

Emergency Preparedness



Are you a HIPAA covered entity looking for resources on creating a plan for your office, staff and patients? Look no further! This e-book will guide you through compiling an Emergency Preparedness Plan that is compliant with HIPAA's Guidelines. We will bring you through an overview of governing legislation in the event of an emergency, discuss how to make a plan for your office, patients and business associates, and lastly give you feedback on how to communicate that plan.

First, let's review the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule that protects individually identifiable information held by "covered entities." The HIPAA Privacy Rule permits covered entities to disclose Protected Health Information (PHI) for a variety of purposes. In addition, "the HIPAA Privacy Rule provides federal protections for protected health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of protected health information needed for patient care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to assure the confidentiality, integrity, and availability of electronic protected health information."

For more information on HIPAA and the law, [click here](#).

Ask the Expert

If you have any questions or comments, you are invited to "Ask the Expert" and our Dexcomm Expert will be happy to try to assist you with your request.

Please Note

Our e-books are designed to provide information about the subject matter covered. It is distributed with the understanding that the authors and the publisher are not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought.




Our passion is properly serving customers. Operating as a 24/7/365 Telephone Answering Service and Medical Exchange since November of 1954 we have developed skills and techniques that allow us to delight a wide range of clients. As we have grown and prospered for over 50 years we feel now is a great time to give something back to our customers, prospective customers and anyone seeking to improve their business success. Included in this book are tips and tools that we hope will make your job a bit easier each day. One of the great learning tools we have employed is the willingness to learn from our mistakes. Please take advantage of our many years of experience and avoid some of the pitfalls that we have learned to overcome. Our hope is that you and your office can adopt some of these tools to make your life a bit less complicated and allow you a bit more uninterrupted leisure time.

Thanks for listening!

INSIDE THIS ISSUE:

Legislation and Emergency Preparedness	<u>3</u>
Game Plan	<u>5</u>
Communication the Plan	<u>6</u>
Toolbox	<u>7</u>
Appendices	<u>8</u>




omm
E. HEARD.

JAMEY HOPPER

Ask the Expert

PRESIDENT





Legislation and Emergency Preparedness

Generally speaking, government legislation allows permissible disclosures that covered entities must make to respond to patients during times of crisis. For example, did you know that health plans and health care providers may disclose prescription information and other health information to other health care providers at shelters to facilitate the treatment of evacuees?

*The U.S. Department of Health and Human Services
Office for Civil Rights recently published the guidelines
and procedures below to determine disclosure.*

Providers and health plans covered by the Privacy Rule can share patient information in the following ways:

TREATMENT

Health care providers can share patient information as necessary to provide treatment.

- Treatment includes
 - sharing information with other providers (including hospitals and clinics)
 - referring patients for treatment (including linking patients with available providers in areas where the patients have relocated)
 - coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services)
- Providers can also share patient information to the extent necessary to seek payment for these health care services.



NOTIFICATION.

Health care providers can share patient information as necessary to identify, locate and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.

- The health care provider should get verbal permission from individuals, when possible; but, if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.
 - Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify or otherwise notify family members and others as to the location and general condition of their loved ones.
- In addition, when a health care provider is sharing information with disaster relief organizations, like the American Red Cross, that are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.





Legislation and Emergency Preparedness (continued)

IMMINENT DANGER

Providers can 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 and the provider's standards of ethical conduct.

FACILITY DIRECTORY

Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition. Of course, the Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the Privacy Rule does not restrict the American Red Cross from sharing patient information.

The use of Business Associate Agreements as a part of your Emergency Preparedness is also strongly encouraged.

[Click here](#) for guidelines and a sample version of an agreement.





Game Plan

In the world of sports, nothing is worse than going into a big game without a game plan! The same is true in business planning. We practice contingency planning in our daily lives in order to bypass crises that could have been avoided. So why not create an Emergency Preparedness Plan for your business?

Plan to Stay in Business by Adopting a Few Best Practices

Be Informed

Know what kinds of emergencies might affect your company. Is your business prone to tornados, coastal hurricanes or earthquakes?

Continuity Planning

Carefully assess how your company functions, both internally and externally. What will happen to your computer equipment or server? Will the goal be to continue operations or to shut down? How will you handle client calls? Will those be forwarded to an answering service or will you manage the phone yourself?

Emergency Planning

Your employees and co-workers are your business's most important and valuable asset. How will they be taken care of and kept safe? Where will they and their families evacuate?

Emergency Supplies

Think first about the basics of survival: fresh water, food, clean air and warmth. If you plan to remain in your office, make sure you have the necessities.



Deciding to Stay or Go

Plan for both possibilities of going to a shelter and evacuating. What factors will determine if you go or stay? At what point will you make the decision?

Fire Safety

Fire is the most common of all business disasters. Have your local fire department conduct an inspection of your business to ensure that your building is up to code. In addition, post evacuation routes next to every exit, and ensure each exit is clearly marked.

Medical Emergencies

Take steps that give you the upper hand in responding to medical emergencies. Consider pre-planning by knowing street closures, quickest routes, and local law enforcement best practices.

Influenza Pandemic

The federal government, states, communities and industry are taking steps to prepare for and respond to an influenza pandemic. [Click here](#) for a guide to preparing for an influenza pandemic.

	JAIMIE GUIDRY
	[Ask the Expert]
	APPLICATION ANALYST

Communicating the Plan

Communicating your plan of action in the case of an emergency is vital for business continuity throughout the event.

Start by following these simple tips:

Involve Co-Workers

Include people from all levels in emergency planning. We don't always think about the little things that can make or break business continuity. This is why involving employees at all levels in the Emergency Preparedness process is important.

Practice the Plan

Drills and exercises will help you prepare. We all know that practice makes perfect.

Promote Preparedness

Encourage your employees and their families to: get a kit, make a plan, be informed. [Click here](#) for guidance on creating family plans.



Crisis Communication Plan

Detail how you will be in contact with employees, customers and others during and after a disaster. Let your employees know when they will be expected to return to work and let your customers know if and when to expect a business interruption. Keep in mind SMS text messaging has been the most reliable method of communicating during recent storms.

Employee Health

Be aware of the health needs of your employees in the event that you may remain together for the duration of the emergency situation. Ask if anyone may need special attention during this time. People who have experienced a disaster may have special recovery needs.





Toolbox



Now that you understand Emergency Preparedness as it relates to HIPAA as well as the importance of getting a game plan in place, we want you to know that Dexcomm is prepared in the event of an emergency. Our staff is prepared to handle your communication needs during the emergency because of our preparedness policies (HR and training), operational systems (multiple locations) and mitigation techniques (generators, backup systems). Visit our website at www.dexcomm.com for a complete list of services and information.

We wish you the best in planning for the worst!

Blogs



- [How to Get Organized by Using Checklists](#)
- [7 Unusual Things You Should Include In Your Business' Disaster Preparedness Kit](#)
- [Easy Data Backup Strategy](#)
- [Power Outage Tips for Technology in Your Office](#)

Websites



- <https://www.quakekare.com/emergency-supplies-kits/recommended-preparedness-kits.html>
- <http://disastersurvivaltools.com/2011/02/emergency-preparedness/>
- http://emergency.superiorenergy.com/emergency_preparedness/



eBooks

- [Prevent Your Mobile Devices from Causing a HIPAA Violation](#)
- [Developing Your Corporate Communication Strategy for Immediate Threats](#)

A Special Thanks To

Our Dexcomm Contributors





Appendices

Work Cited

"Disclosures for Emergency Preparedness - A Decision Tool." *Disclosures for Emergency Preparedness - A Decision Tool*. Web. 22 May 2012. <<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/decisiontoolintro.html>>.

"Governor's Office of Homeland Security & Emergency Preparedness | State of Louisiana." *Governor's Office of Homeland Security & Emergency Preparedness | State of Louisiana*. Web. 22 May 2012. <<http://www.getagameplan.org/planBusiness.htm>>.

"Health Information Privacy." *Health Information Privacy*. Web. 22 May 2012. <<http://www.hhs.gov/ocr/privacy/>>.

Glossary

Covered Entity. The Administrative Simplification standards adopted by Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to any entity that is:

- a) a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider")
- b) a health care clearing house
- c) a health plan

Encryption. A method of converting an original message of regular text into encoded text. <http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2021.html>

HITECH. The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.

Protected Health Information. Individually identifiable health information:

- (1) Except as provided in paragraph
- (2) of this definition, that is:
 - (i) Transmitted by electronic media;
 - (ii) Maintained in electronic media; or acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
 - (ii) Any inadvertent disclosure by a person who is authorized to access
 - (iii) Transmitted or maintained in any other form or medium.
- (2) Protected health information excludes individually identifiable health information in:
 - (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
 - (ii) Records described at 20 U.S.C. 1232g (a)(4)(B)(iv); and
 - (iii) Employment records held by a covered entity in its role as employer.

Physical safeguards. Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. 45 C.F.R. §164.304

Privacy Rule. Requires a covered entity to have written policies and procedures as necessary to implement the privacy standards in the Rule and to train workforce members on those policies and procedures, as necessary and appropriate for the workforce members to perform their functions. 45 C.F.R. § 164.530(b)

Reasonable cause. Means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated. 45 C.F.R. §160.401

Security Rule. Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. 45 C.F.R. §160

Technical safeguards. The technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45C.F.R. §164.304

Willful neglect. Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. 45 C.F.R. §160.401