<u>Note</u>: This draft policy template is based on the SMS Text Messaging Policy developed by the Northwest Center for Public Health Practice (NWCPHP). It has been modified to be North Carolina-specific. More information about texting for public health purposes is available through the NWCPHP's SMS Toolkit, available at

http://www.nwcphp.org/docs/sms-toolkit/overview/index.htm.

Name of Agency/Logo

Policy Name: Text Messaging for Public Health Messages and Appointment Reminders
Policy Number:
Effective Date:

1. Purpose

It is the policy of <u>[agency name]</u> to permit the limited use of text messaging to communicate with the public or clients in a manner that is consistent with the HIPAA Security Rule (45 CFR Part 164, Subpart C). This policy provides for the use of two categories of text messages:

- Public health messages sent to members of the public who sign up to receive the messages.
- Appointment reminders sent to local health department clients.

2. Applicability

This policy is applicable to the following divisions or programs within the [agency name]:

• [Specify divisions or programs].

<u>Note - Consolidated agencies</u>: This policy may not comply with the confidentiality laws that apply to social services or other programs that may be part of your agency. Please consult with an attorney before using this policy with programs other than public health.

3. **Definitions**

- 3.1. SMS or text message: A 160-character message sent over a cell phone or through a web-based interface to one or more cellphone recipients.
- 3.2. Short codes: Five or six digit special telephone numbers used for sending SMS messages.
- 3.3. Protected health information (PHI): Individually identifiable health information in any form whether oral, written or electronic. Individually identifiable health information is information that:

- Relates to the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual; and
- Identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
- 3.4. *Electronic protected health information* (ePHI): Protected health information that is transmitted or maintained in electronic media.
- 3.5. *Subscriber*: A person who opts-in to a program to receive text messages with general public health content, such as educational messages.
- 3.6. Client: A person who receives medical, dental, or other health care services from [agency name].

4. Policies

- 4.1. General Policies Applicable to Both Types of Text Messaging Programs Covered by This Policy (Public Health Messages/Appointment Reminders)
 - 4.1.1. <u>Internal Notice of Text Messaging Program:</u> Consult and inform [agency division] prior to launching a texting program. The [division] will provide logistical assistance and messaging guidance and support.
 - 4.1.2. <u>Approved Devices for Sending Text Messages</u>: Text messages must be sent from devices owned or approved by [agency], or from an approved computer application.

Notes:

- (1) If the agency does not own the devices that will be used for the text messaging program, the agency should approve the devices that will be used. For more information on securing mobile devices, see https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.
- (2) Regardless of whether they are agency-owned, the devices or applications to be used for appointment reminder text messaging programs <u>must not be approved until the security risk assessment required by policy 4.3.1. has been completed.</u>

4.1.3. Public Records:

- a. Public records requests related to the text messaging program should be forwarded to [division or official/staff member] for a decision about whether the requested records may be released.
- On request, the agency will provide access to or copies of text messaging program records that are subject to public access under North Carolina's public records law, G.S. Chapter 132.
- c. The [agency] will not provide access to or copies of records created by a text messaging program for sending appointment reminders to clients in response to a public records request, as those records contain PHI and are excepted from public access by G.S. 130A-12.

<u>Note:</u> The public has a right to access and obtain a copy of records created by government agencies transacting agency business, unless an exception applies. Appointment reminder texts are excepted from this requirement because they contain protected health information, see G.S. 130A-12 (exception for local health department records that contain PHI). However, there is no exception that applies generally to text messages that do not contain PHI. There is also no exception that applies generally to the telephone numbers of members of the public who subscribe to text messages, but it is possible that another exception may apply to protect an individual phone number.

4.1.4. <u>Message Retention:</u> Text messages should be deleted from mobile devices but must be retained elsewhere if required by applicable records retention requirements. Records retention requirements for North Carolina local health departments are established by the North Carolina Department of Natural and Cultural Resources, State Archives, Government Records Section, and are available at http://archives.ncdcr.gov/For-Government/Retention-Schedules/Local-Schedules.

<u>Note</u>: The Government Records Section has a report that addresses some ways to retain text messages that are deleted from devices. See Best Practices for Electronic Communications Usage in North Carolina: Text and Instant Message, available at http://archives.ncdcr.gov/Portals/26/PDF/guidelines/Text Messaging Document.pdf.

- 4.1.5. <u>Training:</u> The [agency] will train employees in this policy. The training will include at least the following:
 - a. Review of all elements of this policy.
 - b. Review of the agency's procedures for implementing the policy, including procedures for sending text messages, retaining text messages, and responding to subscribers or clients who send text messages to the agency.
 - c. Identification of the person(s) within the agency who are responsible for the policy and to whom questions about the policy should be addressed.
 - d. Current information about text messaging best practices, including but not limited to:

- i. Cost: Agency staff should be aware that some people may be charged for text messages by their phone service providers and that messages exceeding 160 characters will be sent as two or more texts. Be judicious in the length of text messages and in the number of text messages you send.
- ii. Client Expectations: Set up clear communications with clients and members of the public about two-way communication, including whether you will return messages. (See also section V.D. of this policy, Responding to Text Messages Received from Members of the Public or Clients.)
- iii. Tone: Agency staff who send text messages should maintain a professional tone at all times. Refrain from using text abbreviations.
- 4.2. Specific Policies for Text Messaging Programs that Send Public Health Messages to Subscribers
 - 4.2.1. <u>Opt-In Requirement</u>: To receive text messages through a program covered by this policy, a subscriber must opt in.
 - a. A subscriber may opt in to receive general public health messages by signing a written opt-in form, using a website form, or using a short code.
 - b. The opt-in method must provide the following information:
 - i. A statement that the subscriber's cellular service provider may charge the subscriber a fee for transmitting and delivering text messages.
 - ii. Instructions for how to opt-out of receiving text messages.
 - iii. A request that the subscriber notify the program of a change in phone number, and information about how to provide that information.
 - c. Opt-out information should be sent to subscribers periodically to remind them how to unsubscribe from text messaging.
 - 4.2.2. <u>Messages Must Not Contain PHI</u>: SMS text messages sent through a program for sending public health messages to subscribers must not contain protected health information.
- 4.3. Specific Policies for Text Messaging Programs that Send Appointment Reminders to Clients

Note: Appointment reminders contain protected health information. Protected health information that is transmitted electronically (ePHI) is subject to the HIPAA Security Rule, which requires covered entities to conduct an initial security risk assessment and periodic security risk analyses to ensure the protection of ePHI. A security risk analysis is required when new methods of storing or transmitting ePHI, such as texting, are adopted. In brief, this requires a covered entity to identify where and how it acquires, creates, or maintains ePHI; assess its current security measures; identify threats to the security of ePHI; and determine the likelihood of those threats occurring. These findings must be documented and used to develop administrative, technical, and physical safeguards for the ePHI. The Security Rule does not prescribe the methods that must be used for a security risk analysis, but guidance from the federal HIPAA enforcement agency (HHS) is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html. An

HHS-developed tool for risk analysis is available at https://www.healthit.gov/providers-professionals/security-risk-assessment.

4.3.1. <u>Security Risk Analysis</u>: The [agency or division] will conduct a security risk analysis before implementing a program to send text messages with appointment reminders.

Note: Some electronic health records include an application for sending text messages to clients. If the agency's EHR has this type of application, as part of its risk analysis, the agency should consult with the EHR vendor to ensure that adequate security measures are in place to protect any ePHI that may be transmitted via the application. Local health departments should not approve the sending of appointment reminders via any device or computer application until the agency has completed the security risk analysis and determined that the requirements of the HIPAA security rule are satisfied.

- 4.3.2. Opt-In Requirement: To receive text messages with appointment reminders, a client must opt in.
 - a. A client may opt in to receive text messages with appointment reminders by signing a written opt-in form.
 - b. The opt-in form must provide the following information:
 - i. A statement that the recipient's cellular service provider may charge the recipient a fee for transmitting and delivering text messages.
 - ii. Instructions for how to opt-out of receiving text messages with appointment reminders.
 - iii. A request that clients receiving text messages with appointment reminders notify the program of phone number changes, and information about how to provide that information.
 - c. Opt-in forms should be stored in accordance with medical record retention requirements.
 - d. The staff of [agency or program] should periodically confirm that the client's contact information is accurate and up-to-date.
 - e. Opt-out information should be sent to clients periodically to remind them how to unsubscribe from text messaging.
- 4.3.3. Administrative, Physical, and Technical Safeguards:
 - a. The [agency] will identify which devices or computer applications may be used for sending appointment reminders by text. No other devices or applications may be used.
 - b. Agency staff should assure that client cell phone numbers are recorded accurately and should periodically verify the number with the client.
 - c. If a mobile device is used to send appointment reminders, staff members must:
 - i. Comply with existing policies for securing mobile devices that are used to access or transmit ePHI.

<u>Note</u>: If there is no existing policy for mobile device use, the agency should create a policy before implementing an appointment-reminder texting program.

ii. Delete the messages after the communication is completed and necessary information is recorded.

<u>Note</u>: The agency should develop a plan to ensure that all text messages sent or received are documented and retained in accordance with medical record and record retention requirements.

- d. Client names must not be stored in the address books or contacts lists of mobile devices.
- e. If a third-party vendor will be used to send text messages with appointment reminders, the [name of IT division or department that supports the agency] must be consulted first to assure an appropriate system is selected and security controls are thoroughly evaluated.
- f. [The security risk analysis may reveal additional administrative, physical, or technical safeguards that are needed. The agency should add those safeguards to this policy.]
- 4.3.4. <u>Message Content</u>: Appointment reminders sent by text message must be limited to the following information:
 - Sender first name (optional)
 - Agency name, or other identifier such as "your doctor" or "your health care provider"

 Note: If the Security Rule requirements for a risk analysis and identification of safeguards have been satisfied, identifying the agency by name might be permitted, but it may still be undesirable. Local health departments should consider this issue carefully. If the agency is identified, it should be identified generically (e.g., "health department" or other name that is recognized in the community). The specific clinic or service should not be identified.
 - Client first name
 - Appointment date and time
 - Telephone number for client to call with questions or to change appointment
 <u>Note</u>: The telephone number should be chosen with care. After completing the security risk analysis, the agency might conclude that it is permissible to leave a number that will identify the department generally, but it still may not be desirable. The number should not be one that will identify the clinic or the
- 4.4. Responding to Text Messages Received from Subscribers or Clients

nature of services.

4.4.1. The [agency] [will/will not] respond to text messages received from subscribers to general public health text messages.

<u>Note</u>: If the agency chooses not to respond to messages from subscribers, you may wish to note this on the opt-in form. If the agency chooses to respond to messages, staff members must be alert to the risk that a message sent by a subscriber may contain PHI. If a message containing PHI is received, the staff member should respond only with a brief message asking the person to call the staff member or another appropriate person in the department.

- 4.4.2. The [agency] will respond to text messages generated by health care clients with a text message asking the client to call. The response should include the first name and phone number of the appropriate person to call.
- 4.4.3. Messages received from subscribers or clients will be deleted from mobile devices after necessary information is documented in accordance with records retention policies.

4.5 Other Uses of Text Messaging by [Agency] Staff

- 4.5.1. The [agency] recognizes that agency staff may use text messaging in ways other than those addressed by this policy. Agency staff who use text messages in the transaction of agency business for purposes not covered by this policy must comply with the following:
 - a. Text messages must not include PHI or other confidential information.
 - b. Retain text messages if retention is required by the North Carolina records retention schedules (see http://archives.ncdcr.gov/For-Government/Retention-Schedules/Local-Schedules).
 - c. On request, provide members of the public access to or copies of text messages, unless an exception to the North Carolina Public Records Law (G.S. Ch. 132) applies. Public records requests for a staff member's text messages should be forwarded to [division or official/staff member] for management.

5. Appendices

Note: The agency should determine the appendices. Recommended appendices include:

- Opt-in form(s) used by subscribers to general public health text messages.
- Opt-in form used by clients for text messages with appointment reminders.
- Existing policies regarding the security of mobile devices.
- Any agency-specific plans or procedures related to any aspect of the policy.
- Identification and contact information for individuals or staff positions that are responsible for this policy or any component of it.