



City and County of San Francisco  
London N. Breed, Mayor

San Francisco Department of Public Health  
Grant Colfax, MD  
Director of Health

## San Francisco Department of Public Health

### *Policy & Procedure Detail*

Policy & Procedure Title: <b>D.1.2 Sending Electronic Messages to Adult Patients (E-Mails, Texts, Faxes, Computerized Voice Messages)</b>	
Category: Privacy	
Effective Date: 6/1/2017	Last Reissue/Revision Date: 11/1/2021
DPH Unit of Origin: Office of Compliance and Privacy Affairs (OCPA)	
Policy Contact - Employee Name and Title; and/or DPH Division: Office of Compliance & Privacy Affairs (OCPA)	
Contact Phone Number(s): 855-729-6040	
Distribution: DPH-wide <input checked="" type="checkbox"/>	If not DPH-wide, other distribution:

### I. PURPOSE OF POLICY

This policy provides guidelines and establishes standards and procedures for the electronic transmission of Protected Health Information (PHI) and the controls that the Department of Public Health (DPH) will employ to protect the security and privacy of electronic PHI (ePHI) when communicating with adult DPH patients (for sake of brevity, "patients" is used to refer patients, clients and residents) through E-mail, SMS (text), computerized voice messaging, and fax communications.

This policy applies to anyone contacting patients on behalf of DPH, including DPH staff, volunteers, interns, and UCSF staff at DPH sites. DPH contractors that wish to electronically communicate with adult patients under the contract must also incorporate controls as outlined in this policy.

This policy does not apply to provider-to-provider electronic communications, patient communications through the DPH electronic health record's patient portal, or other electronic communications that do not involve patients. It also does not apply to communications sent under the authority of the Health Officer or his/her designee. Currently, this policy only applies to patients age 18 and over.

### POLICY STATEMENT

It is the policy of DPH to ensure that electronic communications with patients comply with federal and state privacy laws and regulations.

### II. DEFINITIONS

- A. **Auto dialer.** Any equipment that has the capacity to automatically dial telephone numbers.
- B. **Electronic Protected Health Information (ePHI):** Individually identifiable health information that is transmitted or maintained by electronic media or is maintained in electronic media.
- C. **Encryption:** The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning to the data without the use of a confidential process or key.

---

**The mission of the San Francisco Department of Public Health is to protect and promote the health of all San Franciscans.**

We shall - Assess and research the health of the community - Develop and enforce health policy - Prevent disease and injury -

- Educate the public and train health care providers - Provide quality, comprehensive, culturally-proficient health services - Ensure equal access to all -

---

**D. Modes of Electronic Messaging (e-Messaging):** Examples include:

1. **Computerized Voice Messaging:** Sending automated voice messages to a cellular or home phone designated by the patient.
2. **E-mail Messaging:** Sending automated or manual messages to an email account designated by the patient.
3. **Fax Messaging:** Sending manual messages to a fax machine designated by the patient.
4. **Text Messaging "SMS" (Short Message Service):** Sending automated or manual text messages to a cellular phone designated by the patient.

**E. Patient:** Any individual who is a current or previous DPH patient, client, or resident who has received, is receiving, or will receive healthcare services from DPH.

**F. Protected Health Information (PHI):** Individually identifiable health information maintained or transmitted in any medium: oral, written, or electronic. It involves any information that identifies an individual AND relates to:

1. The individual's past, present or future physical or mental health; OR
2. The provision of health care to the individual; OR
3. The past, present or future payment for health care.

**G. Sensitive Health Service:** Per California Health and Safety Code Section [123148](#), sensitive health services information includes:

1. HIV antibody test results.
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.

**H. Type of Electronic Messaging:**

1. **Auto-created electronic messages:** A DPH-approved computerized messaging system that sends messages to patients based upon a status change or action noted in a database.
2. **Manually-created electronic messages:** Personalized messages written by employees that are sent to patients from a DPH- or UCSF-approved device.

### III. AUTHORIZED USES OF ELECTRONIC MESSAGES

Certain types of automated healthcare calls and texts are allowed by regulation, specifically if they provide important information that patients welcome and often rely on to make informed decisions.

**A. Types of Allowed Calls and Texts**

1. • Appointment and exam confirmations and reminders
2. • Wellness checkups
3. • Hospital pre-registration instructions
4. • Pre-operative instructions
5. • Lab results
6. • Post-discharge follow-up intended to prevent readmission
7. • Prescription notification
8. • Home healthcare instructions

Electronic messaging should primarily be used for non-sensitive and non-urgent issues. Examples of allowed types of calls and texts include:

**B. General Health Promotion.** Patients may be sent electronic messages that include general health education tips and reminders that are relevant to the patient's health. *Examples include:*

1. *Medication reminder goal: Don't leave home without taking your medications today!*
2. *Chinatown Public Health Center has a health fair on 10/25. Please come join us.*
3. *Keep our community protected against the flu. Drop by Southeast Health Center to get your flu shot this season. For more info please visit [www.SFDPH.org](http://www.SFDPH.org).*
4. *Try these healthy eating tips, recipes and check out resources at [www.SFDPH.org](http://www.SFDPH.org).*

**C. Patient Surveys.** Patients may be sent electronic messages that direct patients to complete surveys about the services that they received at different clinics and departments within DPH.**D. Alerts.** Patients may be alerted through electronic messaging about updates or action-required items related to their health. *Examples include:*

1. *Your medication request form has been sent to the pharmacy.*
2. *Please pick up your completed form from our clinic this week.*
3. *Our registration staff will be meeting with you at your next appointment to renew and review the information that we have on file for you as a patient.*
4. *Please monitor and report your blood pressure, your glucose levels, etc. to...*
5. *(Email) "Your labs results indicate that you should come in for an appt."*
6. *(Text) Appt on Thu 11/12 9:00AM Maxine Hall Health Center, 1301 Pierce Street. Come 15 mins early. Bring meds if seeing doctor/nurse/pharmacy. To cancel/resched call 415-292-1300.*
7. *(Automated Call) Hello, this is Maxine Hall Health Center calling from 415-292-1300. We are calling to remind you of your appointment on Thursday November 12 09:00*

*AM at 1301 Pierce Street. Please be sure to arrive 15 minutes before your appointment time. Please also bring your medications if you are seeing a doctor, nurse or pharmacist. If you need to cancel or reschedule, please call us back at 415-292-1300.*

Consult with the Office of Compliance and Privacy Affairs (OCPA) if you have questions regarding allowed calls and texts.

#### IV. PROCEDURES FOR AUTO-CREATED MESSAGING

- A. A DPH oversight process shall be established to ensure that electronic voice and text messaging initiatives meet regulatory and policy requirements and that the same patients are not contacted with uncoordinated and duplicate messaging. Contact OCPA to initiate this process.
- B. Each program utilizing electronic messaging should define a standardized operational and clinical workflow and identify processes for routinely notifying patients of their ability to (and the procedure for) opting out; and for regularly obtaining and updating the patient's designated contact information for phones, E-mails, and faxes.
- C. Use of a third party vendor to send automated messages requires consultation with DPH IT and the Office of Privacy and Compliance Affairs to ensure an appropriate system is selected and security/privacy controls are thoroughly evaluated.
- D. The Federal Communications Commission's (FCC) Telephone Consumer Protection Act (TCPA) regulates automated calling and text messaging consumers. For healthcare organizations subject to HIPAA the patient's prior consent is not required for the use of automatic telephone dialing systems ("auto dialers") and artificial or prerecorded voice messages. If a patient provides their phone number to a HIPAA covered entity, it is considered consent to be contacted for healthcare related messages. Healthcare messages must meet the following regulatory criteria :
  1. Be without charge to the patient (including not being charged against any calling plan limits that may apply);<sup>1</sup>
  2. Be made only to the number provided by the patient;
  3. At the beginning of the message, state the name and contact number of the healthcare provider or clinic/hospital;
  4. Be limited to the authorized purposes (as set forth in Section V herein, Authorized Users of Electronic Messaging) and not include any advertising, telemarketing, debt collection, billing, accounting, or other financial content;
  5. Be concise, generally one minute or less for voice calls and 160 characters (including spaces) or less for texts;
  6. Be limited to no more than one message per day, up to a maximum of three per week, for each healthcare provider;

---

<sup>1</sup> Note: DPH will notice patients initially and routinely that text messaging fees will apply based upon their telephone carrier service, and that they may opt out of the service at any time along with the method for doing so.

7. Offer an easy method to opt out of receiving future messages, including an interactive method for voice calls and a "STOP" reply for texts;<sup>\*</sup> and
8. Immediately honor an opt-out request.

## V. PROCEDURES FOR MANUALLY-CREATED ELECTRONIC MESSAGES (E-MAILS, TEXTS, FAXES)

### A. Procedures for Manually-Created Emails

1. The email subject line should not include the patient's name or any PHI.
2. It is the responsibility of each employee to ensure that e-mail messages containing PHI include the standard DPH Confidentiality statement as follows: *This e-mail is intended for the recipient only. If you receive this e-mail in error, notify the sender and destroy the e-mail immediately. Disclosure of the PHI contained herein may subject the discloser to civil or criminal penalties under state and federal privacy laws.*
3. Any email to patients must be sent using DPH's or UCSF's encrypted electronic messaging system. Writing "Secure" anywhere in the e-mail subject line<sup>2</sup> activates encryption for DPH encrypted emails.
4. Exception: **If a patient specifically asks that the emails they receive NOT be encrypted, the provider must:**
  - a. 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.<sup>3</sup>
  - b. Limit the amount or type of information disclosed in the email to the minimum necessary.
  - c. Double-check accuracy that the email is going to the right person.
  - d. Document the alert to the patient and the patient's decision in the patient's record.
  - e. Insert the following language into the beginning of each unencrypted e-mail: *You have asked that I send emails 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*

---

<sup>2</sup> Using any version of lower and upper case letters and insertion of the term anywhere in the subject line will trigger encryption.

<sup>3</sup> 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.*

*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.*

- B. Procedures for Manually-Created Texts.** Electronic text messaging is not secure unless a secure texting software is used. CareMessaging in EPIC is the preferred texting software. Manually-created text messages should not contain:

1. ePHI unless an exception to the policy has been approved by the Office of Compliance and Privacy Affairs (call 855-729-6040 or email [compliance.privacy@DPH.org](mailto:compliance.privacy@DPH.org)). If approval is provided, sender must follow procedures outlined under AUTO-CREATED ELECTRONIC MESSAGES.
2. Information which can be attributed to a specific patient such as identifiers, addresses, telephone, email addresses

- C. Procedures for Manually-Created Faxes.** PHI should only be faxed to confirmed fax numbers, and shall not be sent to distribution lists. For routine transmission of PHI via Fax, numbers should be programmed into the machine to minimize the potential for error. All faxes containing PHI must include a separate cover sheet. See [Secure Delivery of PHI - Cover Sheet for Fax or Mailing](#). DPH

## VI. PROCEDURES FOR NOTIFYING PATIENTS

- A.** All patients should be notified of DPH's intent to send electronic messages and be given the opportunity to opt out of receiving electronic messages as follows:
1. Patients will receive electronic welcome messages:
    - a. *Sample Email Welcome Notice: You are receiving this email because xxxxx@email.com is signed up to receive DPH communications. If you do not wish to receive e-mail messages from [office/program], please [reply to this e-mail and change the subject line to "Unsubscribe." ] [E-mail us at\_\_\_\_\_]. OR to unsubscribe, please click here (note, this should take them to FAQs).*
    - b. *Sample Text Welcome Notice: Welcome to [Clinic Name]. You will now receive Text updates and messages. Your mobile carrier may charge you for the cost of text messages in the same way they do with any other text messages. To learn more, www.xxxxxxx.com. To cancel call 415-xxx-xxxx.*
  2. Permission is voluntary and patients are under no obligation to receive DPH texts, e-mails, eFaxes or computerized voice messages. Patients who do not wish to receive notices or message may "opt-out" from receiving electronic messages at any time by notifying their provider or clinic/site of care by phone or in writing. Opting out is effective from that date forward, and not retroactively. If a patient informs an employee of his/her desire to opt out, it is that employee's responsibility to notify the appropriate staff to deactivate the patient from electronic messaging.
  3. Patients will be informed that they are to notify their provider or clinic as soon as possible if there has been a change in the phone number.

4. The Notice shall explain that text and computerized voice messaging service are different from patient portal communications that are available through DPH EHRs.
5. The Notice shall inform patients of the potential risks; e.g., DPH cannot promise text or voice messages are secure once they leave DPH and that he/she may be charged for the cost of text or phone messages the same way he/she would with any other text or phone messages.
6. The Welcome and Notification Notice shall include Frequently Asked Questions (FAQs) that are posted on the DPH website.

## VII. PROCEDURES FOR SECURING ELECTRONIC COMMUNICATIONS

- A. DPH and UCSF employees may only use a DPH- or UCSF-issued e-mail account and approved devices to send and receive PHI. They may not use any personal or other email accounts (for example, Yahoo or Gmail) for transmitting PHI. CBOs and other affiliates must follow encryption policies to assure data security. DPH and UCSF employees must use only a landline or cell phone carrier for communicating with patients. The use of web based or other communication software (such as Google voice) is prohibited.
- B. Contact information; e.g., email addresses, telephone numbers and fax numbers, should be checked periodically to ensure that they remain valid.
- C. Emails to or from patients are not to be deleted from employee's email accounts for auditing purposes.
- D. After the electronic message has been recorded, text messages sent via a non-automated system (e.g., via a DPH-issued cell phone) with the patient should be immediately deleted from the cell phone (texts originating from EHRs automatically become part of the patient's permanent record).
- E. Electronic messages that contain ePHI must be stored in a secure manner consistent with DPH Privacy Policies.
- F. Electronic Messages containing PHI may only be sent or received with a device that has been secured in compliance with DPH IT Security Policies and Procedures (DPH Electronic Data Security, Restricted Information Disclosure Prevention and Notification, and Data Encryption).
- G. PHI shall be limited to the minimum necessary amount of PHI for the permitted purpose.
- H. Electronic messages should limit or exclude patient identifiers. Never use first and/or last name in a message or on the subject line of an email.
- I. It is the responsibility of each employee to take the necessary precautions to insure that PHI transmitted via e-messaging is not inappropriately or unlawfully used or disclosed. Adherence to this policy shall be deemed as taking "the necessary precautions," per HIPAA regulations.

- J. Sensitive Test Results: California Health and Safety Code Section [123148](#) prohibits the disclosure by internet posting or other electronic means of clinical laboratory test results related to HIV antibodies, the presence of hepatitis antigens, the abuse of drugs, or specified test results that reveal a malignancy (see Definition) unless the following three (3) criteria are all met: 1) electronic disclosure is requested by the patient, 2) the means of conveyance is deemed appropriate by the health care professional, and 3) a health care professional has already discussed the results with the patient.

#### VIII. REFERENCES

- A. Health Insurance Portability and Accountability Act (HIPAA) and Amendments (HITECH, etc.) 45 CFR 160, 162 and 164
- B. US Department of Health and Human Services, 45 CFR §164.522(b) and §164.530(c)
- C. Office of Civil Rights (OCR) HIPAA Access Frequently Asked Questions (FAQs)
- D. California Medical Information Act, California Civil Code Section 56 et seq.
- E. Information Practices Act of 1977, California Civil Code Sections 1798.29 and 1798.82
- F. California Health and Safety Code Sections 1280.15, 130200-130205, 123148
- G. Federal Communications Commission (FCC) Declaration of Order clarifying and expanding the reach of the Telephone Consumer Protection Act (TCPA) summarized by a health policy law firm.
- H. DPH Policy: Secure Delivery of PHI - Cover Sheet for Fax or Mailing
- I. Title 42 CFR Part 2 Confidentiality of Substance Use Disorder Patient Records



