rely on representations from a public health authority or other public official that the requested information is the minimum necessary for the purpose.

Note: The disclosures listed above are at the discretion of the covered entity and are not required disclosures under the Rule. Some of these disclosures may be required by other federal, state or local laws (for example, mandatory reporting of positive infectious disease test results).

Does the HIPAA Privacy Rule Permit Disclosure to Public Officials Responding to a Bioterrorism Threat or other Public Health Emergency?

Yes. The HIPAA Privacy Rule recognizes that various agencies and public officials will need PHI to deal effectively with a bioterrorism threat or emergency. The public health threat does not have to reach a declared emergency status. If information is needed by a government agency to protect the health of the public (e.g., a food-borne outbreak), the agency may request and receive appropriate clinical and other information about the patient's disease, care, and response to treatment. To facilitate the communications that are essential to a quick and effective response to such events, the HIPAA Privacy Rule permits **covered entities** to disclose needed information to public officials in a variety of ways. Further, if the covered entity has obligations to report test results and other information to public health agencies by statute, rule, or ordinance, the HIPAA Privacy Rule generally permits these disclosures.

Covered entities may disclose PHI, without the individual's authorization, to a public health authority acting as authorized by law in response to a bioterrorism threat or public health emergency (reference [45 CFR 164.512\(b\)](#)), public health activities). The HIPAA Privacy Rule also permits a covered entity to disclose PHI to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism (reference [45 CFR 164.512\(j\)](#)), to avert a serious threat to health or safety). In addition, disclosure of PHI, without the individual's authorization, is permitted where the circumstances of the emergency implicates law enforcement activities (reference [45 CFR 164.512\(f\)](#)); national security and intelligence activities (reference [45 CFR 164.512\(k\)\(2\)](#)); or judicial and administrative proceedings (reference [45 CFR 164.512\(e\)](#)).

Is the HIPAA Privacy Rule “Waived” or “Suspended” During an Emergency?

The HIPAA Privacy Rule is not suspended during a public health or other emergency; however, under certain conditions the Secretary of the U.S. Department of Health and Human Services may waive certain provisions of the HIPAA Privacy Rule section 1135(b)(7) of the Social Security Act, if such a waiver is deemed necessary for the particular incident when the Secretary declares a public health emergency and the President declares an emergency or disaster under the Stafford Act or National Emergencies Act. For more information, access [“Is the HIPAA Privacy Rule suspended during a national or public health emergency?”](#)

Does the HIPAA Privacy Rule Permit Disclosure to Law Enforcement?

A HIPAA-covered entity may disclose PHI to law enforcement with the individual’s signed HIPAA authorization. A covered entity may disclose directory information as mentioned above to law enforcement upon request. Further disclosures to law enforcement for purposes of reunification and family notification are permitted as discussed above.

A HIPAA-covered entity also may disclose PHI to law enforcement without the individual’s signed HIPAA authorization in certain incidents, including:

- To report to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
- To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the premises of the covered entity.
- To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.
- When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity.
- To report PHI to law enforcement when required by law to do so (such as reporting gunshots or stab wounds).
- To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or an administrative request from a law enforcement official (the administrative request must include a written statement that the information requested

is relevant and material, specific and limited in scope, and de-identified information cannot be used).

- To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person, but the information disclosed must be limited to certain basic demographic and health information about the person.
- To respond to a request for PHI about an adult victim of a crime when the victim agrees (or in limited circumstances if the individual is unable to agree). Child abuse or neglect may be reported, without a parent's agreement, to any law enforcement official authorized by law to receive such reports.

How Does the HIPAA Privacy Rule Apply to Disclosures Involving Foreign Nationals?

Covered entities may disclose PHI for all persons, regardless of nationality, according to the [disclosures listed in the Privacy Rule](#) and discussed [above](#). Disclosure of PHI to embassies, consulates or other third parties, such as the American or International Red Cross acting in a capacity to facilitate notifications or repatriation following an emergency, is permitted under the existing disclosures of the HIPAA Privacy Rule, as referenced above.

For More information

- [Bulletin: HIPAA Privacy in Emergency Situations](#)
- [Can healthcare information be shared in a severe disaster?](#)
- [Health Information Privacy – Is HIPAA Privacy Rule Suspended during a National or Public Health Emergency?](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\) Privacy Rule: A Guide for Law Enforcement](#)
- [HIPAA Privacy Rule: Disclosures for Emergency Preparedness – A Decision Tool](#)
- [Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations](#)
- [Incorporating Active Shooter Incident Planning into Health Care Facility Emergency Operations Plans. Appendix A: Information Sharing. \(Page 29 of 33\)](#)
- [When does the Privacy Rule allow covered entities to disclose PHI to law enforcement officials?](#)
- [HIPAA Policy Brief](#)

For more information on HIPAA and Public Health:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html>

For more information on HIPAA and Emergency Preparedness and Response:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/index.html>

General information on understanding the HIPAA Privacy Rule may be found at:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>