HIC Mobile & Handheld Device Policy

Overview

The purpose of this policy is to provide guidelines for acceptable mobile devices, tools and phone usage, as well as establishing the end user expectations of service, quality and cost obligations. Users who are assigned a corporate mobile device or are approved for accessing HIC resources from a BYOD (Bring Your Own Device) mobile handset are required to agree and comply by signing the separate Policy supplement found attached to this document.

Scope

This policy applies to all employees who have been assigned a corporate cell phone, broadband device, or company issued VPN phones, or approved Bring Your Own Devices (BYOD) - As well as associated quality and service to/for each device.

Integrity

This policy has been designed to maintain the integrity of all of HIC's PHI Data as it pertains to our customers, 3rd party entities and minimum compliance standards set forth by our governing agencies and our Board of Directors and shareholders. HIC will maintain a zero tolerance enforcement of this policy. Please make close reference to the 'Special Conditions' clause of this policy below and if you have questions or concerns please address them to your management chain. Please note, however, that exceptions to this policy and its special conditions will not be entertained. We understand that this policy may seem heavy handed and we understand that you may be passionate about an alternative position. In these cases, we encourage you to submit an appropriate business and use case that outlines and clearly expresses the financial benefit in direct comparison of the associated risk value/cost to the HIC Organization. Any submittals will be forwarded to the Executive team for review and follow-up.

Corporate Cell Phones

1. All Corporate Cell phones should be limited to proper business use. The employee may be responsible for personal phone call overages and reimburse HIC.
2. Cell phones can be monitored and logged for all activities and information stored there-in is deemed property of HIC.
3. An employee is obligated to notify the IT department in advance of international travel so that proper and cost effective voice and data plans can be associated to that device and date range.
4. Text messaging should be limited to business use and personal overages maybe obligated to reimburse to HIC.
5. Data usage like applications, web surfing, etc; should be carefully used and may be subject to service provider data caps.
6. Supported WiFi or VoIP calls are subject E911 rules and service. In case of an emergency, user should be aware of limited location services and other factors on locating associated to Wifi/VoIP calls
7. The employee is expected to take reasonable and all precautions including use of any assigned cases or training to prevent any kind of damage to cellular devices. An employee may be subject to reimbursing HIC for any damage or replacement if it is determined to be caused by employee negligence.
8. Employees should exercise best practice and follow local laws regarding phone texting or call usage while driving or operating any motorized or non-motorized vehicles.
9. Corporate Cell Phones will be subject to software installation and update restrictions based on corporate software and data policies.
10. A password pin of at least 8 characters is required for access to corporate data sources including but not limited to emails and corporate files.

11. Corporate cell phones will be required to have an automatic lock enabled with password protection. Interval will be applied based on management policy applied – currently 90 seconds idle time.

BYOD Bring Your Own Device

1. HIC currently supports BYOD for approved employees using most Android and iOS devices. HIC will only support devices left in their OEM, Factory, or Carrier-Specific Firmware. Rooted, Jail-broken or 3rd party ROMS/Firmware cannot be enrolled in this program.
2. Pending qualification, BYOD users will be reimbursed $30 towards their monthly cellular bill to cover business related voice and data applicable charges.
3. HIC is not responsible for any additional expenses incurred from the use of the mobile device including service plans, additional accessories or equipment, special fees and taxes.
4. HIC will install a mobile device management (MDM) agent on all phones enrolled in the BYOD program. In the event of a security breach or separation from HIC, BYOD's will be wiped of all corporate data.
5. A passcode of no less than 8 digits/characters must be maintained at all times. After 10 failed password attempts the device may be wiped of all data. For all intents and purposes, the HIC Password Policy applies where feasible and appropriate.

VOIP - VPN phones and mobility applications

1. VOIP/VPN phones and their quality of service is limited to an employee's home ISP and home network. Please be aware that other home devices and your provider service congestion may cause call latency and/or call drops. HIC may be limited in support or troubleshooting of home ISP and network issues and any issues deemed "local" to the distributed environment are the responsibility of the employee to resolve. The IT department will attempt to give best guidance in these situations.
2. VOIP/VPN phones require physical CAT5/CAT6 cable to home network for connectivity and possible power. Employee is responsible for all hard wiring and power for these phones.
3. VOIP/VPN phones are subject and limited to their respective technology for E911 calls. Employees need to be mindful that emergency response for VPN phones for E911 will be dispatched to HIC offices in San Diego and not the employees' home location.
4. VOIP/VPN mobility application and software work over 3G or 4G cellular but may have best service quality over Wifi.
5. E911 limitations apply to VOIP/VPN mobility and in case of emergency may be dispatched to HIC offices in San Diego.

Bluetooth

Bluetooth accessories will be assigned with corporate devices when necessary. This may include keyboards, data cards, mice, etc.. All cellular phones will come equipped with hardwire headsets or headphones, Bluetooth headsets will not be provided.

Special Conditions: HIPPA Compliance, PHI and Other Sensitive HIC Data stored on Mobile Devices

Because of the nature of our business and its implications on the above compliance measures, effective immediately, email and HIC non-encrypted work related documents and assets will not be allowed on any handheld cellular devices, whether BYOD or Corporate issued. Because of the potential for unmitigated risk related to data leakage of patient health information poses high potential for financial damages, brand tarnishment and significant general business continuity threat to HIC's ongoing business interest, HIC will maintain a zero tolerance policy on these data types as they pertain to customer and patient information stored on an external hand-held device.

From time-to-time and without prior notice, IT and HIC's Security Audit and Enforcement teams may conduct random device audits to police this particular component of the Cellular & Mobile Policy for HIC. If a device (BYOD or Company Issued) is found to have unencrypted files with PII, PHI or other sensitive data onboard, HIC will undertake disciplinary action up to and including on the spot termination of employment.

The organization also understands that this restriction may impact productivity and limit one's ability to take full advantage of the benefits of a mobile smart device. That said, we have deemed the risk of data leakage and potential damages of such an occurrence to outweigh individual personal liberties as they pertain to conducting business on behalf of HIC via a mobile device. HIC provides secure access to information in a variety of forms that complies with the standards set forth by HIPPA and other compliance measures. We expect our employees, vendors and contractors to comply with these policies as set forth here-in. We place a higher value on security and data protection (Patient and Customer) than on personal convenience as it pertains to the execution of HIC day-to-day business.

HIC Cellular/Mobile Policy Supplement

As an HIC employee, I acknowledge and agree:

1. HIC will provide a protective case for the mobile device to help prevent any damages to the device. If I choose to use a different case or do not use the company approved case, I will be solely liable for the repairs of any physical damages to the device.

2. When using my HIC mobile device I shall observe all applicable national, local and state laws including but not limited to all such laws restricting the use of mobile devices while operating a motor vehicle. I will not interact with my mobile device while in my vehicle unless it is stationary and legally parked. I further understand that, if I am involved in a motor vehicle incident resulting from the unlawful, illegal, unsafe, unauthorized or negligent use of my mobile device while driving, I will be solely responsible for all liabilities that result from such action.

3. A passcode of no less than 8 digits must be maintained at all times. Your lock-screen will be auto set to lock after 90 seconds of device idle time. After 10 failed password attempts to log into the device the device will be wiped of all data. Passwords must be kept private and not shared with anyone. It is imperative that passwords not be written down for security reasons.

4. I understand that only HIC approved applications can be installed on this device. Attempting to Install any non-approved applications will be considered a violation of HIC policy and will lead to immediate termination of service and possible employee write-up or other disciplinary action.

5. HIC reserves the right to add or remove features at any time that may change the user experience.

6. HIC reserves the right, at any time and without notice, to suspend or deny access to corporate resources.

7. This Mobile Device Policy supplements the current IT Security manual.

8. Special Conditions Clause Acknowledgement: I understand and acknowledge that I have been briefed and am fully aware of the special conditions clause outlined above in this document and agree to abide by the terms laid out there-in.

I_____, have read and accept the terms and conditions of the HIC Mobile Device Policy listed above.

Employee Signature: _____

Date: _____