Mobile Device and External Network Services Use Policy

Policy Number: A20121114036

Effective Date: 11/14/2012

Sponsoring Department: IT/HR

Impacted Department(s): PBD, Nova

Type of Policy: ☒ Internal ☐ External

Data Classification: ☐Confidential ☒Restricted ☐Public

Applies to (Line of Business):

☒ Corporate (All)
☐ State Products, if yes which plan(s): ☐MediSource;☐MediSource Connect; ☐Child Health Plus; ☐Essential Plan
☐ Medicare, if yes, which plan(s): ☐MAPD; ☐PDP; ☐CSNP; ☐ISNP
☐ Commercial, if yes, which type: ☐Large Group; ☐Small Group; ☐Individual

Excluded Products within the Selected Lines of Business (LOB)

None

Applicable to Vendors? Yes ☐ No☒

Purpose and Applicability:

The purpose of this policy is to define:

1. Eligibility and requirements for the issuance of company-paid and personal devices (BYOD);
2. External, off-network access to Independent Health's Office 365 services ("External Network Services"); and,
3. Associate and selected contractors responsibities and obligations for using these services.

These services are elgibile to associates and selected contractors at Independent Health.

Policy:

Company-Paid Devices and Cellular Plans

Independent Health shall provide a company-paid cellular plan and device to associates and selected contractors only upon demonstrated need and written approval by the Vice President in the relevant business area. IHA subsidiaries also included in this policy are: PBD and Foundation.

Associates who are approved to have a company-paid device will be provided with the following options for a device:

Provided with a company-issued device and service

OR

Transfer current personal mobile number to a company-issued iPhone

The company issued device will have access to Independent Health's approved External Network Services.

Associates who are not eligible to have a company-paid device will have the option to access Independent Health's approved External Network Services on their personal device ("BYOD"), subject to manager approval as described further in this policy.

Eligibility:

Before issuance of any company-paid device as described above, Human Resources will approve all such requests on the following basis:

- The associate or contractor has a demonstrated business need and has written approval by the Vice President in his/her business area.
- The level of associate and whether classified as exempt or non-exempt. Human Resources will review the business necessity for any non-exempt associate and ensure all associates who are issued a device are instructed to follow the Hours of Work Policy when utilizing the device outside of their regular work schedule.
- A SOM request must be submitted by the manager and approved by the VP of the department and an HR business partner
- Mobile device management (MDM) software will be installed on all issued mobile devices and must remain on the device for the duration the cellular plan is charged to Independent Health.

Porting of Device:

Associates who are eligible for a company issued device have the option of porting over their personal phone number to an Independent Health issued mobile device. When selecting this option, the associate must surrender their personal mobile device to IH and will be provided with a device upon converting. If/when the associate leaves IH, the associate will be allowed to keep the IH issued mobile device and mobile number at no cost after removal of Independent Health's data and/or applications.

Roaming:

If an employee is traveling outside of the country, the associate must contact the ServiceDesk to allow IHA to make a temporary change to their contract to include roaming. This will insure that we are not incurring additional costs to our enterprise mobile agreement. Associates may be subject to disciplinary action for failure to comply with this policy.

Personal Device Use of External Network Services ("BYOD"):

Under the BYOD program, associates may request their manager provide approval to access External Network Services from their personal device. This can be accomplished by having the associate submit a SOM request with approval required by the associate's manager.

Associates will be limited to two mobile devices with access to the External Network Services.

Talk, text, and non-External Network Services data usage will not be monitored by Independent Health, and will only be limited based on the associate's cell service and data/Internet service provider (ISP) plans.

Access to Independent Health wireless networks is not allowed for personal or BYOD devices. The storage, recording, or entering of Independent Health member data (PHI/PII), confidential business information (CBI), or other sensitive content to Independent Health unmanaged applications or to the device directly is strictly prohibited. Independent Health reserves the right to suspend access to company resources without notice. Associates are personally liable for all costs associated with their BYOD devices, and for all risks including, but not limited to, the complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable. By utilizing the IH BYOD program, the associate agrees to fully comply with Independent Health Human Resources, Information Security, and IT requirements and to fully cooperate in any investigation (including but not limited to regulatory, audit, and forensics investigation). related to their access of External Network Services from their personal device and which may include providing access to their personal device for these purposes.

Independent Health External Network Services:

Independent Health External Network Services will be restricted to specific applications on the mobile device or device being used to access the External Network Services. Independent Health reserves the right to add, modify, change or disable the use of all or a portion of the External Network Services allowed for use without prior notice.

External Network Service applications allowed for use will be password protected and cloud sync will be disabled. Associates are encouraged not to store personal data in company Network Service applications.

Associate Obligations and Responsibility

- Associates and contractors agree to abide by this policy in whole before they are provided any mobile device or wireless internet device and before they are granted access to any Independent Health External Network Services.
- Associates and contractors have no expectation of privacy when utilizing Independent Health devices or External Network Services. Independent Health monitors devices for compliance with this policy and configuration requirements, and sign-ons to External Network Services will have additional data such as location logged.
- Associates and contractors must abide by all additional requirements for using Independent Health data and information assets as articulated in the Acceptable Use Policy, the Code of Conduct, Associate Handbook and any other relevant or applicable Independent Health policies as may be amended from time to time.
- Any/all Information (example: pictures of whiteboards, email, written or spoken notes) created on a device which pertains to Independent Health business or the business of its affiliates or subsidiaries is considered property of Independent Health and falls within the scope of this policy.
- Independent Health will provide support for all mobile and/or wireless device issues related to our External Network Services and/or the MDM software for company-paid devices. Company-paid devices in need of repair must enter a service desk ticket. The Service Desk will be responsible for following up with the associate and resolving the issue. Independent Health will not provide support for personal owned, BYOD devices.
- Associates and contractors are provided a case for their company-paid mobile device by Independent Health and required to keep it on the device.
- Associates and contractors are required to maintain reasonable physical and logical protection over devices used to access the External Network Services.
- Independent Health is specifically authorized to load MDM software on company-paid devices and require security features be enabled on all devices to ensure they comply with Independent Health's information security policy. Independent Health reserves the right to add, modify, change or disable certain device features required to support Independent Health's information security policies without prior notice. Associates are prohibited from attempting to circumvent the control features

that the MDM software and information security policies will enable (e.g., strong passwords, encryption, and others). Associates and contractors are prohibited from tampering with, uninstallingor otherwise attempting to circumvent the Independent Health MDM technology and policies at any time. Further, associates are prohibited from accessing External Network Services from a "rooted" or "jailbroken" phone.

- Independent Health reserves the right to take possession of any device at any time should it determine, in its sole discretion, that it is needed to maintain and support the legal status of Independent Health or any of its affiliates or subsidiaries. Such legal status includes but is not limited to the protection of Personal Health Information or Confidential Business Information. In order to take possession, approval from Independent Health Counsel, an HR Business Partner, or Chief Information Security Officer must be obtained in writing and be presented to Independent Health Counsel.
- Company-paid mobile devices, when their useful lifespan has reached its end (either due to contract completion, reaching device renewal thresholds, or general deficiencies in the usefulness of the device to meet its intended purpose) or due to damage or no longer meeting the intended purpose must be returned to the IH Service Desk for accounting purposes. If needed, new devices will be provided. Such devices, if not refurbished, shall be wiped and returned to the vendor for credit.
- Associates must maintain the latest operating system version on their device to maintain access to External Network Services. If a device is unable to run a sufficiently up to date version of an operating system, it may not be allowed to access the External Network Services.
- Independent Health will remove all corporate data from the device when an associate's employment ends, the device is lost, or IT detects a data or policy breach, virus, or similar threat to the security of the company's data and technology infrastructure.

Device Loss, Theft, and Damage:

Associates and contractors must report any lost or stolen device which may have access to Independent Health data or External Network Services immediately and within a maximum of one (1) business day of discovery. Lost and stolen devices are to be reported to the IT Service Desk and Information Risk Office. Independent Health will assess the loss or damage to the device on a case by case basis.

In the event the device is unrecoverable, Independent Health will remove all company data from the device. While Independent Health does not expect needing to use wiping features regularly, it is acknowledged that other data may be wiped as an unintended effect of the partial wipe process. Should the associate or contractor desire a full wipe of a lost or stolen device to protect their personal information, the IH Service Desk will accommodate the request.

Any remaining devices which experience physical or other types of damage should be reported to the IH Service Desk immediately so they may be serviced. All attempts will be made to recover data from the devices; however, IH may be unable to restore personal data as a result. Associates should ensure any personal data on a phone has been backed up for recovery purposes.

Hours Worked:

Associates utilizing a device to perform work (including: checking and responding to work related phone calls, emails, texts, and voice mails) during their work day or outside of their regular work schedule, should record such time worked in accordance with the Hours Worked Policy.

Separation of Employment:

For company-paid devices, Human Resources will work with IT as part of its Separation Process to ensure the associate returns the device to IT prior to their last day of employment or service, or when their business need for the device(s) expires, whichever occurs first. An associate, who previously transferred his/her personal mobile number to the company-paid device, will work directly with IT to reclaim his/her personal mobile number and the device.

Upon the date of separation, IH will "wipe" (remove) the MDM software, company applications and company data from the associate or contractor's device. While this wipe is limited to the company data managed by the MDM software, the user acknowledges that other data may be lost as an unintended effect of the partial wipe. The IH Service Desk will be available, prior to the date of separation, to facilitate the removal of Independent Health data to help ensure the protection of personal data if requested by the separating party.

Should an associate or contractor not return or present a device for wiping as stated in this section, or due to the sensitivity of a termination (to be determined in the sole discretion of Independent Health), Independent Health reserves the right to remotely remove the MDM software, Independent Health data, company applications and any other company data from the device(s) upon separation.

Separated associates and contractors are not authorized to use or restore any application or data that originated through the relationship with Independent Health.

Associates who no Longer Require Independent Health Issued Mobile Services:

When it has been determined that the Associate's position no longer requires mobile service, Independent Health has the authority to cancel the contract with the service provider.

- If the associate was provided an Independent Health mobile device and service, they must relinquish the device.
- If the associate previously ported their personal phone number to an Independent Health business mobile account, they will be allowed to keep the IH issued device and mobile number at no cost.

Enforcement & Agreement:

All associates and contractors issued a company-paid device or access External Network Services under this policy will be required to read and sign the IH Mobile Device and External Network Services Attestation within the SOM request and approval process. Failure to adhere to any of the terms of the policy and attestation may result in disciplinary action up to and including termination.

Definitions

IH Data

Any information system, asset, or file where confidential or restricted information is collected, stored, processed, transmitted, or destroyed.

Eligible Persons
All Director level and above, IT on-call associates and outside sales team members.

Jail Break/Root
An attempt to circumvent a mobile device's operating system.

Media Tablet
A media tablet is an open-face wireless device with a touchscreen display and optional physical keyboards. The primary use is the consumption of media; it also has messaging, scheduling, email, and Internet capabilities. Diagonal screen dimensions are typically between 5 inches and 10 inches.

Mobile Applications
Mobile applications are software programs running on a mobile device that provide a specific function or functionality.

Mobile Device
A mobile device is any mobile phone, smartphone or media tablet. Unless otherwise stated, mobile devices refer to any mobile phone, smart phone, or media tablet that is either personally owned by an associate or provided to an associate by IH (IH owned and paid for).

Mobile Device Management (MDM) Software
Mobile device management software is any software used to manage the security, privacy, and general use of information and applications residing on or accessed through mobile devices.

Smartphone
A smartphone is a mobile device with general computing capabilities and the ability to run productivity and lifestyle applications while also allowing users to interact with others via voice, messaging, scheduling, email and the Internet.

Wireless Internet Device
A device that provides internet connectivity to a portable device (e.g., an over-the-air mobile connectivity computer card provided by Verizon)

RESPONSIBLE DEPARTMENTS:

All Departments

APPLICABLE VENDOR(S):

N/A

References

Related Policies, Processes and Other Documents

Code of Conduct
IH Record Retention Policy
Associate Handbook
Hours Worked Policy
Acceptable Use Policy

Regulatory References

List all regulatory references used within this policy.

Version Control

Sponsored By:
Name sponsor: Bill St George
Title of sponsor: Director – IT Service Delivery
Signature of sponsor:

Revision Date	Owner	Notes
10/23/2015	Michael Hastings	Updated policy
10/16/2017	Michael Hastings	IT -Nick Mislin no change, HR Jen Barr and Sandy Calandra add Evolve
10/9/2018	Michael Hastings	Nick Mislin reviewed no updates needed.
11/8/2019	Michael Hastings	Allison Letson, Nick Mislin, Sandy Calandra and Jen Barr added updates due to BYOD

11/9/2020	Bill St George	Remove Evolve, Change sponsor to Bill, removed reference to the 'expense' on page 2 and 'all costs' on page 5, changed help desk to Service Desk in 7 places