Use of Text Messaging and Emails to Contact WIC Participants

Policy No. OM- 450.01

Effective Date: October 2019

No. of Pages: 4

Policy

Local agencies may choose to use text messages and emails to provide appointment reminders, to convey information about the WIC Program, and to promote WIC services and benefits to WIC participants who have previously signed a written authorization electing to receive text messages, emails, or both from the local agency. All text messages and emails sent by a local agency to a WIC participant must protect the confidentiality of a WIC participant's PHI and confidential WIC information from unauthorized disclosure.

Local Agencies must use an encrypted method when sending text or email messages that contain PHI or confidential WIC Information. Local Agencies may send text or email messages that do not contain PHI or confidential WIC information without encryption, although the State WIC Office recommends encryption for all text messages and emails. Examples of each type of message are included in **Attachment A: Examples of WIC Confidential Information and Protected Health Information**. A local agency must ensure that only the minimum PHI necessary to complete the intended purpose is included in the encrypted text message or email. Documentation of all two-way conversations with participants must be placed within the MIS system.

Staff must delete all text messages and text conversations from their cell phones within five (5) days.

While this policy must be used as a minimum standard, local agencies may create their own texting and email policy. However, any texting policy created by a district must, at a minimum, protect PHI under HIPAA and confidential WIC information under the federal regulations and in accordance with DPH policy and must be reviewed and approved by the state WIC office.

Local agencies electing to utilize a third-party vendor to send text messages or emails to WIC participants, the third-party vendor must sign a HIPAA business associate agreement. In addition, the contract with the third-party vendor must specify that the vendor will use encryption to send any text message or email which contains PHI or confidential WIC information.

If any staff member becomes aware of a possible disclosure of PHI that is not permitted under HIPAA or a possible disclosure of confidential WIC information that is not permitted under the federal regulations, the staff member must report the possible disclosure to the State WIC Office's legal team within 24 hours.

Districts shall provide annual training.

Purpose

To ensure that any text messages or emails sent to WIC participants by the local agency protect the confidentiality of PHI and confidential WIC applicant and participant information from unauthorized disclosure, in compliance with the requirements of HIPAA, the federal regulations, and DPH policy.

Use of Text Messaging and Emails to Contact WIC Participants **Policy No. OM- 450.01**

Effective Date: October 2019 No. of Pages: 4

Procedures

I. Before sending a text message or email to a WIC participant, the local agency shall:

A. Explain to each WIC applicant/participant/parent/caregiver that text messages and emails are not secure because:

1. Another person could see and read the text message or email;
2. The text message or email could inadvertently be sent to the wrong person or telephone number;
3. Text messages and emails can be viewed on multiple devices and can be saved electronically, printed out, or played on speakers;
4. Text messages and emails can be forwarded to other people; and
5. While encryption adds an additional layer of privacy protection, even encrypted text messages or emails might not be completely secure.

B. Ask each WIC applicant/participant/parent/caregiver to sign the WIC Participant Email and Texting Consent Form contained in **WIC Participant Email and Text Consent Form**, or another written authorization form that has been approved by the State WIC Office and which states that they have been informed of the risks of sending PHI and confidential WIC information via text messaging and email, and which states that they authorize the clinic to send them text messages, email, or both containing PHI and confidential WIC applicant or participant information, and which also states that their consent is valid for one (1) year, but they may withdraw the authorization at any time.

C. Recommend that, if a WIC participant has any questions about a text message or email they have received from a local agency, the WIC participant call the clinic to ask the question instead of sending the question via text message or email.

D. Explain how to download the application to the WIC applicant/participant/caregiver's cell phone, If the local agency has elected to utilize an encrypted method to send text messages which requires that an application be downloaded to the person's phone before text messages can be received.

II. Provide an in-service training to staff on the appropriate use of texting and emailing to WIC participants. Topics covered must include:

A. Protecting the confidentiality of PHI under HIPAA and confidential WIC information under the federal regulations.

B. Security of devices and methods used for texting.

C. Using only WIC-issued or local agency-issued devices to send a text message to a WIC participant.

D. Use of professional language in text messages and emails without use of abbreviations.

E. Short, Concise Messaging (Less than 160 characters).

F. Translation of messages into the preferred language of an applicant/participant/parent/caregiver with Limited English Proficiency ("LEP"), in accordance with the Department's LEP Policy.

G. Reporting lost or stolen devices immediately to a supervisor.

H. Using text messages only for specific work-related purposes and not for business solicitations, religious or political causes, or any matters outside of a specific WIC-related purpose.

I. When and how to document information sent via text message and email in patient's medical record.

J. Including a simple option for the recipient to opt out of future messages or emails, for example, by replying "STOP" to an incoming text message or clicking on an "unsubscribe" link in an email.

III. Document all information sent to a WIC participant via text messaging or email and any information received from a WIC participant via text messaging or email in the patient's medical record and in the participant's WIC record immediately following the conversation, or no later than within 24 hours after the text message or email is sent or received.

A. Documentation must include:
   1. Date of entry;
   2. Name of staff member sending or receiving the text message or email;
   3. Date of conversation if not documented on the same day;
   4. Brief summary of the communication; and
   5. Documentation that the communication was conducted via text messaging or e-mail.

B. Delete messages when:
   1. Conversation with participant has concluded.
   2. Required documentation has been completed.

Authority

Health Insurance Portability and Acountability Act of 1996 45 C.F.R. §§ 160, 162, and 164

Use of Text Messaging and Emails to Contact WIC Participants **Policy No. OM- 450.01**

Effective Date: October 2019 No. of Pages: 4

DPH Policy # GC-09013, Confidentiality of Personal Health Information and Compliance with HIPAA

DPH Form GC-00901A Business Associate Agreement

7 CFR §§ 246.26(d)

Definitions/Supporting Information

Confidential WIC information - Any information about an applicant or participant, whether it is obtained from the individual, another source, or generated as a result of a WIC application, certification, participation, that individually identifies an applicant or participant and/or family member(s). Examples of confidential WIC information include a participant's name, address, and telephone number.

Covered entities - An entity that is subject to HIPAA because it is a health plan, healthcare clearinghouse, or healthcare provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA. Examples of covered entities include DPH, the Public Health Districts, and the County Boards of Health. In addition, DPH has designated WIC as a covered entity that must comply fully with HIPAA.

Protected Health Information (PHI) - Individually identifiable health information in any form, whether oral, written or electronic. Individually identifiable health information refers to information that: (a) 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 (b) identifies the individual or for which there is a reasonable basis to believe it can be utilized to identify the individual. Examples of PHI include a person's name, home or email address, telephone number, and dates of treatment.

HIPAA – the Health Insurance Portability and Acountability Act of 1996 , which contains a Privacy Rule that defines and limits the circumstance in which an individual's Protected Health Information may be used or disclosed by covered entities. Generally, HIPAA provides that a covered entity may not use or disclose protected health information unless the patient has provided a written authorization or unless disclosure is otherwise permitted under HIPAA.