DPH Business Ethics and Best Practices
All Staff Memo
Revised June 3, 2016

Follow these rules when sending emails to patients…

The US Department of Health and Human Services clarified that the HIPAA Privacy Rule (45 C.F.R. § 164.530(c)) allows health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so (45 C.F.R. § 164.522(b)).

Patients may request or initiate communications with a provider using e-mail. If this situation occurs, the health care provider may assume (unless the patient has explicitly stated otherwise) that email communications are acceptable to the patient.

We are in the process of revising DPH Policies to reflect the above; however, for the sake of swift clarification, this All Staff Memo outlines the following allowances and guidelines for DPH providers and UCSF providers (as it regards patients seen at ZSFG/DPH):

RULES: You may communicate with patients via e-mail so long as you follow these rules:

1. **USE WORK EMAIL ONLY:** Email to patients may only be sent from a DPH or UCSF issued e-mail account. Do not use your personal email account to communicate with patients.

2. **USE SECURE EMAIL**: Any email to patients must be sent using DPH's or UCSF's encrypted electronic messaging system. Writing "SECURE" in the e-mail subject line activates encryption and requires the patient upon receipt to create and use a password to open all DPH/UCSF-encrypted emails.

   Exception: If a patient specifically asks that the emails they receive NOT be encrypted, the provider must:
   - Alert the patient of possible security risks of bypassing the encryption process. If the patient decides s/he wants unencrypted email, the provider may send emails without using the encryption system. Please note that for DPH emails, the encryption system may be activated automatically.*
   - Limit the amount or type of information disclosed in the email to the minimum necessary.
   - Double-check accuracy that the email is going to the right person.
   - Document the alert to the patient and the patient's decision in the patient's record.

- Insert the following language into the beginning of each unencrypted e-mail:

  Per your request, I am communicating with you without going through our encryption software (which would secure our communication but would require you to create and use a password to open my emails). Please note this is not a secure form of communication and the information contained in this e-mail may be at risk. The Department of Public Health does not assume any responsibility or liability for any lost, stolen, or e-mail captured electronically in route. Notify me immediately if you no longer wish me to send you unencrypted emails.

* Please note that the encryption process may be activated by the system even when you do NOT initiate it; that is, even when you exclude the word "Secure" in the subject line, the encryption software may find key words in the email and encrypt it. Thus there may be times when you find you are unable to meet your patient's request to bypass the encryption process. If and when this happens, you will receive an email stating: *Your email was identified as containing confidential information and was sent to the recipient(s) via ZIX secure email in accordance with CCSF Encryption Policies. For more information, please contact your department helpdesk or the DT Customer Service Desk at 581-7100.*

3. **NO NAME OR PHI IN SUBJECT LINE:** Do NOT include the patient's name or any PHI in the subject line.

4. **TAKE EXTRA CARE REGARDING SENSITIVE TEST RESULTS:** California law prohibits disclosure by Internet posting or other electronic means of results related to (1) HIV antibody test; (2) Presence of antigens indicating a hepatitis infection; (3) Abusing the use of drugs; or (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…unless the following 3 criteria are ALL met: electronic disclosure is requested by the patient, the means of conveyance is deemed appropriate by the health care professional, and a health care professional has already discussed the results with the patient. Compliance with these criteria must be documented in the patient's medical record.

5. **DOCUMENT IN THE PATIENT'S MEDICAL RECORD:** Electronic messages that contain ePHI must be stored in a secure manner consistent with DPH Privacy Policies. Do not delete emails to or from patients from your email box. Email communications should be placed into the medical record in a timely fashion. If your medical record is electronic and does not provide a mechanism for uploading emails or scanned copies of the emails, the content of the email communication should be (a) summarized or (b) copied and pasted into the charting.

If you have any questions, please contact the Office of Compliance and Privacy Affairs at 1-855-729-6040 or compliance.privacy@sfdph.org. This All Staff Memo (for purposes of copying and pasting the exception preface) can be found at www.sfdph.org, then Knowledge & Sharing, then Privacy Policies, then All Staff Memos.

Thank you for standing guard over your patient's personal and protected health information. It's important.