Minimum Security Standards for Electronic Protected Health Information

Purpose

Keck Medicine of University of Southern California (USC)[1] recognizes that federal and California law require that Protected Health Information[2] receive the highest level of access control and security protection in order to safeguard the confidentiality and protect the patients' right to privacy of such information consistent with USC's privacy policies.

Definitions

Electronic Protected Health Information or "ePHI" is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

"Workforce" includes individuals who are employed, engaged by or who work at the direction of USC, and who access PHI maintained by USC and includes faculty, staff, employees, students, volunteers and trainees. Please refer to *USC HIPAA Policy Gen-101*.

"Mobile Devices" include but are not limited to laptops, cell phones, smart phones (iPhones, Blackberry, Droid, etc.) tablet computers, iPads, PDAs, USB (flash, thumb) drives, and external hard drives.

"Removable Media" includes but is not limited to CDs, DVDs, magnetic tape, typewriter ribbons and cartridges.

"Virtual Private Network" or "VPN" is a method to allow secure remote access across the Internet by using encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted. Health Sciences IT provides its users an alternative to VPN via the KeckPortal based on Citrix XenApp presentation technology. Citrix XenApp is a thin client technology that allows users to connect to their corporate applications by remotely presenting application video and remotely capturing keyboard and mouse input. No tangible data is transmitted by Citrix XenApp to the remote client workstation that could possibly be stored.

---

[1] For purposes of this policy, Keck Medicine of USC includes USC Norris Cancer Hospital, Keck Hospital of USC, USC's employed physicians, nurses and other clinical personnel, those units of USC that provide clinical services within the Keck School of Medicine, as well as the Keck Doctors of USC., those units that support clinical and clinical research functions, including the Offices of the General Counsel, Audit and Compliance.

[2]Protected Health Information or "PHI" is any individually identifiable health information, in any format, including verbal communications, regarding a patient created as a consequence of the provision of health care. "Individually identifiable" means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as a patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes patient billing and health insurance information and applies to a patient's past, current or future physical or mental health or treatment.

Minimum Security Standards for Electronic Protected Health Information

Policy

It is the policy of USC to protect the privacy and confidentiality of information when transmitted or maintained electronically consistent with federal and California laws and regulations and University policies. This includes ePHI that is:

- Communicated through electronic mail (email)[3];
- Stored or used on mobile devices or other removable media; or
- Accessed remotely; or,
- Accessed through the USC Network by a 3rd party system or server.

A. Communication of ePHI through the use of email

1. Email Systems: USC faculty, staff, contractors, residents and others who have the potential to transmit ePHI should only use the "MED" email system (commonly known as "MedMail") as their means of transmitting corporate email. MedMail provides automated email encryption of ePHI based on HIPAA lexicon and rule sets. MedMail includes email addresses ending in "@med.usc.edu" and "@health.usc.edu" and several other legacy domain names. Email accounts hosted by, but not limited to, Gmail, Yahoo, Hotmail and other non-MedMail systems should not be used. Forwarding of MedMail content to a non-MedMail account is prohibited. For email communications with individuals outside of the MedMail, see Section A.2. under Procedures.
2. Minimum Necessary Use of ePHI: USC workforce members are responsible for taking reasonable steps to protect patient privacy and to guard against unauthorized use of PHI. Only the information necessary to accomplish the purpose should be transmitted and should be distributed to only those with a legitimate "need to know" basis. Disclosures of PHI in email should be in accordance with USC HIPAA Privacy Policy GEN-104 "*Limiting Use and Disclosures of PHI to the Minimum Necessary*".
3. Patient Consent: Prior to beginning an online communication relationship between a provider and a patient, the patient's prior written consent must be obtained (See Attachment A – "*USC Patient Email Consent Form")* regarding the appropriate use and limitations of this form of communication. The patient's consent shall be maintained in the patient's medical record. Note that the professional, ethical, and legal guidelines and requirements applicable to traditional communications between health care providers and/or their patients also apply to electronic communications.
4. Emergency Subject Matter: Email communications should never be used for urgent or emergency problems and cases. USC providers, staff, and patients should be made aware of the risks associated with online communication related to emergency medical situations by making it clear that email should not be utilized to report or seek advice or treatment for an emergency condition. Patients should be instructed to call their physician directly or 911 for emergency assistance, as appropriate.
5. Authentication: USC Workforce members have a responsibility to take reasonable steps to authenticate the identity of correspondent(s) in an electronic communication and to ensure that recipients of information are authorized to receive the communication. Note: A best

[3]Please note that email does not include communication via text messaging. Text messaging of PHI is generally prohibited and can only be done upon approval of an IT approved secured text messaging solution.

practice for verifying the identity of the patient and confirming the accuracy of the email address prior to sending an email is for the provider to request that the patient send a test email and the provider reply back.

6. Unauthorized Access: The use of email communications may increase the risk of unauthorized disclosure of and/or access to ePHI (but should also create a clear record of the disclosure). USC email users should follow procedures that help mitigate that risk. When inappropriate access has occurred, USC may have an obligation to inform the patient of a breach in privacy. The USC Office of Compliance should be contacted immediately when incidents occur for appropriate follow up cases.

B. Storage and use of ePHI on Mobile Devices and Removable Media

1. General Rule:
    i. Data and files containing ePHI should be secured and stored on USC mainframe or network drives and servers.
    ii. All ePHI should be removed from data and files before they are stored on mobile devices or removable media.
    iii. ePHI in the custody or control of USC workforce members must not be stored on mobile devices or removable media unless all the conditions below are satisfied:
        1. There is a compelling patient care, business or academic need.
        2. The device or removable media is USC owned, purchased and/or issued.
        3. Only the minimum necessary amount of ePHI is stored on the device or removable media.
        4. The ePHI is encrypted or other approved security measures have been implemented to protect the restricted information from loss or theft of the data and/or System. ***Please ask your local IT department for assistance in meeting these requirements***.
2. Non USC-owned Devices and Media: Data containing ePHI must never be stored on a non-USC owned computer, mobile device or removable media unless the user has been granted an exception to this policy. Workforce members must return all USC property including ePHI, mobile devices and removable media before they terminate from USC. USC ePHI may not be taken with an individual when he/she terminates from USC unless written permission has been obtained from an appropriate USC authorizing party.
3. Department and program managers are responsible for ensuring that the policy requirements above are met.
4. Cell phones and Smart phones: The provisions in Section 1 and 2 above are not applicable to ePHI in email stored on cell phone or smart phones whether USC owned or personally owned. Storage of ePHI on such devices must meet the following provisions:
    i. There is a compelling patient care, business or academic need and;
    ii. A passcode is set on the device, and
    iii. The passcode is not shared with anyone else, and;
    iv. If the device can support encryption of locally stored email, attachments and other data, the user has enabled this feature and;
    v. The device must have the ability to be remotely wiped in the event the device is lost or stolen, and;
    vi. The user must alert the Office of Compliance if the device is lost or stolen.

C. Remote Access into Networks of USC

1. All remote access to USC applications across the Internet must either use the VPN technology provided by ITS or the KeckPortal as supported by Health IT. Please refer to USC Memorandum "*Important changes for Users Remotely Accessing USC Systems*" issued on January 7, 2013.
2. All devices connecting to Health IT resources via remote access must comply with the provisions of this policy, including non-USC owned equipment.

D. Connecting servers or third party systems to the USC Network

1. USC ITS has established security standards that must be met before any server or third-party system can connect to the USC Network in order to ensure USC Information Systems maintain and uphold appropriate security standards.
2. USC IT Administrators are required to use a "hardening checklist" for any new third-party system or server that is connected to the USC network.
3. USC faculty and staff must cooperate with IT administrators in completing the checklist accurately, completely, and promptly prior to a server or third party system connecting to the USC Network. For more information please refer to USC Memorandum "*Implementation of Hardening Checklist* "and "*Securing USC Information Systems*".

Procedure

A. Email Procedure

1. Email within the MedMail domain: The general guidelines below shall be followed when transmitting ePHI through electronic mail within the med or health.usc.edu email system.
    i. Use precautions when emailing. Sensitive health information such as that dealing with mental health, chemical dependency, sexually transmitted diseases, HIV or other highly personal information should not be transmitted via email. Only include the minimum amount of information in the body of the email for the intended purposes. In addition, if follow up is necessary use an alternative means of communication to discuss the subject of the email – such as telephone. Please refer to USC HIPAA Policies "*Limiting Use and Disclosures of PHI to the Minimum Necessary"* and "Special Privacy Considerations for more information.
    ii. No ePHI should be typed in the "subject field" caption of an email message. Do not use "patient-specific information" such as the patient's name or medical record number in the subject line of the email. However, patient initials, medical record numbers, or patient encounter numbers may be used for billing and clinical areas when sending e-mail within the med or health.usc e-mail system.
    iii. If attaching a document containing ePHI, verify that the correct document is attached. Check that all address fields (e.g. "to", "cc", and "bcc") reflect the correct individuals who will receive the message. Note: A best practice is to password protect the attached document containing the ePHI and sending the password in a separate email to the user.
    iv. If an email containing unencrypted ePHI is sent by accident to an external address, notify the Office of Compliance immediately.
    v. If an email containing ePHI is received in error, send a "reply" email to only the sender noting that it was received in error and that the sender should check that he/she has the correct email address for the individual who should have received the message.

vi. Each recipient on the distribution list should have an individual email address. Be careful when sending electronic mail containing ePHI to a mailing list or to shared email accounts because ePHI may be sent to external addresses or individuals who have no need to view the ePHI.

vii. No person shall make a change to another person's email message and pass it on without making clear where the person made changes. Any changes should be reflected in bold text or through other means to make changes readily identifiable.

viii. Copies of all messages, which are pertinent to a patient's care and treatment, should be placed in the patient's medical record and are subject to electronic discovery. The policies and procedures related to privacy and confidentiality of the traditional paper medical record also apply to email communications.

2. Email Outside the med/health.usc.edu system: In addition to the guidelines stated in Section I above, the below guidelines shall also be followed when emailing Restricted Information **outside** the MedMail system:

   i. Email Communication with Non-Patients:

      1. Emails sent outside the USC network are not always protected from interception during transmission and may be read at their destination by individuals other than the intended recipient. A secured email solution (i.e. encryption) must be utilized for all email messages containing PHI. Please note: An example of secure and encrypted email system is MedMail.
      2. The email subject line should not contain any PHI.
      3. The following footer must be included in all emails containing ePHI: "This email message is confidential, intended only for the recipient(s) named above and may contain information that is privileged, exempt from disclosure under applicable law. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to federal and state penalties. If you are not the intended recipient, please immediately notify us by telephone or return the email to the sender and delete this message from your computer."
      4. For assistance with secure email solutions, contact the Information Security Office or Keck Health IT Help Desk.

   ii. Email Communication between Patients and Providers

      1. Provider Opt In: A provider will decide if he or she wants to include email as a method for communicating with patients. Even if a patient signs the email consent, the provider is not obligated to use email to communicate with that patient.
      2. Patient Consent: Patient must affirm their consent to allow USC healthcare providers to send email containing ePHI to the patient's email address. An "email relationship" must not begin until the patient provides consent. When obtaining patient consent whether by paper, secure portal or other means, the following items should be included:
         a. Turnaround time for email messages;
         b. Instructions on how to escalate to phone calls and office visits;
         c. Statements indemnifying USC for information loss due to technical failures; and
         d. Notice to the patient that standard emails are not secure and pose some risk that the data can be intercepted.

3. USC Email Consent Form: Providers must use the "*USC Email Consent Form"* – see attachment A below.
    a. Patients should complete separate consent forms with each provider he/she wishes to communicate via email.
    b. The signed consent form must be stored in the patient's medical record. When an online secure solution is used, proof of the patient's electronic authorization shall be logged in the solution and enabled to be verified upon USC's request.

iii. Email Communication Content: Email transmission of ePHI should be limited to scheduling and other administrative communications. The emailing of test results, diagnostic or treatment information should not occur. If a patient initiates an email conversation or other secure electronic communication involving clinical areas, a phone or face-to-face discussion should be conducted. None of the following clinical laboratory test results and any other related results shall be conveyed to a patient by email or other electronic means:
    1. HIV antibody test;
    2. Presence of antigens indicating a hepatitis infection;
    3. Abusing the use of drugs;
    4. Test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy.

B. Mobile device and Media

1. All USC owned Mobile Device and Media Must be Encrypted. As noted in USC Policy and Memorandum "*Encryption Standards for Newly Purchased Mobile Storage Devices and Laptops*" all USC owned devices purchased on or after April 22, 2009 must have built-in encryption or accompanied software based encryption solution if such devices will contain ePHI.
2. Passwords for encrypted devices must be properly secured. Passwords for access to encrypted information should not be stored with or near the device.
3. Users must keep track of their mobile devices and removable media to ensure they are not misplaced and that unauthorized individuals do not have access to the device or the Ephi contained on the device.
4. Workforce members who are authorized to maintain ePHI on a mobile device must guard against the unauthorized use or viewing of the ePHI on the device.
5. Any critical data on mobile devices must be backed up in a secure manner and at appropriate frequency based on the nature of the data.
6. Before replacing or disposing of mobile devices or removable media containing ePHI, the user must securely wipe or overwrite the data, contact your local IT department for more information and assistance.
7. If the user has any reason to believe the data on a mobile device or removable media has been compromised, the user must immediately notify his/her Department Administrator and the Office of Compliance.

C. Remote Access

1. Health Sciences IT provides the KeckPortal as the primary means for remote access. The portal is accessible using a web browser. Go to https://keckportal.usc.edu.

2. The initial visit to the KeckPortal will require the installation of the Citrix plug-in. Once the plug-in is installed into the browser, this step can be skipped.
3. The browser will present you a login prompt. Login using your MED username and password.
4. Upon successful login, you will be presented with icons for all of the applications where your account has been granted access.

Enforcement

Failure to follow any of the provisions of this policy and breaches related to the privacy of Protected Health Information or other violations of USC's HIPAA privacy policies may lead to disciplinary action in accordance with applicable university policies and procedures, including the USC Faculty Handbook, SCampus, and Staff Employment Policies and Procedures as applicable.

Forms

See attachment A "USC Patient Email Consent Form"

References

45 CFR 160-164; California Civil Code Section 56 *et seq.*; California Civil Code Sections 1798.29 and 1798.82; California Health and Safety Code 1280.15 and 130203; California Lanterman-Petris Short Act

USC HIPAA Policies Gen-104 "*Limiting Uses and Disclosures of Protected Health Information*", Clin-203 "*Special Privacy Considerations*", PAT-607 "*Mitigation and Sanctions Policy*"; USC Information Security Policy.

USC Memorandum "Important Changes for Users Remotely Accessing USC Systems", "Securing USC Information Systems", "Encryption Requirements for Laptop and Mobile Device Storage"

1206D-1025

USC PATIENT E-MAIL CONSENT FORM
To address the risks of using e-mail
If you choose to communicate with your Provider by e-mail you must review and consent to the conditions or instructions set forth below.

Email Address: _____

1. RISK OF USING E-MAIL

Transmitting patient information by e-mail has a number of risks that patients should consider before using e-mail. These include, but are not limited to, the following risks.

a. E-mail can be circulated, forwarded, stored electronically and on paper, and broadcast to intended and unintended recipients.
b. E-mail senders can easily misaddress an e-mail.
c. Backup copies of e-mail may exist even after the sender or the recipient has deleted his or her copy.
d. Employers and online services have the right to archive and inspect e-mail transmitted through their systems.
e. E-mail can be intercepted, alerted, forwarded, or used without authorization or detection.
   1. Understand that the content of the e-mail may be monitored by USC to ensure appropriate use.
f. E-mail can be used to introduce viruses into computer systems.
g. E-mail can be used as evidence in court.
h. E-mails may not be secure, including at USC, and therefore it is possible that the confidentiality of such communications may be breached by a third party.

2. CONDITIONS FOR THE USE OF E-MAIL

Providers cannot guarantee but will use reasonable means to maintain security and confidentiality of e-mail information sent and received. Providers are not liable for improper disclosure of confidential information that is not caused by Provider's intentional misconduct. Patients must acknowledge and consent to the following conditions:

a. **Although Provider will endeavor to read and respond promptly to an e-mail from the patient, Provider cannot guarantee that any particular e-mail will be read and responded to within any particular period of time. Thus, the patient shall not use e-mail for medical emergencies or other time sensitive matters.**
b. E-mail must be concise. The patient should schedule an appointment if the issue is too complex or sensitive to discuss via e-mail.
c. **All e-mails to or from the patient concerning diagnosis or treatment will be printed out and made part of the patient's medical record. Because they are part of the medical record, other individuals authorized to access the medical record, such as staff and billing personnel, will have access to those e-mails.**
d. Provider may forward e-mails internally to Provider's staff and agent necessary for diagnosis, treatment, reimbursement, and other handling.
e. Provider will not forward patient identifiable e-mails outside of USC healthcare providers without the patient's prior written consent, except as authorized or required by law.
f. The patient should not use e-mail for communication regarding sensitive medical information. According to California law, your provider may not communicate any lab results unless your e-mail correspondence is conducted through a secure server. Additionally, e-mail must never be used for results of testing related to HIV, sexually transmitted disease, hepatitis, drug abuse or presence of malignancy, or for alcohol abuse or mental health issues.
g. Provider is not liable for breaches of confidentiality caused by the patient or any third party.
h. It is the patient's responsibility to follow up and/or schedule an appointment if warranted.

3. INSTRUCTIONS

To communicate by e-mail, the patient shall:

a. Avoid use of his/her employer's computer.
b. Put the patient's name in the body of the e-mail. In the body of the message, include your name and your identification number (Medical Record Number) or your date of birth.
c. Key in the topic (e.g., medical question, billing question) in the subject line.
d. Inform Provider of changes in his/her e-mail address.
e. Acknowledge any e-mail received from the Provider.
f. Take precautions to preserve the confidentiality of the e-mail.

4. PATIENT ACKNOWLEDGEMENT AND AGREEMENT

I acknowledge that I have read and fully understand this consent form. I understand the risks associated with the communication of e-mail between the Providers and me, and consent to the conditions and instructions outlined, as well as any other instructions that the Provider may impose to communicate with patient by e-mail. If I have any questions I may inquire with my treating physician or the USC Privacy Officer.

Patient Signature: _____ Date: _____ Time: _____

Witness Signature: _____ Date: _____ Time: _____

PATIENT E-MAIL CONSENT FORM

PATIENT ID