




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



SUBJECT:	DMHAS Email Encryption Policy
P & P NUMBER:	N/A
APPROVED:	 Miriam Delphin-Rittmon, Ph.D., Commissioner Date: 7/22/2019
EFFECTIVE DATE:	7/22/2019
LAST REVISED:	N/A
REFERENCES:	<u>Unauthorized Disclosure and Breach Notification of Unsecured PHI</u> <u>Computer Use Policy</u> <u>Security for Mobile Computing and Storage Devices</u> https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html https://portal.ct.gov/-/media/DOC/Pdf/HR/D05UseStateSystemspdf.pdf?la=en
FORMS AND ATTACHMENTS:	N/A

STATEMENT OF PURPOSE:

To outline the policy for the use of authorized encryption email service provided by the Department of Mental Health and Addiction services (DMHAS).

POLICY: Email Encryption services provided by the Department of Mental Health and Addiction Services to Authorized Users, offers the ability to use the State of Connecticut Email Service to exchange Protected Health Information (PHI) and other sensitive information in a secure and compliant manner. The ability to send encrypted email through the State of Connecticut Email Service is a technology solution and does not supersede any other DMHAS, State or Federal policy that controls the Exchange of PHI and other sensitive data.

Features of an encrypted email service may include:

- Sends, transmits and stores email messages securely (Encrypted).
- Assures the sender's email identity through a digital signature.
- Allows opening of messages only for the intended recipients.
- Allows the recipient of the message to reply back to the email in an encrypted format.

Training on the proper use of the encryption system will be provided by DMHAS. It is the responsibility of the DMHAS user to comply with the proper usage of the encryption system and the policies surrounding its use. The DMHAS email encryption training can found at [ZixMail](#).

Use of encryption is allowed only from an Authorized DMHAS Physical or Virtual workstation, Laptop or Tablet. The use of Smartphones or personal devices is not permitted.

PROCEDURE: To send or reply to encrypted emails, the user will need to click on the **Encrypt & Send** button in Outlook. To open an encrypted email, the user will need to click on the **Decrypt Message** button in Outlook. It is the responsibility of the sender to ensure that an email that contains PHI or other sensitive information is sent as an encrypted email.

- Sending PHI through an unencrypted email is not allowed.
- Any exchange of PHI in an unencrypted email must be reported immediately to the Facility or DMHAS Chief Compliance Officer.

DMHAS users must follow all other policies and procedures relative to email, such as [Acceptable Use of State Systems Policy](#) and others listed under 'References' in this Policy. The Agency retains the ability to open and collect email in order to adhere to the Freedom of Information Act (FOIA) and open records laws, investigate internal and external agency compliance matters and conduct routine compliance audits. The agency maintains the ability to decrypt any email and no additional presumption of privacy should be assumed by a DMHAS user when sending an encrypted email.

Each user that either sends or receives an encrypted email will be required to generate an "encryption key" that can only be used by the intended user.

- The encryption key is generated by the user.
- The encryption key requires a password/passphrase unique to the user and maintained by the user.
- Use of the encryption key requires the user to enter the password/passphrase when using the encryption application and when restarting the Outlook application.
- An encryption key can be backed up for recovery purposes.