BHS Policies and Procedures	
City and County of San Francisco Department of Public Health San Francisco Health Network BEHAVIORAL HEALTH SERVICES	1380 Howard Street, 5th Floor San Francisco, CA 94103 (415) 255-3400 FAX (415) 255-3567
Policy or Procedure Title: **BHS-IT Mobile Device and Cellular Service Policy and Procedures**	
Issued By: DocuSigned by: David Nish 39FA1D58CE444DA... David Nish Director of Operations Date: September 14, 2022	Manual Number: 2.07-3 References:

Equity Statement: The San Francisco Department of Public Health, Behavioral Health Services (BHS) is committed to leading with race and prioritizing Intersectionality, including sex, gender identity, sexual orientation, age, class, nationality, language, and ability. BHS strives to move forward on the continuum of becoming an anti-racist institution through dismantling racism, building solidarity among racial groups, and working towards becoming a Trauma-Informed/Trauma Healing Organization in partnership with staff, clients, communities, and our contractors. We are committed to ensuring that every policy or procedure, developed and implemented, leads with an equity and anti-racist lens. Our policies will provide the highest quality of care for our diverse clients. We are dedicated to ensuring that our providers are equipped to provide services that are responsive to our clients' needs and lived experiences.

Policy: The San Francisco Department of Public Health Behavioral Health Services (BHS) may issue mobile devices, data cards, and/or mobile hotspots for cellular services to staff when necessary for work-related communications. At present, staff who are providing services in the field will be prioritized to receive mobile devices and cellular service.
This policy defines user eligibility and requirements for continued use. This policy provides guidance for staff requiring BHS-issued cellular service support and defines appropriate usage and maintenance with the goal of maintaining low telecommunication cost for the department.

II. Definitions:

Mobile Device

This refers to any mobile phone, smartphone, or media tablet.

Wireless Internet Cards, Mobile Hotspots, and MiFis

These are cards or devices that allow connectivity to a wireless carrier's cellular network. These allow the user to access the internet from any location. MiFi is a brand name used to describe a wireless router that acts as mobile Wi-Fi hotspot.

Connected Media Tablet

A tablet is an open-face wireless device with a touchscreen display and without physical keyboards. The primary use is the consumption of media; it also has messaging, scheduling, email, and internet capabilities. Screen diagonal dimensions are typically between 5 inches and 10 inches.

III. Approved Reasons for Use

- To provide services that necessitate a mobile phone, wireless card/MiFi, or connected media tablet to support the mission of SFDPH and BHS.
- To maintain the reliability of the systems, infrastructure, and operations to support BHS services.

IV. Policies, Procedures, and Use

A. General

All mobile devices, whether provided by BHS or owned by staff, that have access to BHS systems and applications (for example, DPH Outlook, Teams, Zoom, Avatar, and/or Epic) are governed by this policy. Devices and cellular data use are also subject to all rules and requirements found in the Annual Compliance and Privacy Training as well as Cybersecurity Training *(link to guidelines requested from Compliance*). Note: Applications, including cloud storage software used by staff on their own personal devices are also subject to this policy.

The following general procedures and protocols apply to the use of all mobile devices for work purposes:

- Mobile computing devices must be protected with a password required at the time the device is powered on.
- Passwords must meet the requirements outlined in both the SFDPH Compliance and Privacy Training and Cybersecurity Training [*we wrote to Compliance for links*].
- All data stored on mobile devices shall be encrypted.
- Wireless encrypted security and access protocols shall be used with all wireless network connections.
- Staff shall refrain from using public or unsecured network connections while using their mobile device for work.
- Personal mobile computing devices that require network connectivity must conform to all DPH-IT standards for use and configuration.
- Unattended mobile devices shall be physically secured.
- Mobile devices that access the SFDPH network shall have active and up-to-date anti-malware and firewall protection.
- Devices shall have location services enabled. If the device is lost or stolen, the device will be “bricked” or wiped of all information so they are unusable until recovered or destroyed.

B. User Responsibilities

The following procedures and requirements shall be followed by all users of mobile devices:

- Staff shall immediately report any lost or stolen devices.
- Unauthorized access to a mobile device or data must be immediately reported.
- Mobile devices shall not be “rooted” or have unauthorized software/firmware installed.
- Staff shall not load illegal content or pirated software onto any mobile device.
- Only approved applications are allowed on mobile devices that connect to the SFDPH network.
- Mobile devices and applications shall be kept up-to-date.
- Operating system and application patches should be installed within 30 days of release.
- Staff shall use their SFDPH email when sending or receiving PHI via email.
- Mobile Device Management (MDM) will be used to enforce common security standards and configurations on devices.
- Staff shall not modify configurations.
- Cellular service must be used for work-related activities only, except in cases of emergences (e.g., contacting children, doctors, or family members in urgent situations). Any personal use of cellular service must not interfere with normal conduct of City business. This includes all incoming and outgoing calls, internet, and/or data usage.
- Mobile device for cellular service will be purchased, maintained, and supported through direct billing to the division where the device is used.

- Users must comply with both safety and privacy requirements, as applicable, when carrying or using devices. *Under California state law, mobile device use while driving a motor vehicle is prohibited unless a "hands-free" device is used. While in a vehicle, users must adhere to all traffic safety rules and must pull over to the side of the road to use the device.*
- Users are responsible for the appropriate use and care of the equipment. Loss, theft, or damage must be reported immediately to the designated contact person (usually manager or supervisor). Employee/user will be responsible for the cost of replacement equipment unless justified by department's division head.
- User must contact manager and Telecom.Request@sfdph.org when receiving any message for data use overages.
- When employees leave the City & County of San Francisco, they must turn in all equipment to their manager. The manager is responsible for storing or returning the device and will return the device to BHS-IT. If staff transfer to another BHS program, they may transfer the number and equipment (upon IT and manager approvals) to their new program.

Accountability for Mobile Device and Cellular Data Use

The head of each BHS section or unit operating under the authority of this policy has the responsibility to maintain accountability regarding devices and cellular service usage. Directors/managers must develop a process to monitor devices and usage to ensure that employees are following these policies and to verify that the device continues to be required for the staff person's scope of work. Specifically, BHS directors and/or managers are responsible for the following:

- Devices and cellular service can only be approved and requested by a manager
- Quarterly review and approval of DPH-owned mobile device usage and bills
- Maintenance of a current listing of all active cellular services
- Review, bi-annually, of BHS-issued mobile device usage and cellular services to eliminate payment for unnecessary devices and ensure cost-effective rate plans are employed
- Cellular service will automatically be suspended after 6 months of non-usage without notice and may be disconnected, unless used as emergency line
- If device or data is for emergency use only, please notify Telecom.Request@sfdph.org to temporarily suspend or activate

V. Type of Equipment, Features, and Rate Plans

The contact person (manager or supervisor) in charge of equipment from each BHS program will work with the staff member being issued a mobile device to determine the most appropriate type of equipment, features, and rate plan. While it is important to determine what the staff needs to fulfill their duties, decisions should also consider cost. The need for equipment, features, and rate plans beyond the standard must be justified and documented.

Note: Selecting a plan that does not support an employee's monthly usage will result in overcharges to the requesting department. Staff may contact Telecom.Request@sfdph.org for changes in equipment, features, and rate plans.

VI. Device Requests and Agreements

Acknowledgement Form for Mobile Device (attached)

Fill out the Acknowledgment Form after receiving device

1. Form will be needed for completion once employee receives device
2. If a person other than user is picking up device, the form will be emailed to user to be filled out

Communication Device Request Process and Form for Ordering Devices

Fill out the Communication Device Request Form

1. Form can be requested by sending email to Telecom.Request@sfdph.org.
2. Fill out form and email to Telecom.Request@sfdph.org and it will then be reviewed and approved/denied by the Chief Information Officer of Public Health.
3. A quote will be requested from vendor and quote and CDR form will need to be certified by accounting or finance/budget manager
4. Request will be sent to IT Procurement for processing

IMPORTANT: All users must agree to and accept this policy by signing below prior to issuance of a device or cellular service.

I have read and understand the above policy and agree to fully comply with all expectations and requirements contained therein. (Please print your name and sign below if you agree and keep a copy of this memorandum for your record.)

Check ONE that is being requested:
☐ Cellular Phone ☐ Smart Phone ☐ Mobile Hotspot ☐ Connected Media Tablet
¨ Other _____

_____	_____	_____
PRINT NAME OF USER	USER SIGNATURE	DATE
_____	_____	_____
PRINT NAME OF MANAGER	MANAGER SIGNATURE	

Distribution:
BHS Policies and Procedure are distributed by the DPH Quality Management Office of Regulatory Affairs

Administrative Manual Holders
BHS Programs
SOC Program Managers
BOCC Program Managers
CDTA Program Managers