STATE OF CONNECTICUT
Department of Mental Health & Addiction Services

dmhas Department of Mental Health and Addiction Services

Commissioner's Policy Statement and Implementing Procedures

SUBJECT:	DMHAS Security for Mobile Computing and Storage Devices
P & P NUMBER:	Chapter 7.7
APPROVED:	Miriam Delphin-Rittmon, Commissioner Date: 3/29/2016
EFFECTIVE DATE:	February 9, 2016
REVISED:	
REFERENCES:	CT.GOV/OPM - Policy on Security for Mobile Computing and Storage Devices CT.GOV/OPM - Acceptable Use of State Systems Policy of November, 2006 DMHAS Commissioner Policy and Directives: 3.13 Unauthorized Disclosure and Breach Notification of Unsecured PHI 7.2 Computer Use Policy 7.4 Computer Access Controls 7.6 Computer Policy on Investigations, FOI Request and Monitoring HHS.GOV/OCR - HIPAA Security Rule
FORMS AND ATTACHMENTS	

STATEMENT OF PURPOSE: The purpose of this policy is to ensure that all requirements as set forth by the CT.GOV/OPM "Security for Mobile Computing and Storage Devices Policy" are met and to address additional DMHAS specific restrictions and requirements. This policy covers all DMHAS staff, consultants, contracted individuals, students, per-diems, interns, volunteers, locums, etc., and anyone who has access to protected data as defined within this policy or associated applicable policies.

POLICY: DMHAS Mobile Computing and/or Storage Devices[i] (MC/SDs) are regulated by the CT.GOV/OPM "Security for Mobile Computing and Storage Devices Policy." This policy additionally defines MC/SDs as any portable electronic computing, storage and/or telecommunications devices that can execute programs/applications and/or store electronic data. Failure to store Confidential or Restricted State data (C/RSD)[ii], Electronic Patient Health Information (ePHI)[iii] or other protected data as set forth in this and its associated policies may result in sanctions and/or disciplinary action up to and including termination of employment.

PROCEDURE:
The DMHAS restricts Mobile Computing and/or Storage Device use as follows:

1. Only DMHAS purchased or approved MC/SDs are allowed for use.

2. Users must obtain prior approval by the DMHAS Director of Information Technology (or designee).

3. MC/SDs are allowed to be used only for storage / transport of C/RSD or ePHI after all of the following conditions have been met:
    a. Receipt of a fully completed DMHAS - Mobile Data Control Form signed by the Commissioner (or designee) to document having met these CT.GOV/OPM MC/SD policy requirements that:
        i. The sensitivity of the data has been assessed, and it was determined that the business need necessitating its storage on a MC/SD:
            1. Is due to there being no reasonable alternative means to provide the user with secure remote data access at the time of occurrence,
            2. Outweighs the associated risk of loss or compromise
        ii. The storing of protected data on a MC/SD:
            1. Is necessary to conduct DMHAS business operations,
            2. Is only the minimum data necessary to perform the specific business function,
            3. Will be only for the minimum time needed to perform the business function,
            4. Is encrypted utilizing a method meeting DAS / BEST requirements and was performed by staff designated by the DMHAS Director of Information Technology or designee;
            5. Will be tracked and audited by the DMHAS.
        iii. All associated risks have been accepted.
    b. Receipt of signed, formal acknowledgement(s) from user(s) indicating that they understand, and agree to abide by the rules of this and its associated applicable policies.

4. DMHAS users in the possession of a MC/SD must not leave the MC/SD unattended at any time, and must take all reasonable and appropriate precautions to protect and control the MC/SD from unauthorized physical access, tampering, loss or theft.

5. In the case of theft, loss, misplacement of a MC/SD (regardless of types of data stored) and/or the user has determined non-authorized access or disclosure of information stored on the MC/SD has occurred, all of the following steps must be taken:
    a. For any loss or theft regardless of where it occurred; the user is responsible for immediately notifying all of the following:
        i. Local DMHAS agency police, or if not applicable, the Central Investigative Unit within the DMHAS Office of Safety Services (860)-262-5326.
        ii. Local municipal police only in the case of theft that occurs anywhere other than on State of Connecticut property

iii. DMHAS Central IT and provide all applicable account and device information;
    1. During normal business hours call 860-262-5058,
    2. After normal business hours call 860-262-5000 and ask for the on-call technical support person to be paged to call you back.
iv. The user's supervisor and the facility's Chief Executive Officer (CEO) who are required to notify the DMHAS Director of Compliance.

b. If the MC/SD has associated phone or data accounts, the user is responsible for immediately notifying the facility's business office and provide all applicable account and device information to have the phone or data account disabled and/or deactivated.

c. The user is responsible for obtaining, completing, submitting any forms and/or reports as required; including but not limited to: CO-853 and (in the event of a theft) a police report from DMHAS, local municipality or State of CT Police as applicable dependent upon the property where the theft occurred.

6. If a MC/SD is no longer needed by the user to whom it was assigned to, it must be returned to IT so that tracking and or disposal will be conducted in accordance with applicable CT.GOV/OPM policies.

---

[i] Mobile Computing and/or Storage Devices includes but is not limited to;
a.) Laptops, notebooks, tablets, smartphones or cell phones with internet browsing capability etc.
b.) Electronic storage media equipment such as diskettes, magnetic tape, external/removable hard drives, flash drives, flash cards (e.g., SD, Compact Flash), USB memory devices, jump drives, compact disks, digital video disks, etc.

[ii] Confidential or Restricted State Data includes but is not limited to;
a.) Personally identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual
b.) Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals.

[iii] Protected Health Information (ePHI / PHI) is health information that could reveal the identity of a person including but is not limited to : name, street address, city, county, precinct, zip code, dates (except year) that directly relate to a person (including , social security number, birth date, admission date, medical record number, health plan beneficiary number, discharge date, date of death, and all ages over),telephone numbers, fax numbers, e-mail addresses· account number, certificate/license number, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locator (url), internet protocol (ip) address number, biometric identifiers (for example, finger or voice prints), full face photographs or similar images (unique tattoo's or unique physical attributes, etc.), any unique identifying number, characteristic or code.