December 2017

HIPAA One
PROTECT YOUR ePHI

HIPAA Compliance with Microsoft Windows 10 Enterprise

Steven Marco
HIPAA One
President
CISA

Arch Beard
CISO

Markus Muller
Sr. Network Engineer
CCNP, VCP

About the Author

Steven Marco, President and Founder of HIPAA One, has a passion for Data Security and over 20 years as a leader in executing various regulatory compliance mandates in healthcare IT. A Certified Information Systems Auditor since 1999, he helped pioneer Internet Security Services and manage risk for numerous Fortune 500 companies while at Deloitte. At Resources Global Professionals, he successfully led their Sarbanes Oxley 404 audit and completed an IPO in 2002. Additionally, Steven pioneered a Health IT professional services line leading hundreds of compliance and security projects. Prior to founding HIPAA One, Steven was Product Director at DirectPointe, where he integrated HIPAA and PCI security protocols for their Healthcare and MAS clients. Steve holds a Bachelor's Degree from Ryerson University in Computer Information Systems Management and Corporate Law.

Contents

Part 1 – Updates to Regulations and IT Security Compliance Implications
- HIPAA overview – Review of 18 HIPAA Identifiers

Part 2 - Microsoft's Windows 10 Enterprise: Data Security and HIPAA Compliance
- Updates to Windows 10 for Modern Devices

Part 3 – Windows 10 and HIPAA Traceability Section
- Group Policy Templates to support HIPAA compliance

Appendix A – Active Directory and Registry Settings for Data Security and Cloud Communications with Packet Captures

Appendix B – Response to Microsoft Fall Creators Update for Windows 10

Executive Summary

In today's computing environment, record-breaking data breaches (918 identified breach incidents involving 1.9 billion records in the first half of 2017 alone[1]) including healthcare identity theft are occurring every day. With the Total Average Cost (TAC) of a data breach in the U.S. currently sitting at $7.35 million, and each sensitive or confidential record lost or stolen having a TAC of $225[2], the burden placed on healthcare providers to secure electronic health records is enormous. It is no surprise most of us feel we have lost control of our personal data[3]. This is especially true in the healthcare industry in the form of data breaches and HIPAA Privacy violations. Simultaneously, massive populations of users are fully-embracing new mobile applications to store and share data across platforms. As a result, cloud computing has bridged the gap between consumer devices and sensitive data. Is there a price to pay for our love affair with cloud-based apps and mobile devices?

As a cloud-based technology user, have you ever wondered about the safeguards protecting your personal and health information? Ever contemplated how modern operating systems like Google Android, Apple iOS and Microsoft Windows 10 access your data to provide cloud powered features? For example, Siri, the Dragon dictation cloud, Google Voice search and Docs all send voice recordings to the cloud and back while other built-in OS features share contacts between apps. These separate applications, when brought together on the same device, may also expose or "move" data in unintended ways. How do cloud-powered features impact these risks?

These questions and concerns are currently top-of-mind for IT and legal professionals responsible for managing electronic Protected Health Information (ePHI) while ensuring and maintaining HIPAA compliance. In light of the recent focus on HIPAA enforcement actions, hospitals, clinics, healthcare clearinghouses and business associates are trying to understand how to manage modern operating systems with cloud features to meet HIPAA regulatory mandates. Additionally, many of these healthcare organizations are under pressure to broadly embrace the benefits of cloud computing.

By pursuing global mandates such as the approaching European General Data Protection Regulation (GDPR) and domestic HIPAA mandates, Microsoft has invested heavily in security and privacy technologies to mitigate today's threats and made strides in ensuring personally identifiable information is not provided with the Basic level of Diagnostics Data. In April 2017, Microsoft released Creators Update 1703 for Windows 10[4]. This update provided granular details on amended basic level Windows diagnostic events and fields[5] and most importantly, furthered Microsoft's commitment to decreasing the exposure of ePHI.

The following whitepaper consists of three sections and appendices containing relevant guidance and illustrations intended to demonstrate how Microsoft Windows 10 Enterprise as a baseline operating system may enable and support HIPAA compliance, privacy, and security.

1 Gemalto Inc., Breach Level Index Report H1 2017 - http://www6.gemalto.com/breach-level-index-2017-h1-report
2 Ponemon Institute LLC report - sponsored by IBM Security - 2017 Cost of Data Breach Study - United States. - June 2017
3 Time Magazine, "9 in 10 Americans Feel They've Lost Control of Their Personal Data", November 12, 2014.
4 https://support.microsoft.com/en-us/help/4028685/windows-10-get-the-fall-creators-update
5 https://docs.microsoft.com/en-us/windows/configuration/basic-level-windows-diagnostic-events-and-fields

Part 1: Updates to Regulations and IT Security Compliance Implications

CIOs, IT Directors and IT Managers are often deputized as their organization's Health Insurance Portability and Accountability Act (HIPAA) Security Officer. In addition to being responsible for HIPAA security and compliance, these individuals may also be tasked with overseeing a company-wide upgrade to Windows 10. Organizations in every industry, including the Pentagon and Department of Defense's Secure Host Initiative[6], are upgrading to Windows 10 to improve their security posture. Windows 10 has been designed to be the most secure Windows yet and includes deep architectural advancements that change the game when navigating hacking and malware threats. However, as with all software upgrades, functionality, security and privacy implications must be understood and addressed. As mentioned above, due to Windows 10 (like all modern operating systems) potentially sending data to the cloud as part of its default operation, it is critical HIPAA Security Officers understand: "How does Windows 10 enable me to meet or exceed our HIPAA Security and Privacy requirement in my environment?"

A common misconception in the industry is that using Windows 10 opens an organization to HIPAA violations. The truth is Windows 10 can be easily configured to support HIPAA security and privacy requirements. This paper outlines such configurations and will review the bigger-picture cloud features, as applicable in over-arching security architecture:

The HIPAA Privacy Rule, at a high level, ensures individuals have a defined set of minimum allowable protections under the law. Incorrect configuration of any modern operating system could violate the following laws and may lead to HIPAA non-compliance in areas such as:

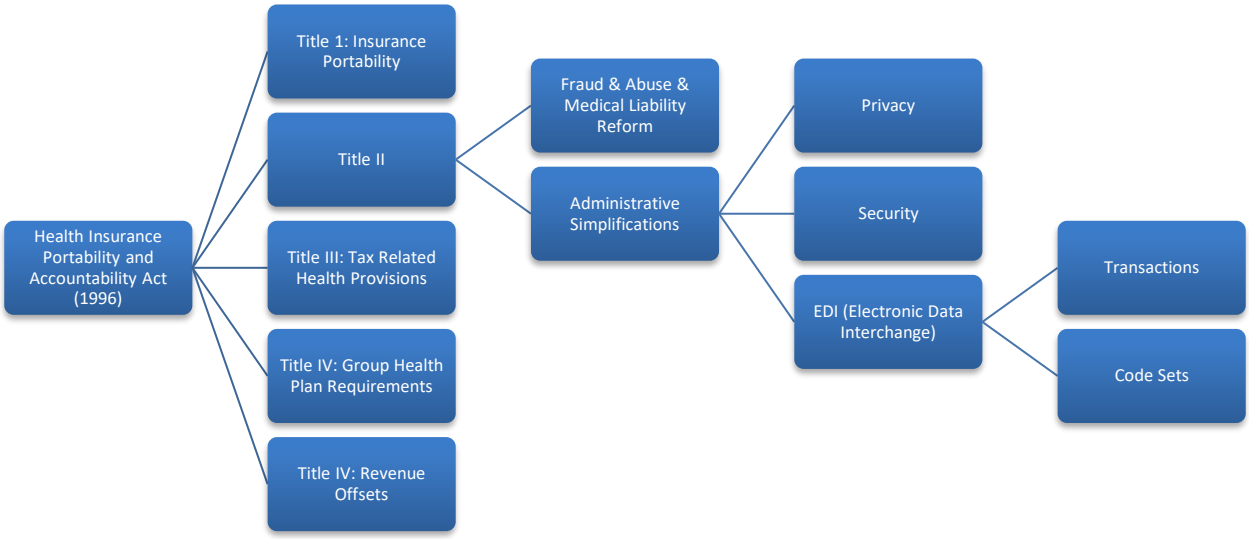
- Access to the health record – See patient rights §164.522, §164.524 §164.526
- Violations of minimum necessary uses of PHI - See use and disclosure §164.514
- Content and right to an Accounting of Disclosures – see privacy management process §164.528
- Business Associate Contracts – See privacy management process §164.504, §164.502, §164.524, §164.526,§164.528

[6] United States Department of Defense, "MEMORANDUM: Implementation of Microsoft Windows 10 Secure Host Baseline", February 26, 2016.

A key component of HIPAA compliance today is the demonstration of appropriate IT-related internal controls designed to mitigate fraud, risk and the implementation of safeguards for legally protected information that is stored and transmitted in electronic form. All users accessing this information are also required to meet IT compliance standards.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act was passed and signed into law on August 21, 1996, adding a new part C to title XI of the Social Security Act (sections 1171–1179.) Its inception was triggered by a growing awareness that American citizens were not provided basic rights to their own health information; specifically, the right to protect their personal information and retain a copy of their own health records. Throughout the 80's and 90's, the Federal government began receiving complaints stating they were not prepared to handle the mounting issue.



Early on, clinics and hospitals were not open to sharing medical records with patients for a number of reasons, including fear of competition and lack of internal processes to handle patient record requests.

Healthcare was late to embrace technology for patient care compared to most other industries. In the mid 2000's, splashy headlines read that America's healthcare costs were amounting to more of its Gross Domestic Product (GDP) than any other developed nation, and higher than many third-world countries. The trend of increasing health insurance premiums over-shadowed the increase in medical care costs as both those who could pay and those who could not were burdened.

In 2009, the world experienced a global recession and a still paper-based healthcare industry experienced skyrocketing costs. Pursuant to the American Recovery and Reinvestment Act (ARRA) passed by President Obama in 2009, $29 billion was earmarked under the HITECH Act to provide both incentives to Covered Entities (hospitals and clinic-based doctors) and penalties in

the form of Civil Monetary Penalties (CMP) for violating HIPAA Privacy, Security and Breach Notification standards. And with that, Meaningful Use was born.

While these changes were taking place, proactive enforcement of HIPAA's basic privacy and security standards were sorely lacking. Millions of records storing personal identities within big-data demographics were being converted to electronic personal health records without ensuring the security of the data. Across the healthcare landscape, medical records were unsecured and exposed. As a result, patient health data began being lost, stolen or inappropriately viewed/disclosed.

That same year, the Office for Civil Rights (OCR) was commissioned with the authority to enforce HIPAA Security, Privacy, and Breach Notifications. This authority allowed the OCR to develop an audit standard, strategy and process to respond to patient complaints and enforce the standards.

As required by the Health Information Technology for Economic and Clinical Health Act (HITECH, February 17, 2009), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) and HIPAA's final "HIPAA Omnibus Rule" (January 25, 2013); OCR issued a final "Guidance on Risk Analysis Requirements under the HIPAA Security Rule" on July 14, 2010. The guidance outlined that only NIST-based risk methodologies focused on security and compliance to the HIPAA rules were acceptable for conducting a bona fide HIPAA Security Risk Assessment and Analysis.

HITECH extended HIPAA's traditional safeguard requirements directly to "business associates" of "covered entities."[7] Covered entities include hospitals, medical billing centers, health insurance companies, healthcare clearinghouses and other healthcare providers. The ruling expanded HITECH's already broad "business associates" category, which includes: health information exchange organizations, e-gateways handling ePHI and subcontractors that create, receive, maintain, or transmit protected health information on behalf of a business associate[8].

Increased enforcement to ensure covered entities and business associates are compliant with the HIPAA Security, Privacy and Breach Notification Rules have raised public awareness for the need to protect ePHI. In recent years, the Office for Civil Rights (OCR) has taken significant strides by imposing fines through settlements against providers who have failed to take reasonable and appropriate safeguards to protect their ePHI.

Specifically, HIPAA requires healthcare organizations to:

1. Ensure the confidentiality, integrity, and availability of all electronically protected health information created, received, maintained, or transmitted
2. Regularly review system activity records, such as audit logs, access reports, and security incident tracking reports
3. Establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process containing ePHI
4. Monitor login attempts and report discrepancies
5. Identify, respond to and document PHI breach incidents as well as properly notify the specified parties

[7] HITECH Act Subtitle D, Section 13401.
[8] HITECH Act Subtitle D, Section 13408.

Under ARRA and HIPAA's Omnibus rule, virtually all organizations that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose ePHI must also comply with rigorous breach notification rules when PHI is compromised. For example, if the number of patients affected by a data privacy breach is more than 500 in a given state or jurisdiction, the media must be notified.[9]

The HIPAA standard for audit controls states, "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."[10] To comply, organizations must have systems and processes that collect, store, alert, and report on non-compliant ePHI access, use, or disclosure (i.e., breach), thus creating the required audit trail and limiting PHI disclosures to the minimum necessary.[11]

ePHI is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to any of the following:

1. The past, present or future physical or mental health or condition of an individual
2. Provision of healthcare to an individual
3. Payment for the provision of healthcare to an individual

If the information identifies or provides a reasonable basis to identify an individual, it is considered individually identifiable health information. Elements that make health information individually identifiable include, but are not limited to, the following 18 Identifiers:

(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

[9] HITECH Act Subtitle D, Section 13402.
[10] 45 CFR § 164.312(b).
[11] 45 CFR § 164.514(d).

(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
(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section[12].

The HIPAA Security Rule imposes standards in five categories: administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and documentation requirements (policies, procedures, etc.).

If a standard applies to ePHI, compliance is not optional. Strict adherence to specially-marked implementation specifications, however, can be considered optional, if after an assessment is performed they are determined to be "not reasonable and appropriate," the rationale to forgo the specification is documented, and evidence can be produced that a good faith effort was made to identify and implement "an equivalent alternative measure." Therefore, implementation specifications are categorized as either "required" or "addressable."

Required: If an implementation specification is marked as "required," it must be implemented by every covered entity.

Addressable: If an implementation specification is marked as "addressable", it may be used to determine if it is "reasonable and appropriate." If deemed reasonable and appropriate to protect ePHI, it must be adopted and followed. If, however, a covered entity has determined that an "addressable" implementation specification is unreasonable and inappropriate for its environment, the entity should make a good faith effort to identify, implement, and document an equally effective alternative solution, or justify and document the decision to do neither.

While the databases of EMR systems are obvious areas where ePHI resides, there are many other systems in which ePHI may be stored or transmitted, including personal (implanted) medical devices, modern medical equipment, tablets, cell phones, copiers, scanners, fax machines, multi-function devices, print servers, ePHI databases, encrypted email, voice mail servers, security camera systems, protected file servers, network shared drives and even on local machines. These "adjunct" areas of ePHI storage may or may not be within the organization's policy restrictions. Compliance with protecting all ePHI, however, is required. A table reflecting the current penalty amounts for violations of HIPAA[13] follows:

TABLE 2—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect-Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect-Not Corrected	50,000	1,500,000

The HIPAA Privacy rule covers protected health information in any medium while the HIPAA Security Rule focuses on the electronic medium, however, it is with both sets of regulations with which the covered entity and business associate is bound. HIPAA requires the covered entity to

[12] 45 C.F.R. § 164.514(b).

[13] See page 5583 of the Federal Register, January 25, 2013. Reference "TABLE 2—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE"

protect/prevent exposure of these 18 elements of specific data CONTENT, any element of which might possibly be transferred from the desktop electronically and may be exposed via email or file transfer. Any/all other content outside of these 18 elements is not identified as protected health information, therefore, not subject to this whitepaper. Additionally, other rules and regulations exist in order to also protect additional sensitive data categories (e.g. FISMA, PCI, SOX, etc.).

When using any desktop operating system, the default configuration *may* violate HIPAA. The Microsoft Privacy Statement as part of the Microsoft License term[14] provides very flexible language on how Personal Data is collected, used and shared. Specifically with respect to Windows, the Privacy Statement[15] states:

"Finally, we will access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to:

1. *Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies;*
2. *Protect our customers, for example to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone;*
3. *Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks; or*
4. *Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services - however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement."*

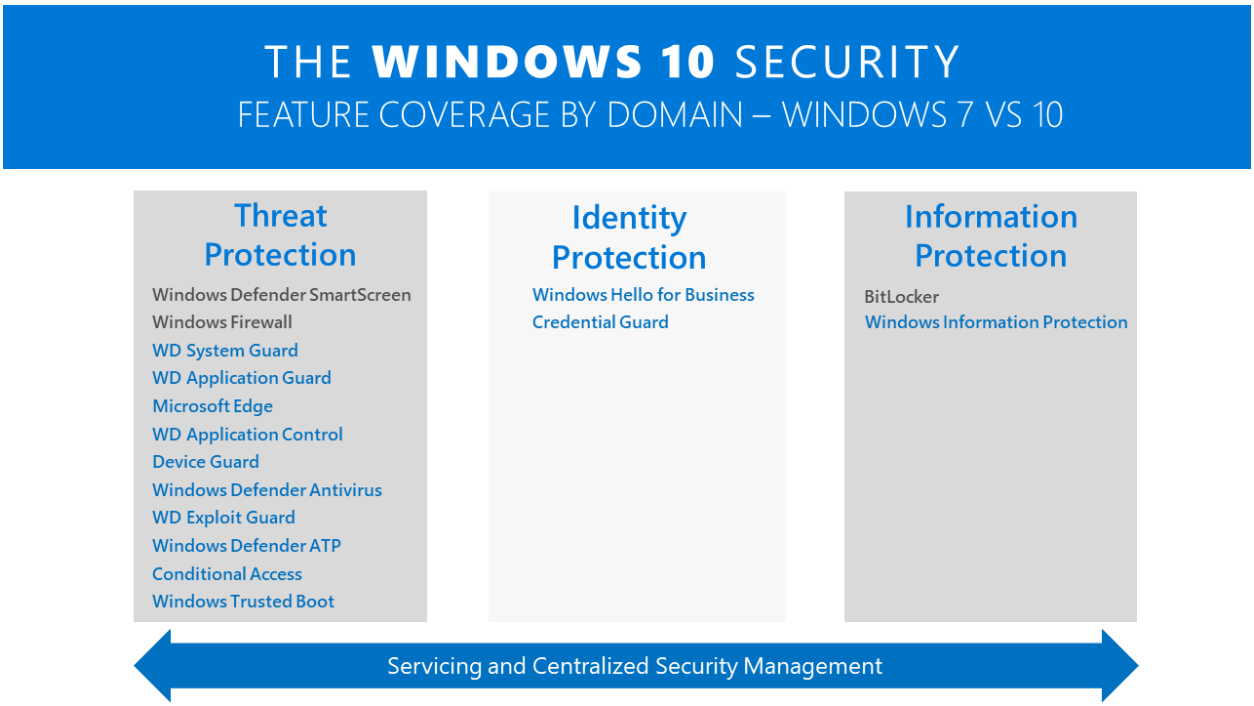
As with any convenient feature, there is always an impact on security, as security and functionality are often inversely related. Thankfully, Windows 10 Enterprise has been overhauled and most-recently updated with the Fall Creators Update to better-address today's persistent threats and helps healthcare organizations to apply their due diligence ensuring security and privacy under HIPAA.

[14] https://www.microsoft.com/en-us/Useterms/Retail/Windows/10/UseTerms_Retail_Windows_10_English.htm
[15] Microsoft, "Microsoft Privacy Statement" https://privacy.microsoft.com/en-us/privacystatement, Updated October 2017. For more information on Privacy, also see: https://privacy.microsoft.com/en-US/windows10privacy.

Part 2: Microsoft Windows 10 Enterprise: Data Security and HIPAA Compliance

With the proliferation of information security threats, mixed with the complexity of meeting HIPAA and GDPR regulatory mandates, healthcare organizations today need as many built-in compliance features as they can get. The Microsoft Windows 10 Enterprise Operating System provides organizations a solid foundation to meet many of the technical and administrative safeguards required by today's HIPAA Security mandates while also providing foundational IT security measures.

Microsoft's Windows 10 Enterprise architecture has been designed to protect user identity, device, and data. Windows 10 Enterprise has taken a fresh approach to operating system architecture and uses hardware-based virtualization to segregate high-value functions such as credential management from the core operating system. This approach dramatically reduces attack surfaces for hackers and malware proliferation.



All these capabilities are designed to provide additional controls for protecting, detecting and reducing the likelihood of data breaches.

Telemetry and Connected Apps

By default, Windows collects diagnostic that Microsoft uses to improve and further develop the product which has resulted in complaints about invasion of privacy including a recent formal notice filed by France's National Data Protection Commission (CNIL) in July of 2016. The formal notice procedure was dropped in June of 2017 and CNIL announced in reference to Microsoft, "The Company has reduced the volume of data collected under the 'base' level of its telemetry service by nearly half, identifying system problems and solving them. It limited this collection to

the data strictly necessary to maintain the system and applications in good working order and to ensure their safety. [16]".

Windows telemetry (which generates diagnostic data) provides vital technical data from Windows devices about the device and how Windows and related software are performing. That data used in the following ways[17]:

- To keep Windows up to date
- To keep Windows secure, reliable, and performant
- To improve Windows – through the aggregate analysis of the use of Windows
- To personalize Windows engagement surfaces

In the Fall Creators Update (Windows 10, version 1709), Telemetry data is categorized into four levels[18]:

- *Security*: Information that's required to help keep Windows secure, including data about the Connected User Experience and Telemetry component settings, the Malicious Software Removal Tool, and Windows Defender Antivirus. Note: This level is only available in Windows 10 Enterprise Edition.

- *Basic*: Basic device info, including: quality-related data, app compatibility, app usage data, and data from the Security level.

- *Enhanced:* Additional insights, including: how Windows and apps are used, how they perform, advanced reliability data, and data from both the Basic and the Security levels. The Creators Update also introduces the 'Limit Enhanced diagnostic data to the minimum required by Windows Analytics' feature, a subset of Enhanced called Device Health. This requires Enterprise or Education version and has the following data flow: Telemetry to Microsoft data center using Microsoft Data Management Service, Telemetry data analyzed by Microsoft Telemetry Service, Telemetry data pushed from Microsoft Telemetry Service to client OMS workspace, Telemetry data available in Device Health.[19]

- *Full:* All data necessary to identify and help to fix problems, plus data from the Security, Basic, and Enhanced levels

[16] https://www.cnil.fr/fr/windows-10-cloture-de-la-procedure-de-mise-en-demeure-lencontre-de-microsoft-corporation
[17] https://privacy.microsoft.com/en-US/windows10privacy
[18] Microsoft Corporation, "Configure Windows 10", October 20, 2017, https://opbuildstorageprod.blob.core.windows.net/output-pdf-files/en-us/MSDN.win-configuration-VSTS/live.pdf
[19] https://docs.microsoft.com/en-us/windows/deployment/update/device-health-monitor

The levels are cumulative and are illustrated in the following diagram:

The Windows 10 Enterprise system telemetry level may be configured utilizing the management tools you're already using. Details on this can be found here: https://technet.microsoft.com/itpro/windows/manage/configure-windows-telemetry-in-your-organization. This article also includes further details on data transmission, endpoints and retention.

Connected Features

There are also new end-user driven features that by default, communicate data that must be understood and accounted for by IT. These features include:

1. *Cortana*: Microsoft's answer to Siri, Google Talk and Alexa. Cortana "learns" how each person speaks and writes by taking samples. In addition, names, nicknames, recent calendar events and contacts are maintained.

2. *Settings Sync*: The default setting allows the operating system to sync a user's settings across multiple devices through the Microsoft cloud. It is intended to sync personal passwords, website plugins, favorites, etc. However, it may lead to users' credentials being vicariously breached if they use the same passwords across work and personal systems. According to Microsoft, the Settings Sync setting will be deprecated then modified for a different "improved" experience past the Fall Creators Update update. For now, turning this setting off or locking it down to only use Enterprise-friendly locations such as OneDrive for Business or SharePoint is recommended if this feature is required.

3. *3rd Party Advertisers*: The Advertising ID provides a unique identifier per user allowing collections of data to be shared with 3rd party advertisers. This is provided to help provide more effective targeted ads when using 3rd party applications. Turning this off will not block ads from appearing, but they will not be personalized.

4. *BitLocker*: *On a PC which is not joined to an Active Directory domain, ensure it meets the Windows Hardware Certification Kit (HCK) requirements: Connected standby and TPM 2.0 with Secure Boot. Windows 10 will automatically backup the recovery key on*

a personal OneDrive account. For domain joined PCs, the administrator can have the key automatically stored within the directory itself then cleared from the local system. Also, if you are using BitLocker or planning to use BitLocker, ensure you use the TPM+PIN option[20],turn off hibernation/sleep support or disable new DMA devices when this computer is locked Group Policy to avoid having to report a breach if a BitLocker-encrypted laptop is lost or stolen.[21]Those familiar with the Windows dialog box offering to send diagnostic information after a program crashes to Microsoft for product improvement.

By providing tools which make it possible to disable these built-in apps' connectivity, Microsoft, as part of its "zero-exhaust" initiative ensures no inadvertent data may be communicated to the Internet or other cloud services. Correctly configuring the telemetry level and app connectivity will significantly reduce your organization's risk of violating HIPAA.

To assist with the deployment of settings to restrict connections from Windows 10 to Microsoft, the Windows Restricted Traffic Limited Functionality Baseline may be applied. This baseline was created in the same way as the Windows security baselines often used to efficiently configure Windows to a known secure state. Running the Windows Restricted Traffic Limited Functionality Baseline on devices in your organization will allow you to quickly configure all of the settings covered in this document. However, some of the settings reduce the functionality and security configuration of your device and are therefore not recommended. Be sure you've chosen the right settings configuration for your environment before applying. Appendix A includes a template developed by HIPAA One that would make a fine configuration basis.

Below are some Microsoft resources to learn more about security configurations and telemetry:

Configure Windows telemetry in your organization
https://technet.microsoft.com/en-us/itpro/windows/manage/configure-windows-telemetry-in-your-organization

Microsoft Security Baselines
https://blogs.technet.microsoft.com/secguide/2017/10/18/security-baseline-for-windows-10-fall-creators-update-v1709-final/

Manage connections from Windows operating system components to Microsoft services
https://technet.microsoft.com/en-us/library/mt577208(v=vs.85).aspx#BKMK_Cortana

The next section will lay-out the HIPAA Security regulations as selected by the Office for Civil Rights (OCR) HIPAA Audit Protocol and break down exactly where Windows 10 Enterprise can help support HIPAA compliance.

[20] https://support.microsoft.com/en-us/kb/2516445

[21] https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-group-policy-settings#disable-new-dma-devices-when-this-computer-is-locked

Part 3: Windows 10 and HIPAA Traceability Section

With the explosive growth of cloud-usage and corresponding data communications, HIPAA One has extensively researched on how to configure Windows 10 Enterprise so that it can be "quiet" in terms of cloud-communications while maximizing functionality and end user experience. Considering HIPAA compliance requires due diligence, HIPAA One constructed the table below to identify the sections related to HIPAA within OCR's Audit Protocol unveiling where Windows 10 Enterprise can be utilized to achieve compliance.

There are other considerations, such as using Windows 10 hardware requirements to leverage Windows 10 Enterprise Operations System Features, the legal implications due to Microsoft's Privacy statements, and other editions of Windows 10 such as Windows 10 Pro and Home which do not offer the same controls (i.e. ability to turn off Telemetry). When installing any operating system in a computing environment which stores ePHI (or accesses sensitive information), it is critical to research and access to resources to manage the risk of information disclosures, even inadvertent outbound communications. Failure to apply some recommended and documented privacy and security strategies for Windows 10 Enterprise in a healthcare environment may expose organizations to potential HIPAA violations and potential penalties aforementioned in Part 1 above.

The following Windows 10 Enterprise HIPAA Safeguards table outlines where an entity may configure the operating system residing on dedicated hardware in alignment with HIPAA. The table demonstrates that Microsoft Windows 10 Enterprise can be configured to resist ePHI leakage through outside or cloud communications.

Appendix A addresses recommended Active Directory Group Policy settings for a basis of HIPAA compliance as it relates to the Windows 10 Enterprise operating system and "ultra-low-exhaust", or "near-zero-cloud" communication instances of the operating system "phoning home" to Microsoft with potential ePHI.

Windows 10 Enterprise (rolled-up with Fall Creators Update October 2017, 64-bit)[22] HIPAA Safeguards					
Section	**Citation**	**Specification**	**Description**	**Windows 10 Implementation Available?**	**Notes**
administrative	164.308(a)(1)(i)	Security Management Process	P&P to manage security violations	-	This is performed outside of the Operating System.
administrative	164.308(a)(1)(ii)(A)	Risk Analysis	Conduct vulnerability assessment	YES	Applying knowledge from this whitepaper helps achieve this requirement regarding ePHI communications outside of Treatment, Payment or Operations (TPO).
administrative	164.308(a)(1)(ii)(B)	Risk Management	Implement security measures to reduce risk of security breaches	YES	Implementing Windows 10 Enterprise with recommended privacy and security guideline.
administrative	164.308(a)(1)(ii)(C)	Sanction Policy	Worker sanction for P&P violations	-	This is performed outside of the Operating System.

[22] Bare metal installation, local installation of Windows 10 Enterprise with Fall Creators Update applied.

Section	Citation	Specification	Description	Windows 10 Implementation Available?	Notes
administrative	164.308(a)(1)(ii)(D)	Information system Activity Review	Procedures to review system activity	-	This is performed outside of the Operating System.
administrative	164.308(a)(2)	Assigned Security Responsibility	Identify security official responsible for P&P	-	This is performed outside of the Operating System.
administrative	164.308(a)(3)(i)	Workforce Security	Implement P&P to ensure appropriate ePHI access	-	This is performed outside of the Operating System.
administrative	164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Authorization/supervision for ePHI access	-	This is performed outside of the Operating System.
administrative	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Procedures to ensure appropriate ePHI access	-	This is performed outside of the Operating System.
administrative	164.308(a)(3)(ii)(C)	Termination Procedures	Procedures to terminate ePHI access	-	This is performed outside of the Operating System.
administrative	164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	P&P to separate ePHI from other operations	-	This is performed outside of the Operating System.
administrative	164.308(a)(4)(ii)(B)	Access Authorization	P&P to authorize access to ePHI	-	This is performed outside of the Operating System.
administrative	164.312(a)(1), 164.308(a)(4)(ii)(C), 164.308(a)(4)(i)	Access Establishment and Modification	P&P to grant access to ePHI	-	This is performed outside of the Operating System.
administrative	164.308(a)(5)(i)	Security Awareness Training	Training program for workers and managers	YES	Exercising diligence using Windows 10 Enterprise can meet this requirement.
administrative	164.308(a)(5)(ii)(A)	Security Reminders	Distribute periodic security updates	YES	Applying knowledge from this whitepaper helps achieve this requirement, along with security reminders, regarding training IT staff on secured OS configurations for HIPAA.
administrative	164.308(a)(5)(ii)(B)	Protection from Malicious Software	Procedures to guard against malicious software	YES	Turn on Windows 10 Security with Windows Defender Antivirus, AppGuard, DeviceGuard, SmartScreen and Microsoft Edge browser usage.
administrative	164.308(a)(5)(ii)(C)	Log-in Monitoring (IT Manager)	Procedures and monitoring of log-in attempts	-	Performed at the server-level.
administrative	164.308(a)(5)(ii)(D)	Password Management	Procedures for password management	YES	Password policies using Administrative Templates.
administrative	164.308(a)(6)(i)	Security Incident Procedures	P&P to manage security incidents	-	This is performed outside of the Operating System.
administrative	164.308(a)(6)(ii)	Response and Reporting	Mitigate and document security incidents	-	This is performed outside of the Operating System.
administrative	164.308(a)(7)(i)	Contingency Plan	Emergency response P&P	-	This is performed outside of the Operating System.
administrative	164.308(a)(7)(ii)(A)	Data Backup Plan	Data backup planning & procedures	-	This is performed outside of the Operating System.
administrative	164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Data recovery planning & procedures	-	This is performed outside of the Operating System.
administrative	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Business continuity procedures	-	This is performed outside of the Operating System.
administrative	164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Contingency planning periodic testing procedures	-	This is performed outside of the Operating System.

Section	Citation	Specification	Description	Windows 10 Implementation Available?	Notes
administrative	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Prioritize data and system criticality for contingency planning	YES	Identify Windows 10 Enterprise systems as access-devices which contain ePHI in a health care environment.
administrative	164.308(a)(8)	Evaluation	Periodic security evaluation	YES	Review Windows 10 Enterprise settings to ensure privacy and security configuration, and they are in line with best-practices.
administrative	164.308(b)(4)	Written Contract	Implement compliant BAAs	YES[23]	Microsoft does sign BAAs for Windows 10 Enterprise users – only if bundled with Microsoft cloud-based services (see footnote for details).
administrative	164.308(b)(1), 164.308(b)(3)	Written Contract	Obtain satisfactory assurances	YES[23]	Microsoft services covered under the BAA have undergone audits conducted by accredited independent auditors for the Microsoft ISO/IEC 27001 certification.
physical	164.310(a)(1)	Facility Access Controls	Physical safeguards for authorized server access	-	This is performed outside of the Operating System.
physical	164.310(a)(2)(i)	Contingency Operations	Procedures to support emergency operations	-	This is performed outside of the Operating System.
physical	164.310(a)(2)(ii)	Facility Security Plan	P&P to safeguard equipment and facilities	-	This is performed outside of the Operating System.
physical	164.310(a)(2)(iii)	Access Control Validation Procedures	Facility access procedures for personnel	-	This is performed outside of the Operating System.
physical	164.310(a)(2)(iv)	Maintenance Records	P&P to document security-related repairs and modifications	-	This is performed outside of the Operating System.
physical	164.310(b)	Workstation Use	P&P to specify workstation environment	-	This is performed outside of the Operating System.
physical	164.310(c)	Workstation Security	Physical safeguards for workstation access	-	This is performed outside of the Operating System.
physical	164.310(d)(2)(i)	Disposal	P&P to manage media and equipment disposal	YES	Using Device Encryption, BitLocker and BitLocker to Go may assist in this requirement rendering the ePHI unusable.
physical	164.310(d)(2)(ii)	Media Re-use	P&P to remove ePHI from media and equipment	YES	Using Device Encryption, BitLocker and BitLocker to Go may assist in this requirement rendering the ePHI unusable.
physical	164.310(d)(1), 164.310(d)(2)(iii)	Accountability	Document hardware and media movement	-	Using System Center Configuration Manager to manage inventory scans can assist in meeting this requirement.

[23] https://www.microsoft.com/en-us/trustcenter/Compliance/HIPAA. Syncing personal content through the OneDrive consumer client is not covered by Microsoft's BAA. Alternatively, Microsoft recommends the use of enterprise-ready cloud storage such as OneDrive for Business which is covered by Microsoft's BAA and enables a healthcare covered entity to properly store and secure its sensitive information. Microsoft does not have a BAA for any version or any part of Windows 10.

Section	Citation	Specification	Description	Windows 10 Implementation Available?	Notes
physical	164.310(d)(2)(iv)	Data Backup and Storage	Backup ePHI before moving equipment	-	This is performed outside of the Operating System.
technical	164.312(a)(2)(i)	Unique User Identification (EMR/ePHI/PII Administrator)	Assign unique IDs to support tracking	-	This is performed outside of the Operating System.
technical	164.312(a)(2)(ii)	Emergency Access Procedure	Procedures to support emergency access	-	This is performed outside of the Operating System.
technical	164.312(a)(2)(iii)	Automatic Logoff	Session termination mechanisms	YES	Idle Timer settings may be set to meet this requirement at the local machine-level.
technical	164.312(a)(2)(iv)	Encryption and Decryption	Mechanism for encryption of stored ePHI	YES	Using Device Encryption, BitLocker and BitLocker to Go may assist in this requirement rendering the ePHI unusable.
technical	164.312(b)	Audit Controls	Procedures and mechanisms for monitoring system activity	-	This is performed outside of the Operating System.
technical	164.312(c)(1)-(2), 170.314(d)(1)(ii)	Mechanism to Authenticate Electronic Protected Health Information	Mechanisms to corroborate ePHI not altered	-	This is performed outside of the Operating System.
technical	164.312(e)(1)-(2)(i), 170.314(d)(8)	Integrity Controls	Measures to ensure integrity of ePHI on transmission	-	This is performed outside of the Operating System.
technical	164.312(e)(1)-(2)(ii)	Encryption	Mechanism for encryption of transmitted ePHI	-	This is performed outside of the Operating System.
organizational	164.314(a)(2)(i)(A)-(C), 164.314(a)(2)(ii)-(iii)	Business Associate Contracts	BAAs must contain security language	YES[24]	Microsoft does sign BAAs for Windows 10 Enterprise users – only in conjunction with Office365.
organizational	164.314(a)(1)	Business Associate Contracts or Other Arrangements	Approval process for contract template deviations	-	This is performed outside of the Operating System.
technical	164.312(d)	Audit Controls	Audit Controls	-	This is performed outside of the Operating System.
technical	164.312(b)	Audit Controls	Procedures and mechanisms to monitor system activity	-	This is performed outside of the Operating System.
organizational	164.314(b)(1)	Requirements and specifications	Plan Sponsor demarcation	-	This is performed outside of the Operating System.
organizational	164.314(b)(1)	Requirements and specifications	Plan Sponsor agreements must contain security language	-	This is performed outside of the Operating System.
organizational	164.314(b)(1), 164.314(b)(2)(i)-(iv)	Requirements and specifications	Plan Sponsor agreements must contain security language	-	This is performed outside of the Operating System.

[24] http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=52&Language=1

Section	Citation	Specification	Description	Windows 10 Implementation Available?	Notes
organizational	164.316(a),(b)(1)	Documentation	Document P&P and actions & activities	-	This is performed outside of the Operating System.
organizational	164.316(b)(2)(i)	Time Limit	Retain documentation for 6 years	-	This is performed outside of the Operating System.
organizational	164.316(b)(2)(ii)	Availability	Documentation available to system administrators	-	This is performed outside of the Operating System.
organizational	164.316(b)(2)(iii)	Updates	Periodic review and updates to changing needs	-	This is performed outside of the Operating System.

Appendix A: Suggested Active Directory Administrative Settings and Registry settings for Data Security and Cloud Communications with Packet Captures

The following configuration was tested and verified to provide minimal cloud-communications that would not compromise required functionality. (e.g. Allow Windows Registration data, etc.). It is provided as a suggested configuration to reduce data communications as initiated by the cloud-features of Windows 10 Enterprise.

The test computer system was a default installation of the Windows 10 Enterprise Anniversary Edition and part of an Active Directory Domain with the following Group Policy Object (GPO) settings:

- Computer Configuration>System>User Profile
  - Turn off the advertising ID
- Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication settings
  - Turn off Automatic Root Certificates Update - Enabled
  - Turn off the handwriting recognition error reporting - Enabled
  - Turn off Windows Customer Experience Improvement Program – Enabled
  - Turn off printing over HTTP – Enabled
  - Turn off downloading of print drivers over http – Enabled
  - Turn off Windows Error Reporting – Enabled
  - Turn off internet file association Service - Enabled
  - Turn off access to the Store – Enabled[25]
  - Turn off handwriting personalization data sharing - Enabled
- Computer Configuration>Administrative Templates>Regional and Language Options>Handwriting personalization
  - Turn off automatic learning - enable
- Computer Configuration > Administrative Templates > System > Device Installation >
  - Prevent device metadata retrieval from the Internet - Enabled
- Computer Configuration>Administrative Templates>Windows Components>Data Collection and Preview Builds>
  - Allow Telemetry – enable – Level 0 (*Microsoft recommends* 1)[26]
  - Disable Pre-release feature or settings – Disabled
  - Toggle User control over insider builds – Disabled
  - Do not show feedback notifications – Enabled
- Computer Configuration > Administrative Templates > Windows Components > Internet Explorer
  - Prevent participation in the Customer Experience Improvement Program – Enabled
  - Turn on Suggested Sites – Disabled

[25] Microsoft recommends disabling the consumer aspects of the store by only showing the private store (which is 100% fully managed by the organization). This allows items such as calculator to continue to be used while reaching the level of security that is desired. All of the necessary steps are available here: https://docs.microsoft.com/en-us/windows/configuration/stop-employees-from-using-microsoft-store

[26] Microsoft recommends maintaining this setting to Level 1 for expedient, relevant security updates. See Appendix B for a post-"Fall Creators Update" discussion on the Basic level of telemetry in a privacy and security baseline.

    - Allow Microsoft services to provide enhanced suggestions as the user types in the Address Bar – Disabled
    - Turn off the auto-complete feature for web addresses - Disabled
    - Disable Periodic Check for Internet Explorer software updates- Disabled
    - Turn off browser geolocation – Enabled
- Computer Configuration > Administrative Templates > Windows Components > Windows Media Digital Rights Management
    - Prevent Windows Media DRM Internet Access – Enabled
- User Configuration > Administrative Templates > Windows Components > Location and Sensors
    - Turn off location - Enabled
    - Turn off sensors - Enabled
- User Configuration > Administrative Templates > Windows Components > Windows Media Player
    - Prevent Music File Media Information Retrieval Enabled
- Computer Configuration>Administrative Templates>Windows Components>Application Compatibility
    - Turn off Application Telemetry – Enabled
    - Turn off Inventory Collector – Enabled
    - Turn off Program Compatibility Assistant - Enabled
    - Turn off Step Recorder – Enabled
- Computer Configuration>Administrative Templates>Windows Components>Camera
    - Allow use of Camera - Disabled
- Computer Configuration > Administrative Templates > Windows Components > App Privacy >
    - Let Windows apps access the camera – Disabled
    - Let Windows apps access location – Disabled
    - Let Windows apps access Microphone – Disabled
    - Let Windows apps access account information – Disabled
    - Let Windows apps control radios – Disabled
    - Let Windows apps sync with devices – Disabled
    - Let Windows apps access motion – Disabled
- Computer Configuration>Administrative Templates>Windows Components>Cloud Content
    - Do not show Windows Tips - Enabled
    - Turn off Microsoft Customer experiences – Enabled
- Computer Configuration > Administrative Templates > Windows Components > File Explorer
    - Configure Windows SmartScreen – Enabled
- Computer Configuration > Administrative Templates > Windows Components > MDM
    - Disabled MDM Enrollment – Enabled
- Computer Configuration > Administrative Templates > Windows Components > Online Assistant
    - Turn off Active Help – enabled

- Computer Configuration > Administrative Templates > Windows Components > OneDrive > OneDrive
    - Prevent the usage of OneDrive for file storage – Enabled[27]
- Computer Configuration > Administrative Templates > Windows Components > Search
    - Allow Cortana – Disabled
- Computer Configuration > Administrative Templates > Windows Components > Store >
    - Disable all apps from Windows Store - Enabled[28]
- Computer Configuration > Administrative Templates > Windows Components > Windows Error Reporting
    - Disable Windows Error Reporting – Enabled
- Computer Configuration > Administrative Templates > Windows Components > Windows Defender > MAPS
    - Join Microsoft MAPS - Disabled[29]
- Computer Configuration\Administrative Templates\Network\WLAN Service\WLAN Settings\
    - Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services – Disabled
    - Do not Allow web search – Enabled
- Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Security Options>Interactive logon
    - Machine inactivity limit - Enabled

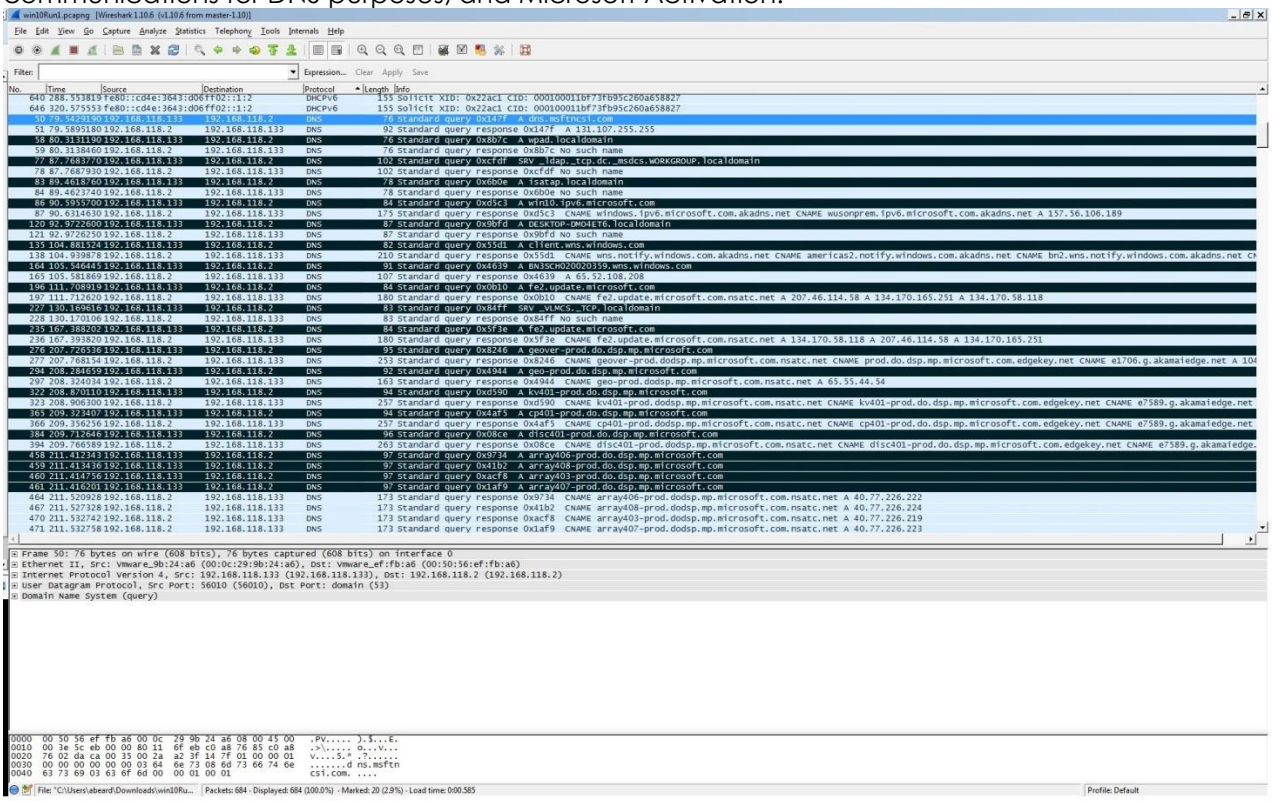
The results of a workstation with the applied above configuration showed conversations kicked-off to the Internet during a 1 hour turn-on, login and wait period. For a copy of the data sniffer

[27] Microsoft recommends the use of enterprise-ready cloud storage such as OneDrive for Business which is covered by Microsoft's BAA and enables a healthcare covered entity to properly store and secure its sensitive information. https://support.office.com/en-us/article/Use-Group-Policy-to-control-OneDrive-sync-client-settings-0ecb2cf5-8882-42b3-a6e9-be6bda30899c.
This policy lets you block users from syncing personal files to the OneDrive storage space they get with a Microsoft account. By default, users are allowed to sync personal OneDrive accounts. Enabling this policy sets the following registry key value to 1.
[HKCU\SOFTWARE\Microsoft\OneDrive]"DisablePersonalSync"=dword:00000001
If this setting us enabled, users will be prevented from setting up a sync relationship for their personal OneDrive account. If they had previously been syncing a personal OneDrive account, they are shown an error when they start the sync client, but their files remain on the computer.
If this setting is disabled, users are allowed to sync personal OneDrive accounts.

[28] Microsoft recommends disabling the consumer aspects of the store by only showing the private store (which is 100% fully managed by the organization). This allows items such as calculator to continue to be used while reaching the level of security that is desired. All of the necessary steps are available here: https://docs.microsoft.com/en-us/windows/configuration/stop-employees-from-using-microsoft-store

[29] Microsoft recommends the Cloud Protection (MAPS) setting to be enabled out of the box as it is one of the most important Antivirus features in Windows. Disabling it will cause a delay in clients receiving the latest threat intelligence by hours making clients dramatically more susceptible to emerging threats like ransomware. Microsoft believes that it is very unlikely the Cloud Protection service would encounter patient information being encoded in the file and folder names as this is a rare application implementation. For this reason, Microsoft recommends the setting should be ENABLED and a caution should clearly be visible. The caution should request that organizations review their applications to see if they encode patient information in the file and folder names and if so the recommendation should be to DISABLE it.

traces in PCAPNG format, click here. A DNS query of packet communications shows limited communications for DNS purposes, and Microsoft Activation.



This is a list of DNS Queries from the WireShark packet capture exercise (Local Area Network Domain references were removed):

DNS.MSFTNCSI.COM
WIN10.IPV6.MICROSOFT.COM
CLIENT.WNS.WINDOWS.COM
BN3SCH020020359.WNS.WINDOWS.COM
FE2.UPDATE.MICROSOFT.COM
FE2.UPDATE.MICROSOFT.COM
GEOVER-PROD.DO.DSP.MP.MICROSOFT.COM
GEO-PROD.DO.DSP.MP.MICROSOFT.COM
KV401-PROD.DO.DSP.MP.MICROSOFT.COM
CP401-PROD.DO.DSP.MP.MICROSOFT.COM
DISC401-PROD.DO.DSP.MP.MICROSOFT.COM
ARRAY406-PROD.DO.DSP.MP.MICROSOFT.COM
ARRAY408-PROD.DO.DSP.MP.MICROSOFT.COM
ARRAY403-PROD.DO.DSP.MP.MICROSOFT.COM
ARRAY407-PROD.DO.DSP.MP.MICROSOFT.COM

Varying results are possible with additional programs installed outside of the base-installation of Windows 10 Enterprise. Therefore, any additional programs, applications or utilities installed that alter data communications are outside the scope of this whitepaper and should be considered when new applications are introduced.

Appendix B: Response to Microsoft Fall Creators Update for Windows 10

In October 2017, Microsoft released the Fall Creators Update for Windows 10. This update provided granular details and a basic level of Windows diagnostic events and fields focused on machine and data extensions. Most importantly, the update furthered Microsoft's commitment to decreasing the exposure of ePHI.

Microsoft continues to be forthcoming regarding the user data they collect and may have taken all steps necessary to minimize the exposure of that data. It is here that Microsoft showcases their pledge to exclude ePHI which may exist on any computer operated by any covered entity.

After the release of the Fall Creators Update in October of 2017, Microsoft issued this statement:

"*We have taken significant steps to ensure that the data collected at the Basic level is limited to the data necessary to keep the device update to date performant and secure. We invite customers to confirm for themselves that the data collected at Basic includes data about the user's device only and does not include the content of documents, emails, or any other sensitive personal information about them or their clients.*" – Marisa Rogers, Microsoft WDG Privacy Officer

HIPAA One reviewed Microsoft's statements and after considering the recent court-order dropped by the French Government[30] and Microsoft's focus on the upcoming GDPR regulatory mandate, Microsoft appears committed to its Covered Entity users.

It is for this reason, HIPAA One has the opinion that the Basic telemetry setting may be used in a healthcare environment to take advantage of the benefits of this diagnostic data with faster bug-fixes, security and performance of their Windows 10 Enterprise installations while retaining adhering to a privacy and security baseline and preparing for GDPR compliance. With new features available such as Windows Analytics[31] to view machine health and upgrade information, healthcare IT decision-makers can decide for themselves if they wish to take a further step in configuring Basic or Security/Off setting in Telemetry.

[30] https://www.cnil.fr/fr/windows-10-cloture-de-la-procedure-de-mise-en-demeure-lencontre-de-microsoft-corporation

[31] https://aka.ms/windowsanalytics