City and County of San Francisco
Daniel Lurie, Mayor

San Francisco Department of Public Health
Daniel Tsai
Director of Health

San Francisco Department of Public Health

*Policy & Procedure Detail**

Policy & Procedure Title: D.1.2 Sending Electronic Messages to Patients	
Category: Privacy	
Effective Date: 6/1/2017	**Last Reviewed/Revised Date:** 01/27/2026
DPH Unit of Origin: Office of Compliance & Privacy Affairs	
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 ☒	**If not DPH-wide, other distribution:**

All sections in table required. Updated 1/2026

I. Purpose and Scope:

A. **Purpose:** The purpose of this policy is to provide guidance and establish standards 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 PHI when communicating with DPH patients through E-mail, SMS (text), any other type of electronic messaging, and fax communications.

B. **Scope:** This policy applies to anyone contacting patients on behalf of DPH, including DPH workforce members and DPH contractors. DPH contractors that engage in electronic communication with patients under a DPH contract must also incorporate controls as outlined in this policy.

II. Definitions:

A. **Auto Dialer:** Any equipment that has the capacity to automatically dial telephone numbers.

B. **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.

C. **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.

D. **Workforce Member:** Refers to DPH employees, UCSF employees providing services for DPH, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of DPH whether they are paid by DPH.

III. Automated Electronic Messages:

A. Permitted Automated Electronic Messages: Automated electronic messaging should be used for non-sensitive and non-urgent issues. Examples of allowed types of calls and texts include:

i. Appointment and exam confirmation and reminders.
ii. Wellness Checkups
iii. Hospital pre-registrations instructions.
iv. Pre-operative instructions.
v. Lab results.
vi. Post-discharge follow-up instructions.
vii. Prescription notifications.
viii. Home health care instructions.
ix. General health promotion.
x. Patient surveys.
    a. Patients may be sent electronic messages that direct patients to complete surveys about the services that they receive at different clinics and departments within DPH.

B. Examples:

i. **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:

    a. *Medication reminder goal: Don't leave home without taking your medications today!*
    b. *Chinatown Public Health Center has a health fair on 10/25. Please come join us.*
    c. *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.*
    d. *Try these healthy eating tips, recipes and check out resources at www.SFDPH.org.*

ii. **Patient Notifications:**

    a. *Your medication request form has been sent to the pharmacy.*
    b. *Please pick up your completed form from our clinic this week.*
    c. *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.*

d. *Please monitor and report your blood pressure, your glucose levels, etc. to…*
e. *"Your labs results indicate that you should come in for an appt."*
f. *Appt on Thu 11/12 9:00AM Maxine Hall Health Center, 1301 Pierce Street.*
g. *Come 15 mins early. Bring meds if seeing doctor/nurse/pharmacy. To cancel/reached call 415-292-1300.*
h. *Hello, this is Maxine Hall Health Center calling from 415-292-1300.*
i. *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.*

C. Procedures for Auto-Created Messaging:

i. **Requirements:** Workforce members must follow the established oversight process 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.

ii. **Workflow:** 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.

iii. **Vendors:** Use of a third-party vendor to send automated messages requires consultation with DPH IT and the Office of Privacy and Compliance Affairs (OCPA) to ensure an appropriate system is selected and security/privacy controls are thoroughly evaluated.

D. Patient Consent for Contact via Automated Calling and SMS Messages:

i. **Oversight:** The Federal Communications Commission's (FCC) Telephone Consumer Protection Act (TCPA) regulates automated calling and text messaging consumers.

ii. **Consent for Automated Calling:** Healthcare Organizations subject to HIPAA are no required to obtain a patient's prior consent for the use of automatic telephone dialing systems.
iii. **Consent for SMS Messages:** If a patient provides their phone number to a HIPAA covered entity (DPH), it is considered consent by the patient to be

contacted for health care related messages. Messages must meet the following requirements:

a. Be without charge to the patient (including not being charged against any calling plan limits that may apply);[1]
b. Be made only to the number provided by the patient;
c. At the beginning of the message, state the name and contact number of the healthcare provider or clinic/hospital;
d. 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;
e. Be concise, generally one minute or less for voice calls and 160 characters (including spaces) or less for texts;
f. Be limited to no more than one message per day, up to a maximum of three per week, for each healthcare provider;
g. Offer an easy method to opt out of receiving future messages, including an interactive method for voice calls and a "STOP" reply for texts;* and
h. Immediately honor an opt-out request.

IV. Manually Created Electronic Messages:

A. Email Procedures:

i. The email subject line should not include the patient's name or any PHI

ii. All email signatures must contain the following statement:
   a. *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.*

iii. All email with PHI or other sensitive data must contain the word “SECURE” in the subject line.

iv. All email sent to patients that contain PHI must be encrypted. Encryption is activated when “SECURE” is entered in the subject line.

[1] 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.

v. **Patient Opt-Out of Encryption**: If a patient specifically asks that emails sent to them are not to be encrypted then:
   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.
   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 email: *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 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. Manually Created SMS (Text) Messages:

i. **Prohibition:** DPH workforce members are not permitted to use any text messaging application to send PHI to patients. Only DPH authorized text messaging applications may be used with appropriate approval.

C. **Faxing:** PHI should only be faxed to confirmed fax numbers and must 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 issued by DPH.

V. Notification to Patients:

A. **Requirements:** All patients must be notified of DPH's intent to send electronic messages and be given the opportunity to opt-out of receiving electronic messages.
   i. 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.
   ii. The Notice shall explain that text and computerized voice messaging service are different from patient portal communications that are available through DPH EHRs.

iii. 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.
iv. The Notice shall include Frequently Asked Questions (FAQs) that are posted on the DPH website.

B. **Patient Permission:** Patient permission is voluntary, and patients are under no obligation to receive DPH texts, e-mails, faxes 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.

VI. Procedures for Securing Electronic Communications:

A. **Authorized Email Accounts:** 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.

i. Contact information, e.g., email addresses, telephone numbers and fax numbers, should be checked periodically to ensure that they remain valid.

ii. Emails to or from patients are not to be deleted from employee's email accounts for auditing purposes.

B. **Sending and Storage**:

i. **Sending:** 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). 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.

ii. **Storage:** Electronic messages that contain ePHI must be stored in a secure manner consistent with DPH Privacy Policies.

C. **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.

D. **Responsibility:** It is the responsibility of each employee to take the necessary precautions to ensure 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.

Last Reviewed/Revised Date: 10/18/2017; 11/01/2021, 01/27/26