Department of Behavioral Health

TRANSMITTAL LETTER

SUBJECT **Issuance and Use of Wireless Communication Devices and Other Portable Technology Equipment**		
POLICY NUMBER **DBH Policy 811.1**	**DATE** JAN 1 3 2016	**TL#** 297

Purpose. To establish the criteria for the issuance, use, and maintenance of wireless communication devices and other portable technology equipment (as defined in Section 5e below), in compliance with federal and District privacy laws and regulations.

Applicability. Department of Behavioral Health (DBH) employees (including interns, residents, and contracted medical professionals). Also see Section 9 regarding DBH-certified providers and contractors.

Policy Clearance. Reviewed by affected responsible staff and cleared through appropriate Behavioral Health Authority (BHA) offices.

Effective Date. This policy is effective immediately.

Superseded Policy. Supersedes DMH Policy 811.1C, Wireless Communication Devices and Other Portable Technology, dated January 10, 2013

Distribution. This policy will be posted on the DBH web site at www.dbh.dc.gov under Policies and Rules. Applicable entities are required to ensure that affected staff is familiar with the contents of this policy.

Tanya A. Royster, M. D.
Director, DBH

GOVERNMENT OF THE DISTRICT OF COLUMBIA DEPARTMENT OF BEHAVIORAL HEALTH	Policy No. 811.1	Date JAN 1 3 2016	Page 1
	Supersedes DMH 811.1C, Wireless Communication Devices and Other Portable Technology, dated January 10, 2013		

Subject: Issuance and Use of Wireless Communication Devices and Other Portable Technology Equipment

1. **Purpose**. To establish the criteria for the issuance, use, and maintenance of wireless communication devices and other portable technology equipment (as defined in Section 5e below), in compliance with federal and District privacy laws and regulations.

2. **Applicability**. Department of Behavioral Health (DBH) employees (including interns, residents, and contracted medical professionals). Also see Section 9 regarding DBH-certified providers and contractors.

3. **Authority**. Department of Behavioral Health Establishment Act of 2013; Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended; the District Mental Health Information Act (MHIA) of 1978, as amended; and 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records.

4. **Policy**. DBH will support maximum productivity and cost-effectiveness when employing wireless communication devices and other portable technology equipment in service delivery and in effectively managing the usage of these devices by employees, while also ensuring protected health information (PHI) is secured.

5. **Definitions**.

5a. Consumer/client - individuals receiving behavioral health services or supports from DBH or DBH-certified or contracted providers

5b. Secure Network Drives – For purposes of this policy, secure network drives include the employee's personal drive (H drive), or a program or office shared drive (S). The Global Drive (W) is not considered a secure Network Drive. PHI should never be stored on the Global (W) drive, which has unlimited access, unless in a restricted folder.

5c. Protected Health Information (PHI) - Any written, recorded, electronic (ePHI) or oral information created or received by DBH or its providers which either (1) identifies, or could be used to identify, a consumer/client; or (2) relates to the past, present, or future physical or behavioral health or condition of a consumer/client; the provision of health care to a consumer/client; or the past, present, or future payment for the provision of health care to a consumer/client.

5d. Sensitive Information – Any confidential information such as PHI, privileged information under attorney/client relationship, information related to privacy act, or proprietary information.

5e. Wireless communication devices and other portable technology equipment – A device that transmits and receives data, text, and/or voice without being physically connected to a network. This definition includes but is not limited to such devices as cellular telephones, laptops, flash drives, pagers, wireless internet services, wireless data devices (e.g., blackberry devices), wireless air cards, and cellular telephone/two-way radio combination devices and satellite phones.

5f. Encrypted – The reversible conversion of readable information into unreadable, protected form so that only a recipient who has the appropriate "key" can convert the information back into original readable form.

5g. Virtual Private Network (VPN) – A system that extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network. This is done by establishing a virtual point to point connection through the use of dedicated connections, encryption, or a combination of the two.

6. **Procedures and Responsibilities**.

6a. Employee qualifications to receive portable communication devices. The employee shall meet one or more of the following criteria in order for a wireless communication device to be assigned:

(1) The duties of the position or assignments are such that immediate emergency response is critical to successfully carrying out the job;

(2) The duties of the position or assignments require response and decision-making to life-threatening or other safety issues and situations;

(3) The duties or assignments associated with the position make it necessary that the incumbent be accessible to communicate with senior management or job-related stakeholders at any time;

(4) The duties of the position require a significant amount of travel during regular work hours, making the wireless device a productivity enhancement tool; or

(5) The duties of the position may lead to potentially dangerous scenarios and situations and there is no acceptable and reliable alternative communication system.

6b. The Employee shall:

(1) Exercise reasonable care in securing, protecting, handling and transporting DBH-issued devices. Employees shall not leave the devices unattended in vehicles, in unsecured office space, or in any other unsecured location outside of the employee's possession or control.

(2) Store PHI on Secure Network Drives in folders that are only accessible by individuals with a need to know the information.

(3) Safeguard and secure their DBH-issued passwords. Employees are prohibited from sharing or disclosing their passwords to other DBH employees unless required by business necessity.

(4) Encrypt any e-mail transmission containing protected health information sent to an authorized recipient outside of the dc.gov e-mail domain.

(5) Encrypt all e-mail transmissions that contain files or attachments with protected health information. This includes transmissions within the dc.gov e-mail domain. Employees with the need to routinely send files and spreadsheets through e-mail as part of their official duties shall request that the DBH CIO install encryption software on their work computer and shall utilize the encryption software when sending e-mails under this subsection.

(6) Limit the amount of protected health information contained in any e-mail transmissions to the minimum necessary. Employees shall not use full names, dates of birth, or Social Security Numbers in any e-mail when the purpose of the transmission can be accomplished with initials and other de-identified information.

(7) Not use USB (flash drives) unless approved in advance by the DBH Chief Information Officer or designee and the USB drive is encrypted. Employees shall immediately delete the PHI from the flash drive when the transfer of data is complete and return the flash drive to the DBH CIO or designee.

(8) Ensure that any laptops that will contain PHI are encrypted.

(9) Account for any and all PHI contained on the portable device in the event that a portable device is lost /stolen.

(10) Follow the chain of command for approval when requesting a wireless communication device and other portable technology equipment with appropriate justification depending on job requirements (see Exhibit 1, Request Form for Wireless Communication Device and Other Portable Technology Equipment):

(a) Supervisor
(b) Program Manager/Department Head
(c) DBH Chief Information Officer/designee

(11) Use portable communication devices for official business purposes only and in compliance with this policy and all applicable federal and District laws, rules, and regulations. Any improper use of DBH issued wireless devices may result in employee disciplinary action up to and including termination.

(12) Complete and sign the Record of Acknowledgement of Receipt of Wireless Communication Device (Exhibit 2), and provide form to DBH Information Services.

(13) Not use the portable device while driving.

(14) Not access, download, view, or transmit sexually explicit material (including

pornography), fraudulent information, harassing material, or racially derogatory information.

(15) Not store any data on the equipment that is not business-related (e.g. music, video, etc.).

(16) Not access PHI from any personally-owned wireless communication device unless using VPN technology.

(17) Report inoperable or damaged portable communication device to his/her supervisor and DBH Information Services within twenty four (24) hours upon discovery.

(18) Report lost, missing, stolen, portable communication device to his/her supervisor and DBH Information Services at DBHIT@dc.gov immediately, within one (1) hour, and complete a Major Unusual Incident report, in accordance with DBH Policy 480.1C, Reporting Major Unusual Incidents (MUIs) and Unusual Incidents (UIs).

(19) Return wireless communication device and other portable technology equipment to DBH Information Services upon separation from DBH, or when the qualifications stated in Section 6a above are no longer applicable.

(20) Immediately report any transmission of PHI sent to the wrong recipient by contacting the DBH Privacy Officer.

6c. The Supervisor shall:

(1) Review employee's requests per requirements of his/her position description and job assignments.

(2) Ensure that use of device or equipment is for approved reasons and in compliance with this policy and all applicable federal and District laws, rules, and regulations.

(3) Be responsible for controlling and managing wireless devices and related services. Ensure that no employee is permitted to exchange, upgrade, or substitute his/her wireless communication device without approval of DBH Information Services. A wireless device is only to be used by the individual to whom it is issued.

(4) Reasonably monitor employees' compliance with this policy.

(5) Ensure that employees are aware of the dangers associated with driving while using wireless devices, particularly while driving a government vehicle.

(6) Closely manage and monitor allocation of wireless communication devices to employees. This includes assessing an employee's use both prior to ordering a new device and periodically thereafter; and contacting DBH Information Services prior to an employee's separation/transfer to confirm what portable devices have been issued to the employee and ensure devices are returned.

(7) Follow employee separation procedures, including notification of the Division of

Human Resources, financial officer, and DBH Information Services when an employee is separating from DBH (see DBH Policy 770.1 Clearance of Personnel for Separation or Transfer).

(8) Ensure that the employees who no longer meet the qualifications stated in Section 6a above return the portable device to DBH Information Services.

6d. The Chief Information Officer/designee shall:

(1) Be responsible for procurement, installation, selection of mobile devices, equipment and peripherals in accordance with the DC Office of the Chief Technology Office (OCTO) and DBH standards and inventory control. The CIO is responsible for ensuring that the Department's use and issuance of mobile devices complies with the privacy and security requirements in the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations.

(2) Ensure that all wireless devices, including laptops and smart phones, issued to DBH staff are encrypted prior to issuance with passwords that exceed six (6) digits and letters.

(3) Monitor through periodic inspection and coordination with the DBH privacy office DBH employees' compliance with this policy.

(4) Maintain tracking records whenever property is distributed to individuals or returned. Also see Section 6b (5) above.

(5) Provide support and maintenance for portable devices and peripherals.

(6) Communicate to users that when using these devices/equipment, security can be compromised. Employees are to use caution and good judgment when communicating sensitive information via wireless devices.

(7) Ensure that established protocols are followed and documented accordingly in the case of lost, missing, or stolen wireless devices.

(8) Provide final approval of requests for portable communication devices/peripherals in accordance with Section 6a above, which includes justification and recommendation of employee's supervisor. Provision of portable communication devices/peripherals is contingent upon availability of DBH resources.

(9) Immediately disable and wipe lost devices that cannot be retrieved.

7. **Consequences for Unauthorized Use of Wireless Communication Devices and Other Portable Technology Equipment**.

7a. The unauthorized use of wireless communication devices and other portable technology equipment is prohibited. Violations of this policy constitute neglect of duty and may result in removal of assigned equipment, reimbursement by DBH employee for replacement, and/or disciplinary action including termination (see District Personnel Manual, Chapter 16 for guidelines).

7b. Any unauthorized or inappropriate use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems, by the user or by another who has been permitted or enabled access to the system by the user, may subject the user to criminal and civil sanctions pursuant to federal and state law as well as disciplinary action.

8. **Reimbursement**. Employees shall reimburse the Department for the cost of any device issued under this policy that is lost, stolen or damaged as a result of the employee's intentional or negligent action. DBH reserves the right to recoup the value of any unreturned, damaged, or lost property that was loaned to a DBH employee through all appropriate means, including deductions from the employee's final pay check, on a case by case basis.

9. **Specific Guidance for DBH Certified Providers and Contractors**.

9a. DBH certified providers and contractors who have an agreement with DBH to provide mental health or substance use disorder services and supports shall have policies and procedures in place to:

(1) Ensure the confidentiality and security of PHI owned and/or maintained by the District of Columbia in all formats and computer systems in accordance with HIPAA, MHIA, 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records, and the DBH Privacy Manual, as applicable.

(2) Prohibit storing any PHI on wireless communication devices unless the device is encrypted to ensure that PHI is appropriately safeguarded from unauthorized access.

9b. Failure to ensure compliance with HIPAA, MHIA, 42 CFR Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records and the DBH Privacy Manual may result in consequences pursuant to the provider's contract with DBH, in addition to federal and District civil and criminal actions.

9c. The DBH Office of Accountability will monitor DBH certified providers during routine reviews to ensure policies are in place regarding the protection of PHI on wireless communication devices as stated above.

10. **Training**. The DBH Information Services will provide training on this policy to DBH employees who receive portable communication devices.

11. **Related References**.

DBH Policy 623.1 Accountability for Government Property
DBH Policy 480.1C Reporting Major Unusual Incidents (MUIs) and Unusual Incidents (UIs)
DBH Policy 770.1A Clearance of Personnel for Separation or Transfer
DBH Policy 645.1, DBH Privacy Policies and Procedures
District of Columbia Mental Health Information Act of 1978, as amended (MHIA)
Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA)
Health Information Technology for Economic and Clinical Health Act (HITECH)
42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records.

12. **Exhibits**.

Exhibit 1 – Request Form for Wireless Communication Device & Other Portable Technology
Exhibit 2 – Record of Acknowledgement of Receipt of Wireless Communication Device

Approved by:

Tanya A. Royster, M. D.
Director, DBH

(Signature) 1/13/2016 (Date)

REQUEST FORM FOR WIRELESS COMMUNICATION DEVICE AND OTHER PORTABLE TECHNOLOGY EQUIPMENT

Instructions: Follow the chain of command for approval when requesting wireless communication device and other portable technology equipment with appropriate justification depending on job requirements:

Requested by: _____ Date: _____
Employee Name and Title

Type of Device Requested (Wireless communication device and other portable technology equipment – a device that transmits and receives data, text, and/or voice without being physically connected to a network). This definition includes but is not limited to such devices as cellular telephones, laptops, flash drives, pagers, wireless internet services, wireless data devices (e.g., blackberry devices), wireless air cards, and cellular telephone/two-way radio combination devices and satellite phones.

Justification (Check all that apply):

Employee qualifications to receive portable communication devices. The employee shall meet one or more of the following criteria in order for a wireless communication device to be assigned:

( ) The duties of the position or assignments are such that immediate emergency response is critical to successfully carrying out the job;

( ) The duties of the position or assignments require response and decision-making to life threatening or other safety issues and situations;

( ) The duties or assignments associated with the position make it necessary that the incumbent be accessible to communicate with senior management or job-related stakeholders at any time;

( ) The duties of the position require a significant amount of travel during regular work hours, making the wireless device a productivity enhancement tool; or

( ) The duties of the position may lead to potentially dangerous scenarios and situations, and there is no acceptable and reliable alternative communication system.

Approvals	Signature	Date
Supervisor		
Program Manager/Department Head		
DBH Chief Information Officer/designee		

RECORD OF ACKNOWLEDGEMENT OF RECEIPT OF WIRELESS COMMUNICATION DEVICE

PROPERTY ISSUED TO:	AGENCY	OFFICE/DIVISION	LOCATIC
Name:_____ (Last) (First) (MI)			

I have received the item(s) listed below on: (insert date of receipt) _____. **I understand and agree to the following per DBH Policy 811.1, Wireless Communication Devices and Other Portable Technology Equipment:**

(1) Exercise reasonable care in securing, protecting, handling and transporting DBH-issued devices. I will not leave the device unattended in vehicles, in unsecured office space, or in any other unsecured location outside of my possession or control.

(2) Store PHI on Secure Network Drives in folders that are only accessible by individuals with a need to know the information.

(3) Safeguard and secure my DBH-issued passwords. I acknowledge that I am prohibited from sharing or disclosing my passwords to other DBH employees unless required by business necessity.

(4) Encrypt any e-mail transmission containing protected health information sent to an authorized recipient outside of the dc.gov e-mail domain.

(5) Encrypt all e-mail transmissions that contain files or attachments with protected health information. This includes transmissions within the dc.gov e-mail domain. If I have a need to routinely send files and spreadsheets through e-mail as part of my official duties, I agree to request that the DBH CIO install encryption software on my work computer and shall utilize the encryption software when sending e-mails under this subsection.

(6) Limit the amount of protected health information contained in any e-mail transmissions to the minimum necessary. I will not use full names, dates of birth, or Social Security Numbers in any e-mail when the purpose of the transmission can be accomplished with initials and de-identified information.

(7) Not use USB (flash drives) unless approved in advance by the DBH Chief Information Officer or designee and the USB drive is encrypted. When authorized to USB, I agree to immediately delete the PHI from the flash drive when the transfer of data is complete and return the flash drive to the DBH CIO or designee.

(8) Ensure that any laptops that will contain PHI are encrypted.

(9) Understand that portable communication devices are for official business purposes only and in compliance with this policy and all applicable federal and District laws, rules, and regulations. Any improper use of DBH issued wireless devices may result in employee disciplinary action up to and including termination.

(10) Not use the portable device while driving.

(11) Not access, download, view, or transmit sexually explicit material (including pornography), fraudulent information, harassing material, or racially derogatory information.

(12) Not store any data on the equipment that is not business-related (e.g. music, video, etc.).

(13) Not access PHI from any personally-owned wireless communication device unless using VPN technology.

(14) Take reasonable measures to prevent the inadvertent communication of protected health information to the wrong person and to immediately report to the DBH Privacy Officer any inadvertent communications.

(15) Report inoperable or damaged portable communication device to his/her supervisor and DBH Information Services within twenty four (24) hours upon discovery.

(16) Report lost, missing, stolen, portable communication device to his/her supervisor and DBH Information Services at DBHIT@dc.gov immediately, and within one (1) twenty four (24) hours or the next business day upon discovery, and complete a Major Unusual Incident report, in accordance with DBH Policy 480.1C, Reporting Major Unusual Incidents (MUIs) and Unusual Incidents (UIs).

(17) I will return wireless communication device and other portable technology equipment to DBH Information Services upon separation from DBH, or when my job assignments no longer qualify me to have this device per Section 6a of DBH Policy 811.1.

The unauthorized use of wireless communication device and other portable technology equipment is prohibited. Violations may result in removal of assigned equipment, reimbursement by employee for replacement, and/or disciplinary action including termination (see District Personnel Manual, Chapter 16 for guidelines).

Any unauthorized or inappropriate use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems, by the user or by another who has been permitted or enabled access to the system by the user, may subject the user to criminal and civil sanctions pursuant to federal and state law as well as disciplinary action.

Reimbursement. I agree to reimburse the Department for the repair or replacement costs of the device identified below lost, stolen or damaged as a result of my intentional or negligent conduct or failure to comply with DBH Policy 811.1. I acknowledge that the Department reserves the right to recoup the value of any unreturned, damaged, or lost property that was issued to me through all appropriate means on a case by case basis, including from my pay check.

Item No.	Description	Model	Serial #	Accessories

Signature of Recipient: _____ Date : _____

Signature of Issuer: _____ Date: _____

Printed Name and Title of Issuer: _____