Electronic, Digital And Internet Communication, Including Social Networking And User-Created Web Content

Purpose And Scope

Acknowledging the benefits to patients when healthcare providers are readily accessible, healthcare providers must consider protection of confidential information, loss of personal interactions and the possibility of misunderstanding of communications when interacting with patients via non-verbal mechanisms. Inappropriate use of communication tools, such as posting patient personal health information (PHI) or patient photographs/videos on social media sites, blogs, or discussion boards can violate federal, state, and/or local laws, resulting in the posting healthcare provider facing the possibilities of civil liability, employment related discipline including job loss, disciplinary actions by licensing and credentialing authorities, and criminal investigations and sanctions.

The ever evolving world of communication tools, and in particular the area of the digital, electronic, and Internet communication platforms, represents a challenge to individuals and groups to be engaged and relevant in their community while maintaining professional standards of comport. With the advent of social media outlets and advancing capabilities of mobile devices, employees, faculty, residents, students, staff, and associates (henceforth "healthcare providers") must be cognizant and respectful of patient privacy and confidentiality as protected by the Health Information Portability and Accountability Act of 1996, as amended from time to time (collectively referred to as "HIPAA").

The purpose of this policy is to ensure the proper and uniform use of digital and electronic communication tools in the University of South Alabama ("USA") healthcare, education, and associated settings to reduce the risk of inappropriate or unlawful disclosures of protected health information ("PHI"). It is the intent of this policy statement to establish procedures and provide guidelines for the professional use of digital, electronic and Internet communication tools.

This policy addresses activities that (1) affiliate or identify a healthcare provider with USA or any members of its organized healthcare arrangements (OHCA) as delineated in the privacy notice, (2) use USA-provided communication tools, including but not limited to web pages, text messaging, email correspondence, and current or future social media websites, or (3) appear to represent the interests of USA. This policy is not intended to impact activities that do not represent USA and are purely related to personal matters not involving patients, including legally protected free speech.

Policy Applies To The Following:

1. **Activities that would fall under the jurisdiction of HIPAA, such as handling of protected health information by USA healthcare providers via digital, electronic, and Internet communication tools, including remote access into USA medical records of PHI.**
2. **Digital and electronic communications between healthcare providers in the process of carrying out their professional responsibilities.**
3. **Activities on electronic media and user-created web content. Common communication platforms and web content include email; text and instant messaging; cell phones, tablets and other mobile devices; blogs and journaling; internet posts and comments; and social media networks, including, but not limited to, Doximity, Facebook, Flickr, Foursquare, Google +, LinkedIn, MySpace, Pinterest, Tumblr, Twitter, and YouTube.**

Policy

1. **Protected Health Information**

   With very limited exceptions and only as authorized by the HIPAA Compliance Office, identifiable PHI, including identifiable case descriptions, must never be published, on the Internet or otherwise, without the patient's expressed and documented permission. This applies even if no one other than a patient is able to identify him/herself from the posted information. Healthcare providers must adhere to all HIPAA principles, including the reporting of HIPAA violations. PHI should be accessed and transmitted only in accordance with USA HIPAA privacy and security policies.
2. **Representation of USA or USA Hospitals**
3. **Unauthorized use of institutional information or logos is prohibited as is creation of any social media site that is branded to represent USA, and authorization must be obtained from the USA Public Relations Department. Only individuals authorized by the University are permitted to represent USA online. Management of any USA webpage or social media site will be the responsibility of the authorized creating division/department/section/office. Official posts must respect copyright, fair use, and financial disclosure laws. Posting of institutional phone numbers, email addresses, web addresses, photographs or videos to the Internet must be done in accordance with USA policy.**
4. **Communication Using E-mail, Texting, and Instant Messaging**
5. **Secure platforms for communicating PHI by healthcare providers are (1) Safebox (2) USA provided Microsoft Exchange/Outlook, and (3) secure portal communication systems (e.g. NextGen, Sorian). USA healthcare providers are fully responsible for their communications whether on USA-owned or personally-owned communication devices. Digital communication tools may supplement, but not replace, face-to-face interaction. Text messaging and email communication should not be used unless documented HIPAA-compliant authorization is made by the patient. Publicly available email (Hotmail, Gmail, Yahoo, etc.), texting, and instant messaging systems are not secure, do not guarantee confidential communication, and cannot be used for communicating PHI. Furthermore, healthcare providers cannot be certain that no other party has access to the patient's communications.**
6. **Offering Medical Advice**
7. **It is never appropriate to provide medical advice on a social networking site. Interactions between patients and healthcare providers should occur within an established healthcare relationship. Initial assessment of a patient's condition and development of a care plan must be performed in an appropriate clinical setting.**
8. **Privacy Settings**
9. **Healthcare providers should consider setting privacy at the highest level on all social networking sites.**
10. **This policy is not meant to discourage the use of innovative technologies, but to provide guidance and heighten the awareness of healthcare providers at USA to the potential risks and consequences.**
11. **Violations of this or any USA computer or information privacy policies or laws, including, but not limited to, those regarding student and patient information, may lead to disciplinary action, up to and including termination and/or legal action.**

Procedures

USA recognizes the rapidly changing landscape of communication tools. Healthcare providers will adhere to professional standards in their use of digital, electronic, and Internet communication tools by acknowledging and observing the following:

1. **USA institutional resources are provided to healthcare providers for the primary purpose of timely completion of their educational and clinical/work duties, including the access and transmission of PHI. Personal use of USA resources should not interfere with these duties.**
2. **USA healthcare providers should not expect privacy when using institutional computers.**
3. **Privacy and confidentiality between the healthcare provider and the patient are of the utmost importance. All healthcare providers have an obligation to maintain their personal access authorization through their supervisory personnel/ leadership.**
4. **Be aware that photographs taken in the healthcare environment may contain PHI, including the presence of patients in the background or foreground of the photograph.**
5. **Remote access into any USA system containing PHI should be performed in a secure environment. Remote access into any USA medical record system in public venues or via open Wifi connections should not be considered secure or HIPAA compliant. Passwords to USA medical record systems should not be stored in an unprotected repository.**

6. **All material published on the Internet via email, social media, or otherwise, should be considered public and permanent; published information cannot be recovered. Be aware that your relationship to USA can be discovered on the Internet without including a specific reference to your USA affiliation in any specific post. Healthcare providers must consider the content to be posted and the message it sends about them, their profession, and USA. USA reserves the right to request that certain subjects be avoided and that individuals withdraw certain posts as well as remove inappropriate comments.**
7. **The healthcare provider is owner of and responsible for the content of his/her own Internet and social media blogs/posts, pictures, etc., including but not limited to any legal liability incurred (defamation, harassment, obscenity, libel, slander, privacy issues regarding students or patients, etc.).**
8. **Misrepresentation of professional credentials or failure to reveal conflicts of interest via electronic, digital, or Internet platforms may result in disciplinary action by USA or credentialing authorities.**
9. **The tone and content of all USA-related electronic communications should remain professional. Respect among healthcare providers must occur in a multidisciplinary environment.**
10. **Healthcare providers should use separate personal and professional social networking accounts. For personal activity, the use of a non-USA email address as your primary means of contact is encouraged.**
11. **Do not post any material that is obscene, pornographic, defamatory, libelous or unlawfully threatening to another person or any other entity.**
12. **Healthcare providers are discouraged from interacting with any current or former patient on any social networking site or checking patient profiles on social networking sites.**
13. **Only reputable sites and sources should be used as medical education resources, including for patient education. Any referral made by a USA healthcare provider represents a tacit endorsement of that site by our institution.**
14. **Internet repository accounts, such as Dropbox and Google Docs, shall be utilized solely for the purposes of posting documents available in the public domain. Under no circumstances will non-public documents, particularly those containing PHI, be posted to any Internet repository account. USA-affiliated Internet repository accounts will be audited monthly with quarterly reports provided to the appropriate supervisory personnel/leadership. USA provides Safebox as a secure and safe method for sharing sensitive data with other USA faculty and staff. Note: Refer to the Computer Services Center for guidance on setup and use of Safebox.**
15. **Personal calls should not be initiated and/or received in patient care areas, public service areas, within view of patients or visitors. Ring tones and alerts should be set to vibrate or silent mode. Wireless headsets may not be used.**
16. **The use of personal entertainment devices (E.G., MP3 players, DVD players, cell phone entertainment features, cell phone texting, employee personal laptop, etc.) are not allowed in patient care areas, public service areas, or within view of patients or visitors unless being used for USA business.**
17. **Devices must not produce electromagnetic interference (EMI) with biomedical equipment.**
18. **Healthcare providers will be provided with training in the use of electronic, digital, and Internet communication platforms by their department. This training must be documented.**