STATE OF CONNECTICUT
Department of Mental Health & Addiction Services
Commissioner's Policy Statement and Implementing Procedures

dmhas
A Healthcare Service Agency

SUBJECT/POLICY NAME:	Electronic Communication ("Electronic Communication") with Active DMHAS Clients
POLICY CHAPTER	INFORMATION MANAGEMENT
APPROVED BY:	9/12/23 Nancy Navarretta MA, LPC, NCC, Commissioner
EFFECTIVE DATE:	DATE: 09/12/23
LAST REVISED DATE :	DATE: 09/12/23
POLICY OWNER:	INFORMATION MANAGEMENT

STATEMENT OF PURPOSE: To ensure effective and legally compliant use of electronic communication between the Department of Mental Health and Addiction Services (henceforth referred to as DMHAS) workforce and active DMHAS clients. This policy applies to the organization's workforce in its entirety.

POLICY: It is the policy of DMHAS to comply with all applicable laws. This policy provides guidance on appropriate standards for secure and effective use of this organization's ability to send and receive electronic communications with active DMHAS clients, in order to comply with the privacy and security standards of Health Insurance Portability and Accountability Act (HIPAA).

ELECTRONIC COMMUNICATIONS PROCEDURE

Not only must electronic communication be HIPAA compliant but must also comply with FCC Telephone Consumer Protection Act (TCPA) and Cellular Telecommunications Industry Association (CTIA) messaging principles and best practices.

Rulings and regulations implemented by the FCC may relate to specific requirements based on federal law, while wireless carriers and communication platforms may have more stringent policies for sending messages (e.g., SMS) through their networks.

It is critical that DMHAS workforce ensures patient consent before sending patients Electronic Communications. Documentation of such consent by completion of the *Electronic Communication Consent* form is required. This form is to be placed in the patient's medical record.

DMHAS workforce may use state issued mobile devices to communicate with active DMHAS clients in compliance with all applicable laws and regulations, including but not limited to, HIPAA.

DMHAS workforce are prohibited from sending Electronic Communications containing PHI or ePHI in violation of HIPAA, or any other applicable laws or regulations.

Additionally:

- The Electronic Communication must be communicated from the sending device, through the mobile provider or a software application to the recipient's device in a secure manner.
- State issued mobile devices used for Electronic Communications must be periodically provided to IT for proper processing. Mobile devices must be returned to IT when employee leaves state service. The IT department must securely wipe all mobile devices, after proper preservation of records, when they are returned.
- Personal mobile devices must not be used for any Electronic Communications with active DMHAS clients. If DMHAS workforce has ever used a personal device, they must contact the IT department to securely wipe the device after proper preservation of records.
- Report all Electronic Communications that are received or sent out that contain any ePHI and any/all communications that are sent to the wrong intended individual immediately to the Chief Compliance Officer and the IT Security Officer.

PROCEDURE: The following safeguards must be implemented by all DMHAS workforce sending and/or receiving messages:

- The mobile device must be password protected; this feature must never be disabled.
- The mobile device must be configured to lock automatically after a period of inactivity (not to exceed 5 minutes).
- All messages must be limited to the minimum information necessary for the permitted purpose.

REFERENCES:

FORMS AND ATTACHMENTS: Electronic Communication Consent.