From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

Important: Personal Owned Device Policy Change

On April 7, 2018, cloud applications will no longer be available on personal mobile devices. Personal devices include mobile phones and its accessories (e.g. wearables, watches), tablets with or without cellular connection, other devices not designated as company owned. Work will ONLY be allowed on company owned devices.

Questions & Answers

Why is the policy changing?

The current risks to mobile devices are:

- Lost/Stolen Mobile Device
- Using an unsecured Wi-Fi network
- Inadvertently downloading viruses or other malware
- Exposure to new vulnerabilities in mobile devices (e.g. Bluetooth) (Armis, 2017)
- Unintentional disclosure to unauthorized individuals when sharing devices with family, friends, and/or coworkers

What could happen if PHI was sent or stored unauthorized from my mobile device?

These situations listed above risk the potential of mail containing PHI copied to other locations resulting in large fines and penalties. The fines can range of $100 to $50,000 for the HIPAA violation (even when knowing and using protective measures) (Hold, 2017). For example, the Fresenius Medical Care North America (FMCNA) has agreed to pay $3.5 million to the U.S. Department of health and human services (HHS) Office for Civil Rights (OCR) to settle for HIPAA violations (HHS.gov, 2018).

Will this new policy affect my ability to work from home?

No, login from *corporate owned* laptops and phones are still allowed from home. The policy only affects personal mobile devices (e.g. mobile phone, tablet, etc.). The reason to switch back to corporate owned devices are the following:

1) **More secure-** Option to wipe devices and revoke access to applications to be HIPAA compliant
2) **Ownership-** Protecting information by owning the device, phone number, & contacts
3) **Increased Performance-** Specific devices tuned to business needs with corresponding data plans (Knuckles, 2013)

Why did personal mobile phones become allowed in the first place?

The BYOD (bring your own device) policy was designed to two primary objectives for HIC: One, to enable employees to increase work performance with devices they are familiar with; Two, to cut HIC costs and expenses of maintaining cell phones and IoT devices. As employees of HIC are tasked to comply with HIPAA regulations and secure electronic patient health records (ePHI), this proved to be increasingly difficult with the introduction of the BYOD policy that includes many different devices, configurations, and vulnerabilities.

Important Statistics to Know

The following statistics may help employees understand the new policy:

- 49% of organizations using SharePoint had a data breach in the past two years (Metalogix, 2017).
- Top two security threats According to “The State of Cybersecurity in Healthcare Organizations”:
    - Employee-owned mobile devices being used to access ePHI (76%)
    - Mobile devise accessing ePHI without proper security installed (72%) (ESET, 2016)

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

New Guidelines

Three tiers of connection to Office 365 (Outlook, SharePoint) and Citrix ShareFile when working at home:

Tier	Ownership	Ownership	Mobile Access to Outlook	Tablet Access to Outlook
I	HIC	HIC owned devices for qualified HIC employees as described in policy	**Yes**	**Yes**
II	Employee	Employee owned devices managed and supported by HIC	**No**	***For Low-to-Mod HIPAA Risk Depts.**
III	Employee	Employee owned devices NOT managed or supported by HIC	**Never**	**Never**
Tier system from (Phelps, 2013)				

* Low-Moderate HIPAA Risk Departments include Marketing, Financial, Underwriting, Legal, and HR.
For more info regarding departments with HIPAA risk, see supplemental III, "Mapping PHI Risk by Department".

Alternatives

As stated, company owned devices are allowed. If you believe the new access policy poses a detriment to your work quality, please contact your supervisor to submit a form to obtain a HIC issued mobile phone, table, or laptop.

Program Enforcement

As of April 7, 2018, devices marked in tier II (employee owned devices managed or supported by HIC), will no longer have access to Office 365 and Citrix ShareFile. The mobile device profile will be removed from both Azure and Citrix XenMobile databases from these applications on the evening of April 6, 2018. Individuals who circumvent these rules by downloading PHI data to devices listed below will be disciplined according to the HIC Security Policy. The following is forbidden:

- Storing PHI on personally owned storage media for take home: USB, CD, external drives
- Sending PHI from Personal email accounts
- Mobile phone/tablet recording: taking pictures and/or texting PHI information

How you can get caught:

- Alerts from outbound emails containing PHI (e.g. Data Leakage Prevention (DLP) platform)
- Audits by external auditors, internal audit team, or IT security team
- Discovery by coworkers and managers
- Alerts of unauthorized devices connecting to the system
- Security camera office monitoring

Rewards

Individuals and groups who follow the HIC Security Policy throughout the year will be entitled to one of the following:

- Gift card (e.g. movie, restaurant, iTunes, entertainment)
- Paid-time off
- Cash reward up to $1,000*

*Cash reward may be provided to those individuals reporting breach in policy.

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

Supplemental I: What does PHI Include?

Protected health information is defined in 45 CFR 160.103, where 'CFR' means 'Code of Federal Regulations', and, as defined, is referenced in Section 13400 of Subtitle D ('Privacy') of the HITECH Act.

(2) (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
(A) Names;
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; an

(HIPAA, 2017)

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

Supplemental II: Affected Software/Platforms and Technical Implementation of New Policy

Affected Software/Platforms		
Software/Platform	**Description**	**Link**
MS Office 365	*Create, edit, and share from your PC/Mac or your iOS, Android™, or Windows device with anyone in real time*	https://products.office.com/en-us/business/explore-office-365-for-business
MS SharePoint	*SharePoint Server 2016 provides a broad array of features and capabilities to help ensure that sensitive information remains safe and the right people have access to the right information, at the right time.*	https://products.office.com/en-us/sharepoint/sharepoint-server
MS Office Mobile	*View, edit, and create documents with the familiar Office interface optimized for mobile phones and tablets*	https://products.office.com/en-us/mobile/office
Citrix ShareFile	*File sync and sharing built for mobile business*	https://www.citrix.com/products/sharefile/

Policy Enforcement Software/Platforms		
Software/Platform	**Description**	**Link**
MS Azure (for active directory)	When a user requests access to an Office 365 service from a supported device platform, Azure AD authenticates the user and the device. Azure AD grants access to the service only if the user conforms to the policy set for the service.	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-device-policies
	Removing Mobile Devices from Azure	https://docs.microsoft.com/en-us/azure/active-directory/device-management-azure-portal
Citrix XenMobile	Enterprise mobility management solution	https://www.citrix.com/products/xenmobile/
	Managing Devices	https://docs.citrix.com/en-us/xenmobile/8-6/xm-dm-manage-logon-webconsole-tsk/xmob-dm-manage-devices-addmanually-tsk.html

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

MS Azure Conditional Access		
Policy Item	**Description**	**MS Technical Link**
Users/Groups	*What users do you want to control – Users can be included/excluded from the policy if required. You will always get the person who is too important for this policy and wants to access everything from their personal iPad. It also allows you to test policies before rolling out to the wider business avoiding locking everyone out!*	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-manage-groups
Cloud Apps	*What apps do you want to control? Conditional Access does not need to apply to all of Office 365, you can be more granular and just control access to specific apps – E.g. Exchange Online.*	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-mam
Client App	*Control what app/software the user is connecting from to the data – E.g. allow browsers but disable mobile and desktop Outlook apps.*	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-mam
Device Platform	*Control what devices users can connect from – E.g. allow Windows and iOS but block Android phones*	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-policy-connected-applications
Location	*Control what IPs can connect to Office 365 – E.g. could limit this to the office external IP.*	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-named-locations
Sign-In Risk	*Control signs in if Office 365/Azure thinks the sign in is not coming from the genuine user – E.g. if someone signs in from London then New York 30 mins later.*	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection-playbook
(Hynes, n.d.)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

Supplemental III: Mapping PHI Risk by Department

Dept.	Dept. Description	PHI/EPHI Leakage Risk
Office Claims	Responsible for establishing Company claim policies as well as overseeing large property and casualty claims.	**HIGH**
Workers' Comp Claims	Handles Workers' Compensation, long-term "no fault," and medical claims. The Department also handles medical cost containment and pre-certification of medical treatment.	
Commercial Lines Underwriting	Responsible for establishing, implementing, and monitoring the company Commercial underwriting program.	**LOW**
Underwriting Operations	Responsible for Commercial and Personal Lines rate, rule, and form filings and regulatory changes, compliance with department of insurance regulations, market conduct exam coordination, and forms management.	
Home Office Loss Control	Sets direction and policy for the Loss Control Consultants who are located in each regional office. Helps reduce and control exposures and hazards that can lead to a loss by working with our policyholders on their risk control programs.	
Personal Lines Underwriting	sets the Personal Lines pricing and risk selection standards for the company. They develop products, maintain the automated underwriting systems and workflows, develop and manage the interface with vendor and agency systems, and administer the Vibrant Personal Lines Practice and Blue Streak programs, special high-performance agency programs.	**MODERATE**
Customer Services	Range of insurance related services with customers.	**HIGH**
Accounts Receivable	handles cash processing for direct billed premium payments, accounting tasks related to agency billed business, collection of earned premium on cancelled policies and outstanding audit balances, as well as the entry of loss notices for claims handlers	
Personal Lines Services	processes Personal Lines policy transactions, inputs underwriting information used to evaluate exposures and make decisions, inputs loss notices for claims handlers and resolves phone calls from policyholders and agents.	
Commercial Lines Services	processes Commercial Lines policy transactions, inputs underwriting information used to evaluate exposures and make decisions, inputs loss notices for claims handlers and resolves phone calls from policyholders and agents.	
Premium Audit	orders, evaluates, and processes all premium audits for the company, inputs loss notices for claims handlers, and services phone calls from policyholders and agents.	
Office Services	distributes all incoming and outgoing documents. They are responsible for our Home Office telephone services and our in-house printing services.	
Finance	Various finance related tasks to maintain revenues	**LOW**
Actuarial	Has the role of analyzing data and working with other company personnel to set the prices Central charges for our insurance products.	
Analytic	provides exceptional insights into our customer segmentation, retention and pricing in an effort to provide higher quality, better priced products to meet the needs of our policy holders.	
Corporate Accounting	oversees the preparation of internal and external operating and financial reports for state insurance departments, rating bureaus, and company management.	
Risk Management and Innovation	is responsible for the negotiation and administration of reinsurance contracts; monitoring and controlling exposure to catastrophes; authoring and coordinating the submission of Central's Own Risk and Solvency Assessment (ORSA); directing the efforts of Enterprise Risk Management (ERM); oversight and management of the corporate fleet	
Human Resources	responsible for all human resource activities for the company. This includes employment-related activities such as recruiting, hiring, training, compensation, job classification and assignment, promotion, transfers, and employee relations.	**LOW**
Learning & Development	reports to Central's Employment Manager. They develop, implement, maintain, and monitor effective training and education programs to assist employees and agents in meeting or exceeding their responsibilities and encourage future development.	
Facilities	responsible for the maintenance of buildings and grounds, as well as the purchasing and servicing of office equipment and supplies	
Information Technology	designs, develops, and maintains a wide variety of multi-functional computer systems supporting company and agency operations as well as insured customers that include Internet, personal computer, mobile, and mainframe platforms.	**HIGH**
Legal	responsible for the management of all corporate legal and regulatory issues and the provision of legal counsel that assists in developing and advancing the company's strategic business objectives.	**LOW**
Internal Audit	provides independent, objective assurance and consulting services to the company. This includes examining and evaluating the company's governance, risk management, and internal control processes. Internal Audit has a dual reporting relationship to the General Counsel and the Audit Committee of the Board of Directors.	**MODERATE**
Marketing	responsible for communicating Central's products and programs to our agents and policyholders. Marketing is also responsible for the creation of promotional materials and Internet publishing, including social media and videos.	**LOW**

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

References

Ablett, J. (2017, March 28). *Is Office 365 HIPAA compliant?* Adeliarisk.com. Retrieved from https://adeliarisk.com/office-365-hipaa-compliant/

Armis. (2017). *The Attack Vector "BlueBorne" Exposes Almost Every Connected Device.* Armis.com. Retrieved from https://www.armis.com/blueborne/

Bitglass.com. (2014). Bitglass Whitepaper: *HIPAA Compliance, PHI and BYOD.* Retrieved from http://cdn2.hubspot.net/hub/313952/file-847410035-pdf/Collateral/HIPAA_PHI_BYOD.pdf?submissionGuid=235409c4-52ea-41d7-9763-1bb7e1943a31

Central-Insurance. (n.d.). *Company Structure.* Retrieved March 31, 2018 from http://www.central-insurance.com/docs/careers-structure.htm#clund

ESET. (2016). *THE STATE OF CYBERSECURITY IN HEALTHCARE ORGANIZATIONS IN 2016.* Retrieved from https://cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf

HealthIT. (n.d.). *Managing Mobile Devices in Your Health Care Organization.* Healthit.gov. Retrieved March 28, 2018 from https://www.healthit.gov/sites/default/files/fact-sheet-managing-mobile-devices-in-your-health-care-organization.pdf

HIMSS Analytics. (2017). *2017 Essentials Brief: Mobile.* Retrieved from http://www.himssanalytics.org/sites/himssanalytics/files/2017_Essentials%20Brief_Mobile_SNAPSHOT%20REPORT.pdf

HIPAA. (2017). *HIPAA 'Protected Health Information': What Does PHI Include?* Hipaa.com https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

Hold, D. (2017, July 6). *Protecting ePHI in a BYOD Healthcare Environment* [Blog post]. Enterprise.efax.com. https://enterprise.efax.com/blog/protecting-ephi-in-a-byod-healthcare-environment

Hynes, S. (n.d.). *How to restrict access to Office 365 through Microsoft's Conditional* Access [Blog Post]. Core.co.uk. Retrieved from https://core.co.uk/blog/restricting-access-office-365/

Kleyman, B. (2018, January 29). *4 Key Ways to Overcome Healthcare BYOD Security Challenges*. Retrieved from https://healthitsecurity.com/news/4-key-ways-to-overcome-healthcare-byod-security-challenges

Knuckles, B. (2013, December 9). *Should You Buy Your Employees iPhones? BYOD Pros and Cons.* Retrieved from https://www.businessnewsdaily.com/5586-iphone-byod-pros-cons-small-business.html

Metalogix. (2017, May 4). *One in Two Organizations Have Had a SharePoint Data Breach, According to New Study.* Retrieved from https://www.prnewswire.com/news-releases/one-in-two-organizations-have-had-a-sharepoint-data-breach-according-to-new-study-300451690.html

Microsoft. (n.d.). *Capabilities of built-in Mobile Device Management for Office 365.* Support.office.com. Retrieved March 27, 2018 from https://support.office.com/en-us/article/capabilities-of-built-in-mobile-device-management-for-office-365-a1da44e5-7475-4992-be91-9ccec25905b0#bkmk_accesscontrol

O'Dowd, E. (2017, February 15). *How to Secure an Evolving HIT BYOD Mobile Infrastructure*. Retrieved from https://hitinfrastructure.com/news/how-to-secure-an-evolving-hit-byod-mobile-infrastructure

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 2, 2018
Subject: Health Insurance Company (HIC) Corporate Mobile Policy

Phelps, T. (2013, August 6). *13 Best Practices for Developing Your Mobile Device Policy.* Retrieved from www.netstandard.com/13-best-practices-for-developing-your-mobile-device-policy/

Logo from:

MarksMan Healthcare Communications. (n.d.). *HEOR – INDIA CONCLAVE (HIC).* Bna.com. Retrieved March 14, 2018 from https://marksmanhealthcare.com/heor-india-conclave/