BRING YOUR OWN DEVICE (BYOD)

PURPOSE: To establish guidelines for employees of Care Staffing Professionals use of personally owned electronic devices for work-related purposes.

SCOPE: This policy applies to all Care Staffing Professionals Divisions and employees.

PROCEDURE: Employees of Care Staffing Professionals may have the opportunity to use personal devices for work-related activities when authorized in writing, in advance, by management. Personal devices include personally owned cellphones, tablets, smartphones, laptops, computers, personal digital assistants, desktops, remote communication devices, or any other method currently available or developed in the future by which employees not in the same physical location may communicate or access company information.

Device protocols

To ensure the security of Care Staffing Professionals information and patient information entrusted to Care Staffing Professionals, employees who are authorized to use a personal device for work-related purposes must ensure the personal device has anti-virus software installed and activated. The anti-virus software must have the ability to store all company related information including, but not limited to, emails, calendar information, contacts, contract agreements, third-party accounts, forms, invoices, licenses, photo stock, tax documentation, and vendor management systems. The anti-virus software must be approved by Care Staffing Professionals management prior to use.

Employees shall only secure company information in areas of their personal device controlled by the anti-virus software. Employees shall not use cloud-based applications or other backup applications that allow company related information to be transferred or stored in areas not used or authorized by management. Employees should be aware that not all third-party cloud applications and storage locations offer adequate security and, therefore, no employee shall use applications or protocols that allow for company information to be transferred to other personal or home devices without written consent of management and inspection of the device by the IT department. Employees are also prohibited from using unsecure internet sites.

Initial Connections

IT will provide support to authorized employees needing assistance with connecting and accessing information in emails and cloud services.

Auto-Fetching – Android Users

Employees of Care Staffing Professionals should be aware of tactics used by attackers to automatically download malicious software used to exploit personal devices. Employees who are authorized to use a personal android device for work-related purposes shall disable auto-fetching of SMS video messages to prevent an attacker from getting their device to automatically download a malicious video containing 'Stagefright' exploits. 'Stagefright' allows an attacker to perform arbitrary operations on devices through remote code execution and privilege escalation. (Android Community)

Passcode Requirements

Employees requesting authorization to utilize their personal device for work related purposes shall have a complex passcode placed on their device. Acceptable forms of passcodes include fingerprint and an alphanumeric password. Alphanumeric passwords are required for initial startup of device. Alphanumeric passwords shall contain at minimum of 8 characters, one capital letter, one number, and one symbol. Other security features such as face recognition, 4 digit numeral PIN, and patterns do not meet the requirements of this policy.

Annual Recertification

Care Staffing Professionals employees authorized to use their personal devices for work-related purpose shall complete an annual recertification wherein they agree to the terms and conditions of this policy prior to continued access to company information via their personal device.

Emails

Employees shall not respond to or download attachments from unfamiliar emails unless there is sufficient cause to believe the email was solicited or reasonably related to work related activity.

In cases of email recovery, employee shall not send usernames and passwords in the same email correspondence. Employees should be cautious when sharing passcode information through the same communication median and consider sending layered security information in separate messages.

Application Passcode Reset

Employees of Care Staffing Professionals who store, process, or transmit company information via their authorized personal device are required to protect company information. Failure to comply with this policy could result in significant loss of company data, trade secrets, trust, fines by the federal government, and patient/client information. Therefore, Care Staffing Professional employees will be requested to change their company email password every 120 days. Employees will not be allowed to repeat the last 10 passcodes. Passwords shall contain at minimum one capital letter, one number, and one symbol.

Restrictions on Use

To facilitate compliance with the Health Insurance Portability and Accountability Act (HIPPA) Standards for Privacy of Individual Identifiable Health Information (Privacy Standards), 45 CFR

Parts 160 and 164, and any and all other Federal regulations and interpretive guidelines, employees whose devices allow for the use of a camera or recording devices are restricted from using such features in medical facilities and Care Staffing Professionals' offices unless authorized in advance by management.

The Health Insurance Portability and Accountability Act (HIPPA) offers that following definitions of terms to identify potential violations:

1. ***Audio Recording:*** recording an individual's voice using video recording (e.g., video cameras, cellular telephones), tape recorders, or other technologies capable of capturing audio.
2. ***Authorization:*** a written form executed by the patient or the patient's legal representative that meets the requirements in the Authorization for Uses and Disclosures of Protected Health Information policy.
3. ***Consent:*** the patient's or patient's legal representative's written acknowledgment and/or agreement of the use and/or disclosure of protected health information for treatment, payment, or health operations purposes or other reasons permitted by the HIPAA Privacy Rule.
4. ***Photography:*** recording an individual's likeness (e.g., image, picture) using photography (e.g., cameras, cellular telephones), video recording (e.g., video cameras, cellular telephones), digital imaging (e.g., digital cameras, web cameras), or other technologies capable of capturing an image (e.g., Skype).

The above definitions do not include medical imaging such as MRIs, CTs, laparoscopy equipment, etc. or images of specimens.

Employees are expected to exercise the same discretion as though it were a company device. No employee shall use their device for harassment, discrimination, or retaliation. No employee shall use a personal device for transmitting trade secrets or confidential information to unauthorized person(s) and shall restrict their use to work-related activities.

Employees who work in hazardous areas, emergency rooms, intensive care units, labor & delivery wards, and areas where constant monitoring of patients is required shall refrain from using personal devices while at their work station, as their required attention to the critical care of patients could be diminished or impair the quality of the patients' care. Each contracted facility may have similar policies in place regarding use of personal devices. Employees shall make themselves familiar with said policies and adhere to them.

Employees may not use their personal devices during periods of unpaid leave or when they are relieved of their duty/responsibilities. Care Staffing professionals reserves the right to deactivate or lock employees out of their company email and the companies cloud services during periods of paid or unpaid leave.

Employees are not allowed to store information from previous or outside employment on the company's network.

Family and friends should not use any personal device that has been authorized for work-related purposes. Employees are liable for all damages and leaks of information resulting from allowing use of the personal device.

Privacy / Company Access

Care Staffing Professionals retains the right to inspect, monitor, and preserve any communications that use the Care Staffing Professionals' network in any manner. No employee who uses the company's network, including cloud services, shall expect any privacy except that which is governed by law.

Care Staffing Professionals management also reserves the right to collect, retain, and publicize any personal and company related data on personal devices gathered as a result of use of the company's network and report it to government agencies or third parties during personnel investigations, criminal investigations, or civil litigation. Management may also review and analyze activity and patterns to ensure users of the network and cloud services are using these areas in accordance to company policies. No employee shall disable or change the settings of any software used to monitor activity of network users.

No employee shall access or browse non-work-related websites while on their personal device in conjunction with being connected to the company's network.

Company Allowance / Reimbursement

Employee who are authorized to use personal devices for work-related purpose shall receive a previously agreed upon monthly allowance for the installation and use of software, service protection plan, and applications required to ensure compliance with this policy. If an employee obtains or purchases a service protection plan, application, or software that exceeds the amount of the previously agreed upon monthly allowance, Care Staffing Professionals will not be liable for the cost difference.

Legal / Safety

Employees of Care Staffing Professionals are expected to adhere to all applicable municipal, state, and federal laws pertaining to the use of devices at all times.

Employees are hereby put on notice that some states preclude persons from using devices while driving a motor vehicle. Employees whose regular duties include occasional driving to and from contract facilities are encouraged to make themselves aware of all municipal, state, and federal laws pertaining to the use of devices while operating a motor vehicle.

Care Staffing Professionals prohibits the use of personal devices while driving, no matter the circumstances. Examples include, but are not limited to, stop or slowed traffic, reporting of incidents, response to communications marked with high importance, and telephone calls requiring immediate attention. Employees are required to pull over to the side of the road prior to accepting any call or communication. Employees of Care Staffing Professionals should give special care when driving through inclement weather, unfamiliar areas, or hazardous road conditions.

Employees who are charged with traffic violations resulting from the use of a personal device while operating a motor vehicle are solely responsible for all fines and penalties incurred because of their use.

As stated in previous sections, employees who work in hazardous areas, emergency rooms, intensive care units, labor & delivery wards, and areas where constant monitoring of patients is required shall refrain from using personal devices while at their work station, as their required

attention to the critical care of patients could be diminished or impair the quality of the patients' care. Each contracted facility may have similar policies in place regarding use of personal devices. Employees shall make themselves familiar with said policies and adhere to them.

Use of Cookies

Tracking information is automatically collected about all visitors to the Care Staffing Professionals website. This information consists of both individual and aggregated tracking information and is automatically gathered using "cookies". A cookie is a small data file containing information such as a user's login name that is written to the user's hard drive by a web server and used to track the pages visited.

We use cookies in several ways to track user behavior. Cookies store visitors' preferences and past activity on our site to provide better service to our visitors. We also use tracking information on an aggregate basis to track what services and areas our viewers are visiting most frequently to analyze: traffic patterns on our sites as well as provide anonymous reporting of usage for internal and external clients. In all cases, cookies used by Care Staffing Professionals are encoded and contain a unique digital signature to prevent tampering. They do not contain user passwords.

If you are accessing the website of Care Staffing Professionals, you can control your browser's settings regarding cookies by selecting "Internet Options" or "Preferences" in the menu bar of your browser. This will allow you to prevent your browser from accepting new cookies, notify you when you receive a new cookie, or disable cookies altogether. However, cookies allow you to easily navigate our website providing you with fastest most consistent results. We recommend that you leave them turned on. If you are accessing the website of Care Staffing Professionals through an alternative method such as a mobile application or third-party content distribution service, you understand that you may not have the ability to disable cookies depending on the specific access method.

Lost, Stolen, Hacked or Damaged Device

Employees of Care Staffing Professionals are expected to protect personal devices authorized for work-related purposes from loss, theft, damage, and cyber-attack.

In an effort to protect sensitive company data, employees who are authorized for use personal devices for work-related purpose are required to have applications installed on their devices that allow for "remote-wipe" of data from their phone in the event of loss. Employees should also be aware that having such an application may also effect personal data stored on the phone. Employees shall be responsible for recalling the title, username, and password of the "remote-wipe" application and provide such information to the IT department upon request.

Care Staffing Professionals will not be responsible for loss or damaged of personal applications or data such as photos and downloaded files resulting from the use of work-related material, company cloud services, company communication mediums, or the wiping of company related information. Employees are encouraged to seek out apps that allow restoration of their personal data to another device upon wiping it from the lost stolen, hacked, or damaged device.

Employees shall immediately notify management in the event their personal device is lost, stolen, hacked, or damaged. If IT is unable to repair the device, the device can be sent to a reputable third-party vendor and the employee is responsible for all cost associated with the repair of the personal device.

Replacement Devices

Care Staffing Professionals will not be responsible for providing loaner or replacement devices for employees while the phone or tablet is being serviced. Employees are encouraged to review their service protection plan for coverages and allowances.

Incident Tracking

Policy Violations

Any employee who has not received authorization from Care Staffing Professionals management and who do not have written consent shall not be permitted to use a personal device for work purposes. Failure to comply with Care Staffing Professionals policies and procedures may result in disciplinary action, up to and including termination of employment.

Employees who attempt to access company information and/or cloud services with a jailbroken Apple device or rooted Android device will be denied access to the network and excluded from future access.

Partial Invalidity

These terms, conditions and disclaimers of use shall be governed by and construed in accordance with the laws of the State of California, without regard to its conflict of law provisions. In the event any provision herein is determined to be invalid or unenforceable, such invalidity or unenforceability shall not in any way affect the validity or enforceability of the remaining provisions of this policy.

Termination of Employment

Upon resignation, termination, relief of duty, or suspension of an employee, the employee shall produce the personal device for inspection. Personal devices authorized for work-related purposes shall be subject to inspect upon request and all company data on personal devices will be removed upon termination of employment.

Internet Links

Data Breach Notification Laws by State (http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx)