DISASTER PLANNING IN SENIOR LIVING: HIPAA STILL MATTERS

BRITTANY PAPE, ESQ., CHC, CHPC
DIRECTOR OF COMPLIANCE, SENIOR LIFESTYLE CORPORATION

SCOTT GIMA, MHA, RN
COO, EXECUTIVE VP, MPA

MARGARET SCAVOTTO, JD, CHC
PRESIDENT, MPA
HIPAA SECURITY RISK ASSESSMENT

DISASTER PLANNING

Standard 164.308(a)(7), Contingency Plan, requires covered entities to:

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
SECURITY POLICIES

1. Data Backup Plan (R) – 164.308(a)(7)(ii)(A): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

2. Disaster Recovery Plan (R) – 164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.

3. Emergency Mode Operation Plan (R) – 164.308(a)(7)(ii)(C): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.


5. Applications and Data Criticality Analysis (A) – 164.308(a)(7)(ii)(E): Assess the relative criticality of specific applications and data in support of other contingency plan components.

6. Contingency Plan (Standard) – 164.308(a)(7)(1) Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (such as fire, flood, vandalism, system failure, and natural disaster) that damages systems managing ePHI.
SECURITY RISK ANALYSIS

• Identify key information that is needed to continue care of residents

• Determine how to access key information based on types of disasters

• Address each possible type of disaster

• Identify major scenarios
  – Evacuation not required – shelter in place. Much easier to maintain PHI security.
  – Evacuation required.

SECURITY RISK ANALYSIS

• Threats
• Vulnerabilities
• Risk is based on the probability of a threat on a vulnerability and the overall impact on operations
SECURITY RISK ANALYSIS

Examples:
• Exposed water pipe directly above an EHR server
• Hurricane
• Tornado

PLAN FOR TECHNOLOGY

• What tools will help you in a disaster?
• Address them in your HIPAA security risk analysis.
• Train staff on what can and can’t be used.
...BUT ALSO PLAN FOR THE BASICS

- Plan for technology failing: Joplin tornado, Missouri, 2011

- Plastic bins placed at each nurses’ station that contain pens, pencils, blank nursing notes, paper, flashlights, batteries, walkie talkies

- Runners

- Train staff on these methods as well.

FOLLOWING HIPAA IN AN EVACUATION

- Protect records at original site, during transport, and at new location.

- Prioritize residents without using names.

- Send paper records with the resident – lock up records not in use.

- Physical security during evacuation is essential.

- EHR access and security at new location.
TRAINING

• What to do and what not to do
• Include HIPAA every step of the way
• Common sense counts – we can’t anticipate every app
• Drills
COMMUNICATION

Communication is a component of any disaster plan, and social media must be addressed in any disaster plan.

1. Internal versus External Communication
2. Accessing versus Disseminating Information
3. Identify and Monitor Potential Threats

KEY PRIORITIES

• Resident well being and safety
• Medications
• Food
• Necessary treatments and support – oxygen, wound care, breathing treatments
• Medications, medical supplies at new location(s)
• Staff support – rest and food (meals, snacks, drinks)
HIPAA TEMPORARILY WAIVED REQUIREMENTS

APPLICABILITY TO LTC

• Confirm with the LTC is a covered entity and whether HIPAA applies.

• While some HHS guidance may be more applicable to hospital providers, utilize the guidance about sharing resident information under the Privacy Rule in emergency situations to similarly proceed, as applicable.
WHAT’S WAIVED?

If the President declares an emergency or disaster and the HHS Secretary declares a public health emergency, then the HHS Secretary may waive sanctions and penalties against LTCs that do not comply with certain HIPAA provisions. During this time, the following HIPAA Privacy Rule provisions may be temporarily waived:

1. The requirements to obtain a resident’s agreement to speak with family members or friends involved in the resident’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 resident’s right to request privacy restrictions.
5. The resident’s right to request confidential communications.

PERMITTED DISCLOSURES

During a public health emergency, an LTC may disclose protected health information without authorization:

1. Treatment: as necessary to provide treatment
2. Notification: 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
3. Imminent Danger: 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
4. Facility Directory: if maintaining a directory of individuals, providers may tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition
WHAT’S NOT WAIVED?

• The REST of the Privacy Rule...
• The Minimum Necessary Rule still applies.
WHAT’S NOT WAIVED?

• The waivers do NOT change how providers can communicate with the media.
• Follow your directory.
• For all other requests, get an authorization.

WHAT’S NOT WAIVED?

• The Security Rule is not waived!

• Providers must still safeguard resident information.

• “covered entities must continue to implement reasonable safeguards to protect resident information against intentional or unintentional impermissible uses and disclosures”

• “must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information”
SOCIAL MEDIA
IN A DISASTER

WHAT IS SOCIAL MEDIA?

“Social media” is broad and constantly evolving. The term generally refers to Internet-based tools that allow individuals and communities to gather and communicate; to share information, ideas, personal messages, images, and other content.

- In some cases, to collaborate with other users in real time.
- Examples of social media platforms: Twitter, Facebook, LinkedIn, Snapchat, and YouTube, LinkedIn, blogs
REASONS FOR USING SOCIAL MEDIA IN A DISASTER

Primary reasons include posting information for public knowledge (e.g., road closures, shelter locations, and weather updates) and gleaning information to help allocate resources including the following:
1. Coordination activities
2. Status and location
3. The effect of the disaster on their surroundings
4. Where and how to locate shelter and supplies
5. How to report to areas that need volunteer support (and how to make donations over the internet)
6. Strategies for obtaining medical care
7. Marketing or promotion of the success of the community and safety of the residents

CONNECTIVITY DURING A DISASTER

During disasters social media provides access to relevant and timely information from both official and non-official sources, and facilitates a feeling of connectedness.
1. Connectivity to loved ones and the facility
2. Real time or live information
3. Government use of social media to community to public
RISKS OF USING SOCIAL MEDIA IN A DISASTER

1. Potential HIPAA privacy rule violations.
2. Inaccurate information received
3. Misinformation could go viral in an instant
4. Lack of social media control over the “story”

COMMUNICATION ISSUES

A component of any disaster plan, social media presents further issues

1. Centralized and Decentralized
2. Designated Spokespersons
3. False Information
SOCIAL MEDIA BREACHES: MAN VERSUS 6 TRAIN

• An emergency room nurse posted a photo to Instagram of an empty trauma room where a resident was treated for injuries after he was hit by a subway train.

• She posted the photo to Instagram with the caption: "Man Vs 6 Train...The After. #lifesaving #EMS #NYC #ER #Nurses #Doctors #nymed #trauma #realLife."

• The photo was originally posted by one of the nurse's colleagues.

• The nurse, who was on the TV show NYMed, was fired from her job.

SOCIAL MEDIA BREACHES: SHARK ATTACK

• In 2010, multiple hospital employees were disciplined after they took cell phone photographs of a resident treated in the ER following a shark attack.

• The resident was bitten twice while kite boarding – he had one bite with teeth marks across the buttocks, and a 9 inch bite on his right thigh that hit the bone. The employees emailed the photos.
SOCIAL MEDIA BREACHES: “WE WORKED CODE IN A CHICKEN COOP!”

• A man had a heart attack inside his chicken coop. His wife called 911, and EMS came and administered CPR in the chicken coop. The man did not survive.

• One of the EMS workers later made a Facebook post that said: “well, we had a first... We worked a code in a chicken coop! Knee deep in chicken droppings.”

SOCIAL MEDIA BREACHES: PARAMEDIC SELFIE WAR

• Two paramedics were arrested and face criminal charges after they engaged in a selfie war by text.
• They competed to take the most shocking pictures of themselves with residents in compromising positions.
SOCIAL MEDIA BREACHES: #BYEBYEANKLE

• A paramedic who responded to a motorcycle crash took photographs of the resident’s injuries and posted them to his Instagram account. The resident lost his leg.
• The Instagram post included a graphic photo of the resident’s injured leg, and included the following comment: “This is what happens when you’re careless in the rain on a motorcycle,” and was accompanied by hashtags: “#byebyeankle, #thelouderyouscreamthefasterwego and #oncethedoorscloseyourassismine”

SOCIAL MEDIA BREACHES: WELL-MEANING BREACHES

Memorials: “Fly away until another day soon we will be on are [sic] way.”

Proud employees and friends:
• “This is my friend.”
• “I am holding her hand til she falls asleep”
ABUSE ISSUES

Pictures or recordings that would demean or humiliate a resident(s) are mental abuse.


ABUSE ISSUES

- Three employees of a Georgia long term care facility were asked to monitor a resident until hospice arrived.

- Instead of monitoring the resident, the employees made a video titled “The End”, using Snapchat, of themselves vaping, using profanity, and making obscene gestures.

- The resident – who was dying – is visible in the background. Another employee saw the video and reported it.

- The three caregivers were arrested and charged with exploiting an elderly and disabled person. They face 20 years in prison and a fine of up to $50,000.
SOCIAL MEDIA IN A DISASTER POLICY CONSIDERATIONS

1. Require a signed HIPAA authorization before any resident-specific information may be posted on social media.
2. Develop clear policies covering social media use and ensure all employees are aware of how HIPAA relates to social media platforms.
3. Train all staff on acceptable social media use as part of HIPAA training and conduct refresher training sessions annually.
4. Provide examples to staff on what is acceptable – and what is not – to improve understanding.
5. Communicate the possible penalties for social media HIPAA violations – termination, loss of license, and criminal penalties.
6. Ensure all new uses of social media sites are approved by your compliance department.
7. Review and update your policies on social media annually.
8. Develop policies and procedures on use of social media for marketing, including standardizing how marketing takes place on social media accounts.

SOCIAL MEDIA IN A DISASTER POLICY CONSIDERATIONS CONTINUED

1. Require all social media posts to be approved by your legal or compliance department prior to posting.
2. Monitor your facility’s social media accounts and communications and implement controls that can flag potential HIPAA violations.
3. Maintain a record of social media posts using your facility’s official accounts that preserves posts, edits, and the format of social media messages.
4. Do not enter into social media discussions with residents who have disclosed PHI on social media.
5. Encourage employees to report any potential HIPAA violations.
6. Ensure social media accounts are included in your facility’s risk assessments.
7. Ensure appropriate access controls are in place to prevent unauthorized use of corporate social media accounts.
8. Moderate all comments on social media platforms.
SOCIAL MEDIA DO’S AND DON’TS EXAMPLES

Understand what is considered a HIPAA violation on social media. Common examples of social media HIPAA violations include:

1. Posting verbal “gossip” about a resident to unauthorized individuals, even if the name is not disclosed.
2. Sharing of photographs or videos, or any form of PHI without written consent from a resident.
3. A mistaken belief that posts are private or have been deleted when they are still visible to the public.
4. Posting of any information that could allow an individual to be identified
5. Sharing of seemingly innocent comments or pictures, such as a workplace lunch which happens to have PHI visible (e.g. visible resident files underneath).
6. Sharing of photos, videos, or text on social media platforms within a private group

TRAINING DO’S AND DON’TS

• Train on privacy, security, breaches, and social media
• Use examples!
• You don’t need a resident name to violate HIPAA
• The fact that someone is our resident is PHI
• A photo is PHI
• Even if your Facebook settings are private, you could have a breach
• Social media is usually not encrypted