AG.607 ELECTRONIC COMMUNICATION OF PROTECTED HEALTH INFORMATION

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration and Governance	Reviewed Date(s):	

Printed copies are for reference only. Please refer to the electronic copy of this document for the latest version.

Notice: Under the federal Health Insurance Portability and Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's confidential health information "give way" to those California state law provisions, and other federal provisions, that are more stringent than HIPAA

ODCHC staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact your immediate supervisor or the Privacy Officer.

PURPOSE:

Electronic communication of patient protected health information both internal and external presents a significant risk of accidental or deliberate disclosure. This policy outlines the security measures that must be taken whenever protected health information is included in an electronic message.

DEFINITIONS:

Electronic message: Any message created sent forwarded, replied to, transmitted, stored, copied, downloaded, displayed, viewed, or read by means of telecommunication networks or computer systems. This definition applies equally to the contents of such messages; transitional information associated with such messages, such as headers, summaries, addresses, and addressees; and attachments (text, audio, video).

Electronic messaging system: Any messaging system that depends on electronic facilities to create, send, forward, reply to, transmit, store, copy, download, display, view, or read electronic messages, including services such as email, text messaging, instant messaging, social networking, blogging, electronic bulletin boards, list serves, news groups.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low possibility of assigning meaning to the data without the use of a confidential process or key

POLICY:

Open Door Community Health Centers (ODCHC) protects protected health information (PHI) through administrative and technical actions that prevent the accidental or deliberate release of patient health information.

Open Door Community Health Centers staff and business associates must comply with the following security measures whenever protected health information is included in an electronic message:

- The use and disclosure must be permitted by the ODCHC Policy: AG_Use and Disclosure of Protected Health Information.
- Electronic messages containing PHI will not be sent or received except with a device that has been secured by ODCHC IT staff.
- PHI must be limited to the ODCHC Policy: AG_Minimum Necessary Standard.
- Highly sensitive PHI (for example mental health, substance abuse, or HIV information) will only be transmitted by electronic message with specific consent via NCHIIN.

Approved By: Board of Directors	Adopted Date: 6/22/20
Distribution: All Staff	Revision Date(s):
Category: Administration and Governance	Reviewed Date(s):

Printed copies are for reference only. Please refer to the electronic copy of this document for the latest version.

- ODCHC staff must use IT approved methods (Epic Staff Message, SPARK, or MyChart) to communicate when PHI is involved in the communication. PHI will not be communicated with external electronic communication systems such as Google or Yahoo accounts.

- Text messaging will not be used to send PHI unless the text message is encrypted both in transit and at rest using an appropriate encryption methodology. The encrypted text message must not be decrypted and stored on the cellular provider's systems in ways that can be accessed by unauthorized personnel.
    - If the text message meets the above requirements the message will be limited to the minimum information necessary for the permitted purpose
    - Text messaging will not be used to transmit patient orders
    - If a text message, containing PHI, is sent it must be reported to ODCHC's Privacy Officer through a Consolidated Situation Report

REFERENCES:

California Hospital Association, California Health Information Privacy Manual, 2017
HIPAA rules and regulations, 45 CFR 164
Yale University HIPAA Policy 5123, Electronic Communication of Health Related Information (Email, Voice Mail, and other Electronic Messaging Systems 3-8-2016
ecfirst White Paper, The CIO's Guide to HIPAA Compliant Text Messaging2013

ASSOCIATED DOCUMENTS:

ITEP 1.1.0 Mobile Device and Remote Access Appropriate Use
ITEP 1.2.0 Computer, Email and Internet Usage
AG_Minimum Necessary Standard
AG_Use and Disclosure of Protected Health Information
MS_Telephone, Verbal, and Texting Orders_ROC

KEYWORD TAGS:

Communication, electronic, text, texting, messaging, HIPAA, HIPPA, PHI