DEBORAH SPECIALTY PHYSICIANS

BRING YOUR OWN DEVICE (BYOD)

Purpose:

The use of Personal Devices (defined to include, but not be limited to, smartphones, tablets, notebooks, laptops) has become commonplace for both our personal and professional lives. Deborah Specialty Physicians ("DSP") understands that there are benefits to allowing employees to use their personal devices for work-related tasks. This raises safety, privacy, and timekeeping concerns however that must be addressed. This policy provides guidelines for appropriate use of personal devices in the workplace and is designed to protect the confidentiality of protected information and improve staff efficiency.

Policy:

- Use of Personal Devices at work should be limited to work-related activities. If Personal Device use is necessary when interacting with patients or others, it is incumbent upon the user to inform patients that the Personal Device is in use for work-related reasons or the furtherance of patient care activities. Non-work-related activities on Personal Devices is to be kept to an absolute minimum.
- DSP will use its discretion to determine which employees may use Personal Devices to perform work-related activities and/or connect to hospital network applications or directories. Use of Personal Devices may not be appropriate for all employees. Use of Personal Devices is voluntary and will be permitted under specific circumstances for secure communications and access to computer systems containing Electronic Protected Health Information (ePHI). All employees must submit a signed and dated copy of this policy prior to requesting access through the use of a Personal Device.
- Any user who desires "active-sync" real-time access to emails and calendars through the native apps on their Personal Device must complete and sign DHLC form APM.111.AS.
- Under no circumstances shall orders be initiated through secure messaging. Orders must continue to be initiated through the EHR or, when permitted, DSP's verbal order protocol.
- The sending of sensitive PHI including, but not limited to, mental health, HIV, drug and alcohol, genetics and issues relating to minors via any form of messaging is prohibited, even when HIPAA and HITECH standards and encryption requirements are met.
- Use of shorthand, abbreviations, brevity and any "auto-correct" function is discouraged due to the risk of misinterpretation of message content.
- Secure messages are not sent to or stored in the EHR. Any information related to the patient's care or medical decision-making must be documented in the patient's records in the EHR
- If a misdirected transmission should occur, the sending user must notify the erroneous recipient of the error and the erroneous recipient should immediately delete the message without reading it. If the incident is deemed to be reportable from a compliance standpoint, the sending user must also inform the HIPAA Security Officer and the Privacy Officer of the error.
- All data transmitted for work-related purposes via Personal Devices is DSP's sole property. There should be no expectation of privacy for any work-related information received, sent, or stored on a Personal Device. DSP has an absolute right of access to all of the work-related information and may exercise its right whenever it is deemed reasonable and necessary by management.
- All applications on employees' Personal Devices used to access DSP data will be fully compliant with HIPAA and HIPAA-related rules as they may change from time to time.
- Personal Devices and third-party applications (refer to Third-Party Applications section below) must remain up-to-date, as older versions may not meet current security standards. DSP's IS department will advise whether a device or particular versions of an operating system or an app is supported. It is your responsibility to maintain the latest versions of security software on your Personal Device.
- Security settings may not be altered and employees using their Personal Devices will provide DSP access to any Personal Device when requested or required for DSP's legitimate business purposes, including without limitation in the event of a security incident or investigation for the search of work-related information. DSP will not be responsible for loss or damage of personal applications or data resulting from the use of DSP applications or the wiping of DSP information.

DEBORAH SPECIALTY PHYSICIANS

BRING YOUR OWN DEVICE (BYOD)

- All costs associated with use of a Personal Device shall be borne by the employee, unless otherwise stated in writing. The secure messaging tool furnished by DSP uses a negligible amount of data on a data plan unless large files or video are shared. Any data transmitted over the Deborah Wi-Fi network will not result in data charges. DSP takes no financial responsibility for the impact access using a Personal Device will have on a data plan.
- Personal Devices in patient care areas must be cleaned at least daily in accordance with infection control best practices.
- When and where you may use Personal Devices within DSP property is subject to the general policies covering the usage of Personal Devices. Use of Personal Devices in certain Office Practice areas of or under certain circumstances, may be prohibited to safeguard against security concerns, and may interfere with certain medical equipment. Personal Devices may not be used in any area where mobile phone usage is not permitted.
- Employees are prohibited from using Personal Devices while driving, in accordance with State Law. You must pull to the side of the road and safely stop the vehicle before reviewing emails or text messages. If your vehicle has a Bluetooth or other hands-free device, making and receiving calls and the initiation and read-back of text messages via speech-based virtual assistant tools is permitted, including conversion of speech to text provided you are able to do so safely. Use of Personal Devices while driving is otherwise prohibited. You are expected to exercise the utmost caution and place safety first. The user will be solely responsible for any traffic violations or other fines and penalties results from the use of the Personal Device. If you are charged with a traffic violation resulting from the use of Personal Devices while driving, you will be solely responsible for all liabilities that result from such actions.
- To ensure the confidentiality of PHI, a user may not use traditional text messaging or multimedia messaging services when sending electronic Protected Health Information (ePHI) or any other type of work-related data via a Personal Device.
- All text-based correspondence between employees that would have otherwise been transmitted through traditional text messaging must be transmitted exclusively through DSP's secure messaging platform. This will allow for appropriate audit trails of correspondence to be tracked, should it be necessary.
- DSP policy prohibits sharing of secure or sensitive information including screen capture with users who are not bound by the organization's security and privacy policies.
- Two levels of security are required for all Personal Devices and enterprise applications used in the workplace. All devices must have their own passwords or use touch ID to ensure no unauthorized access to your content is available. Personal Devices must lock after no more than five minutes of inactivity to protect the phone from unauthorized accesses.
- Hourly (non-exempt) employees may never use their Personal Devices for work purposes during unpaid periods - that is when not "on the clock" and being paid, with the exception of "de minimis" activities such as checking work schedules or brief communications with managers. Exempt staff may not use their Personal Devices for work purposes during periods of unpaid leave, with the same exceptions referenced directly above.
- DSP reserves the right to periodically audit user device settings and to deactivate access to DSP software, emails, documents and other information on an employee's Personal Device during periods of leave or when otherwise deemed appropriate.
- All Personal Devices used to conduct DSP business are subject to acceptable terms of use, including without limitation prohibitions on the use of any device in a manner that may be construed by others as harassing or offensive.

DEBORAH SPECIALTY PHYSICIANS

BRING YOUR OWN DEVICE (BYOD)

- Authorized Personal Device users must comply with security restrictions that may become necessary in the future in order to optimally protect the Personal Device. Failure to abide by all such requirements will render user unable to continue to utilize their Personal Devices.
- If a Personal Device is lost or stolen, the employee will report the loss to DSP and to their carrier as quickly as possible, but in a window of time never to exceed 24 hours.
- DSP reserves the right to disconnect devices or disable services without notification if necessary
- DSP reserves the right to take appropriate disciplinary action up to and including termination of employment for noncompliance with the terms of this policy.

Third-Party Applications

- Use of third-party applications to send DSP information is subject to DSP policies and should be reviewed by the DSP Security Officer before utilization.
- Any ePHI sent or other confidential information sent or received via Personal Devices, must use a third-party communication app to ensure that all messages are HIPAA-compliant.
- ePHI should not be sent or received via unsecure, cloud-based hosting or file-sharing services such as Dropbox.
- Authorized work related pictures, video, voice files, and other data must be sent within secure applications and only if it is directly related to the provision of effective patient care. In no situation are you permitted to use the local storage on your Personal Device for work-related data. And in no case shall pictures, videos, etc. be posted to any social media sites.

Effective: 12/01/2020

DEBORAH SPECIALTY PHYSICIANS

BRING YOUR OWN DEVICE (BYOD)

I agree to fully abide by the terms articulated herein.

Employee: _____

SIGNATURE: _____ Date: _____

Executive Director-Administration: Victor Hatala

SIGNATURE: _____ Date: _____