Healthcare

ALERTBULLETIN®

A Risk Management Update | 2023 Issue 3

Smartphones and Social Media: Tips on Preventing Staff Misuse

Portable digital technology plays an essential role in every aspect of modern life, including the aging services industry. The pervasive use of smartphones within facilities enables instant communication and close, ongoing collaboration among caregivers, residents and family members. However, smartphones and related applications (hereafter "apps") may be misused by staff members, making it essential that aging services leadership be cognizant of the risks associated with these devices.

This edition of *AlertBulletin*® examines three major types of liability – privacy breaches, unauthorized social media posting and data spoliation claims – that may arise from careless or unapproved use of mobile phones, social media platforms and data storage systems in the residential care setting. A number of risk management strategies are included to help administrative and clinical leaders effectively address these challenges.

Personal Phone Use and Privacy

Aging services providers may use smartphones, laptops and tablets to communicate with one another and to avail themselves of online information resources. Some organizations also permit staff to access electronic healthcare records (EHR) and clinical databases via authorized apps that interface with the facility's EHR and IT systems. Although personal device use is clinically convenient, protected health information (PHI) may be improperly disclosed or vulnerable to hacking if devices are lost or stolen, user authentication protocols are inadequate, or data are transmitted over unsecured public Wi-Fi networks.

In accordance with HIPAA-related regulations, facilities should maintain an up-to-date roster of all staff-owned devices permitted to connect to their network. Access should be authorized solely to those with appropriate security controls, such as user authentication and access passwords, as well as effective anti-virus and anti-malware safeguards. Organizations should note personal device activity in their routine HIPAA security risk assessment and conduct regular audits of staff compliance with mobile phone security measures.

Monitoring personal device use represents one element of a formal, HIPAA-compliant mobile device policy and training program. Organizations also should implement the following privacy and security safeguards as adaptable to their environment, among others:

- **Require staff to report certain uses of their personal devices,** e.g., to access resident information through the EHR or to review databases through approved clinical apps, and strictly prohibit staff from storing resident-related data on their personal devices.
- **Ensure that all digital devices are password-protected,** and that healthcare data are digitally watermarked for easy tracking in the event of a breach.
- **Strictly prohibit automatic logins** and require an additional password or access key for software apps that may contain PHI.
- **Check that anti-virus software is installed on all mobile devices,** and regularly perform security scans on random devices to guard against malware.

- **Install security patches on personal devices** and require permission to access facility networks and intranets.
- **Instruct staff to set their devices and software apps to automatic logout,** or alternatively to lock mode, if devices are left idle for an agreed-upon period of time, such as five minutes.
- **Use multi-factor authentication** as an extra layer of security when accessing PHI – e.g., utilizing usernames and passwords as the primary safety measure, then requiring an additional step, such as keycard access, fingerprint verification or iris scan.
- **Designate a private Wi-Fi network that staff can use to safely access data,** as well as a secure text messaging service to ensure that communications are not intercepted.
- **Limit use of high-risk "share" interfaces,** such as Bluetooth technology.
- **Implement a security system** that warns users not to access potentially hazardous websites, and that also alerts administrators if a compromised or unauthorized device is detected on the network.
- **Direct staff to accept automatic security updates,** in order to ensure the latest protection against cyber threats.
- **Mandate immediate reporting of lost devices**, and institute remote data-erasure capabilities in the event of loss or theft.
- **Terminate access passwords and logins to data systems for departing employees,** so that PHI can no longer be accessed from their personal device.

The above-referenced security provisions should be supplemented by policies designed to prevent misuse of smartphones and to minimize cellphone-related distractions. (For sample guidelines, see "Smartphone Etiquette: Eight Suggested Protocols," below.) For more information about HIPAA, data security and use of mobile devices, visit this HealthIT website, as well as this related site.

Social Media Don'ts

A quick, thoughtless post can lead to long-term disaster. Remind staff to keep these "don'ts" in mind whenever they use social media:

- **Don't** talk about residents or identify coworkers by name.
- **Don't** mention your employer on your social media profile.
- **Don't** post your work hours, for reasons of personal safety.
- **Don't** post to social media while at work.
- **Don't** post anything you would not say in a face-to-face encounter.
- **Don't** denigrate your employer, co-workers, industry or profession online – not even jokingly.

Smartphone Etiquette: Eight Suggested Protocols

The following sample guidelines on mobile phone use should be modified, as necessary, to reflect specific organizational risks:

1. **As a general rule, put smartphones aside** and disable social media app notifications when providing care to residents.
2. **If it is necessary to use a personal device while on duty, ask the permission of residents** and explain the reason, noting both the online clinical app that is being used and the resource that will be accessed.
3. **Offer to show the smartphone screen to residents,** when appropriate, in order to demonstrate compliance with rules.
4. **Avoid using smartphones for personal calls**, texting and social media posting in resident care areas.
5. **Create no-phone zones** in bathrooms, showers and other sensitive areas.
6. **Designate Wi-Fi zones for smartphone use**, such as staff break rooms or other areas where residents are not present.
7. **Turn off mobile devices in the presence of clinical support equipment,** such as cardiac implantable electronic devices, in order to prevent potential magnetic interference.
8. **Reduce the risk of interruption and distraction by setting smartphones to "silent" or "airplane" mode during resident encounters.** Alternatively, place devices in the "do not disturb" mode that limits calls to pre-identified emergency contacts.

Inform staff that failure to adhere to established rules of smartphone conduct will result in disciplinary action ranging from verbal warnings to job termination, depending upon the seriousness of the infraction.

Unauthorized Social Media Posting

In today's technology-driven culture, it is unreasonable to expect aging services providers and staff to simply avoid utilizing social media. At the same time, facility personnel must understand that failure to exercise caution when posting work-related content can create significant personal and organizational risk, including potential exposure to civil monetary penalties under the HIPAA Privacy Rule and the federal Conditions of Participation. In fact, following a rash of denigrating postings about residents, the Centers for Medicare & Medicaid Services (CMS) has elevated enforcement activities regarding social media abuse of residents. Specifically, CMS prohibits facilities from "taking or using photographs or recordings in any manner that would demean or humiliate residents. This would include using any type of equipment (e.g., cameras, smartphones and other electronic devices) to take, keep or distribute photographs and recordings on social media."

Pursuant to these CMS directives, aging services organizations should develop cellphone photography guidelines and inform staff about abuse prevention policies, including misuse of social media. Staff training sessions should include examples of appropriate and inappropriate uses of social media, explain the protocol for reporting improper postings, and convey other privacy-related policies and procedures, such as the following protocols, which should be modified as necessary:

- **Draft and enforce organizational protocols with staff members regarding clinical photography,** focusing on authorization requirements, image storage guidelines, and equipment selection and use.
- **Obtain written permission from residents** before taking and/or posting photos and videos.
- **Do not capture or retain images of resident wounds** on personal communication devices.
- **Avoid posting resident pictures or related information to social media accounts** or sharing them with friends via texting or email.
- **Verify whether social media sites have permission to access posted photos and videos,** and also check social media security settings to ensure that images cannot be automatically uploaded without the account owner's express approval.
- **Utilize facility-created social network sites,** when available, to communicate work-related information in a secure manner, and access social media only from the organization's designated Wi-Fi network.

Many aging services facilities have their own social media pages where staff can post authorized photos of residents. These images should not be uploaded to the resident EHR. Before taking photos or videotaping residents for purposes of display on the facility's own social media site, ask these basic questions, among others:

- **Are formal rules implemented concerning management of the facility's social media site,** addressing such questions as who is authorized to photograph residents and who is responsible for the use and storage of images?
- **Is it clearly explained to the resident(s) why the image is being taken,** how it will be displayed or stored, and who will have access to it?
- **Has the resident's written consent been obtained** before any photographs are taken or posted?
- **Are safeguards implemented and monitored to prevent the unauthorized use or copying of posted images,** e.g., via a textual or semi-transparent watermark on the image, or a copyright notice stating that displayed images are personal property and cannot be used without the express consent of the resident and facility?
- **Do storage guidelines permit residents to view archived images at any point in time,** as well as to request the removal of posted images from social media sites?
- **Does the organization maintain records of images authorized to appear on its social media site,** indicating when, how, why and by whom the photograph has been taken?

To ensure compliance with CMS requirements, require staff members to acknowledge in writing that they have read social media policy statements, and also that they agree to comply with organizational rules governing cellphone use and social media conduct. (See "Social Media Don'ts" on page 2.)

Quick Links

- "HIPAA and Social Media Guidelines," *HIPAA Journal*, March 20, 2023.
- "Mobile Data Security and HIPAA Compliance," *HIPAA Journal*, 2015.
- Saul, H.C. and Pool, M.M. "Evaluating Legal Risks in Photos of Nursing Home Residents on Social Media." *McKnights Long-Term Care News*, August 29, 2016.
- Vearrier, L., Rosenberger, K., Weber, V. "Use of Personal Devices in Healthcare: Guidelines From a Roundtable Discussion." *Journal of Mobile Technology in Medicine*, posted December 4, 2018.

Spoliation of Images and Files

In the event of litigation, aging services organizations are expected to produce clinical and other health data in a reasonable timeframe as part of the discovery process. Such discovery may include data stored on smartphones, tablets and laptops, as well as desktop computers of members and providers, hard drives and external media.

Record retention guidelines should include preservation of all discoverable data, whether on portable devices or networked computers, in order to prevent claims of spoliation, i.e., destruction or alteration of evidence. Although sanctions for intentional destruction of evidence vary widely, at a minimum, the jury in a professional liability lawsuit may be directed to infer that the missing or damaged material is harmful to the aging services organization's case. The court also may decide to impose fines and penalties on the defendant and/or exclude witness testimony or other evidence.

Management of imaging data can be a burdensome task for organizations, so innovative techniques – e.g., data replication, cloud technologies, tiered storage systems – should be considered to help enhance retention and minimize exposure to spoliation claims. While there is no single record retention schedule that all aging services organizations and providers must follow, resident healthcare information records are generally maintained for five years after discharge, unless state law or regulation mandates otherwise. In addition, HIPAA requires that covered entities, including physicians and organizations that bill services to Medicare, retain privacy-related documentation for six years from the date of its creation. As retention policies for digital imaging vary from state to state, administrators are encouraged to review their respective state statute of limitations to ensure compliance with applicable laws and regulations.

Did someone forward this newsletter to you? If you would like to receive future issues of *AlertBulletin*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

The digital technology and social media platforms that connect us also create a variety of risks in the aging services context, ranging from violations of resident privacy to distraction from job duties to spoliation of discoverable data. The advice and guidelines suggested in this publication, when adapted to address unique organizational realities and challenges, can help ensure that smartphones and other electronic devices function as valuable tools, rather than sources of potential liability.

A Note on Retention of Surveillance Footage and Infrared Sensor Data

During the discovery phase of fall-related lawsuits, plaintiff attorneys frequently request surveillance video footage, as well as infrared sensor data from falls mitigation programs. As a result, questions often arise about how long these recordings and data should be retained.

Most security video surveillance cameras contain a built-in memory that typically erases footage after a week or month, which limits such devices' usefulness in the event of a claim. For this reason, aging services organizations often utilize additional tools – such as outside servers, cloud-based storage systems or secure digital (SD) flash memory cards designed for portable devices – to preserve surveillance video on a long-term basis. Although storage periods may vary, it is sound practice to establish a formal policy governing retention of security camera footage for consistency, regulatory compliance and legal defensibility purposes in the event of a claim.

In the case of infrared sensor data, artificial intelligence (AI)-driven software receives and interprets the data. Generally speaking, sensor data can be deleted once it is processed by the AI software, without requiring an auxiliary memory backup system.

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.

Published by CNA. For additional information, please contact CNA at 1-866-262-0540. The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situation. Please note that Internet links cited herein are active as of the date of publication, but may be subject to change or discontinuation and are provided solely for convenience. CNA does not make any representations, endorsements, or assurances about content contained on any website referred to herein or on the accuracy of any of the content contained on third party websites. The views, statements, and materials contained on the website are those of the owner of the site. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities.

Published 8/23. CNA AB23-3.