Windows 10 & HIPAA

Data privacy and security concerns are mounting against Microsoft's newest operating system.

We look at trends in how Microsoft has handled data security in the past,

and tell you what you can do to protect your data moving forward.

Brought to you by:

Compliancy Group

Achieve.Illustrate.Maintain.

Compliance Simplified

One Year Out: Is Windows 10 HIPAA Compliant?

Since it was first released in July of 2015, Microsoft has remained silent about Windows 10 and HIPAA compliance. The organization has been asked time and again by journalists, thinkers, and influencers across the tech and health care IT industries about whether or not the most recent iteration of their Windows operating system complies with data privacy and security regulations set forth by the US government under HIPAA.

Similar to its peers Apple and Google, Microsoft has avoided the topic of HIPAA, leaving the liability in the hands of their users.

Contrary to its silence on Windows 10, Microsoft has been vocal about its HIPAA-compliant Office 365. The company willingly signs Business Associate Agreements (BAAs) with SharePoint Online cloud-storage service users, and many HIPAA Covered Entities and Business Associates have since adopted it for their businesses.

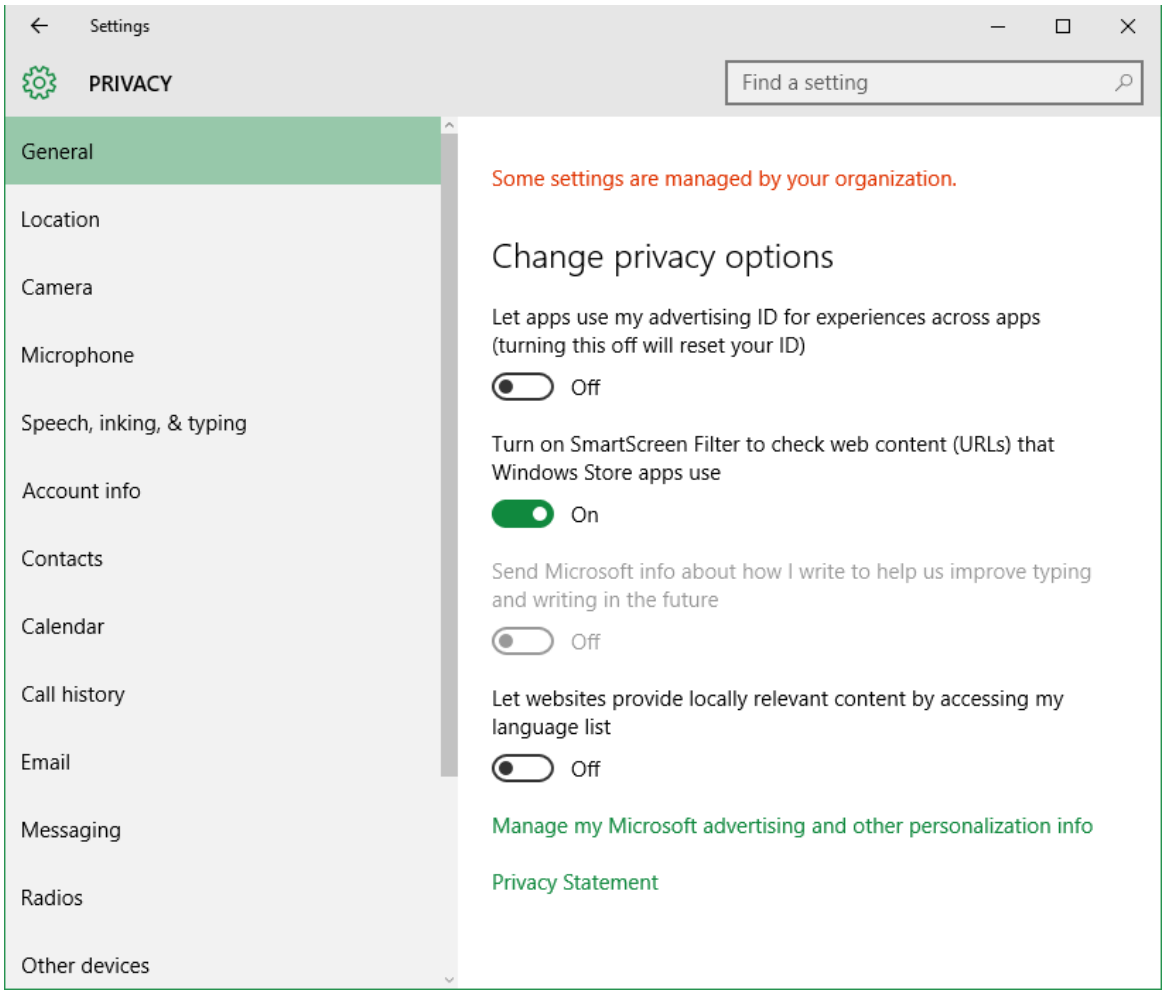
Understanding what exactly Windows 10 does with users' data is where the major conflicts with HIPAA come into play. We're going to be discussing what you can do to limit the amount of data that Microsoft can access from your device, but first let's dive into the issue of security.

Windows and Data Security

Windows users face a dilemma: new operating systems collect data for Microsoft, but older operating systems can expose data to hackers and malware. Both cases pose serious issues for HIPAA-beholden organizations, begging the question: Is Windows HIPAA Compliant? To answer, we'll need to dive into some of the ongoing security issues that affect Windows devices.

Windows XP was first released in 2001, and was the most widely used Windows operating system for 11 years until Windows 7 overtook it in August 2012. Now, Microsoft is no longer releasing security updates or patches for the system. Since extended support ended in May of 2014, numerous security holes have been discovered within the operating system. Windows XP devices are remotely exploitable, meaning that attackers can access users' computers and execute any function they want, virtually unfettered because of these security loopholes. About 7% of Windows users still use XP, posing a serious risk to any data still being stored or processed by these devices.

Conversely, Windows 10 is routinely updated through service packs from Microsoft. Security is a far less sensitive issue for users because of some of the built-in measures that come standard on all Windows 10 devices.



SmartScreen Filter is an Internet Explorer feature that can stop websites from downloading malware or phishing your personal data. This feature will be activated by default on your device, but can be accessed by going to **Settings > Privacy > General** and then reading through the privacy options listed on the right.

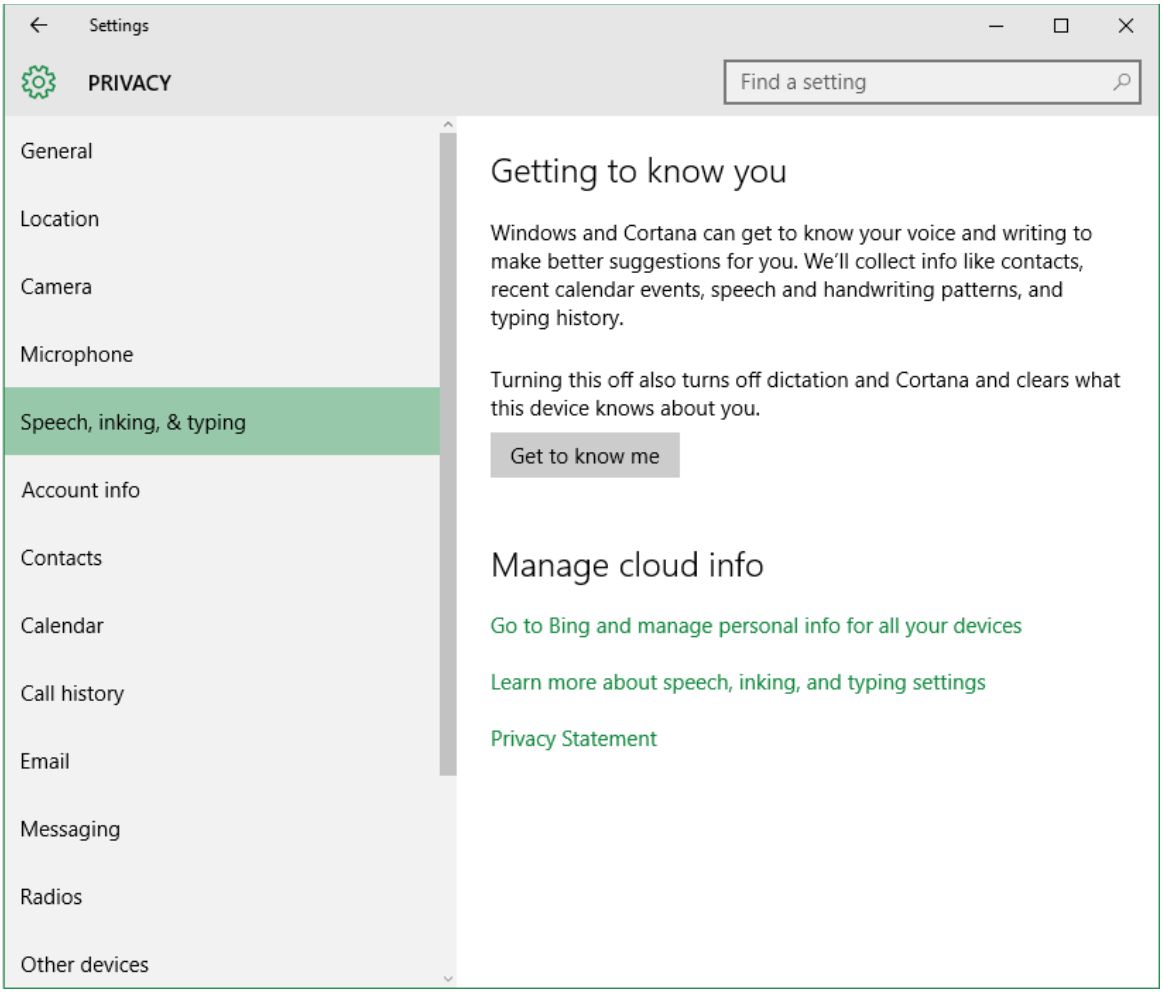
Windows and Data Privacy

The **Settings > Privacy** screen is also where users can access a variety of other privacy options. If you installed Windows 10 using the "Express Install" option, it's extremely important that you click through these menus and set as many of these options to **Off** as possible.

By default, Windows 10 devices automatically share the maximum amount of users' information with Microsoft. Microsoft uses this data to customize users' experience with ads and apps. For users who don't handle sensitive data, this doesn't pose a serious issue. But for HIPAA-beholden organizations and health care practices, this is precisely the kind of sharing that can lead to serious breaches of protected health information (PHI).

By navigating through these **Privacy** menus, users can significantly limit the amount of data that gets processed by Microsoft.

Some Windows 10 devices are also equipped with Cortana, a personal AI assistant similar to Apple's Siri. Devices with Cortana enabled will collect any speech, writing, or typing done on them to personalize users' experience. This data collection poses a significant risk to the privacy and integrity of data being stored on Windows 10 devices in addition to anything spoken near or typed on one of these devices.



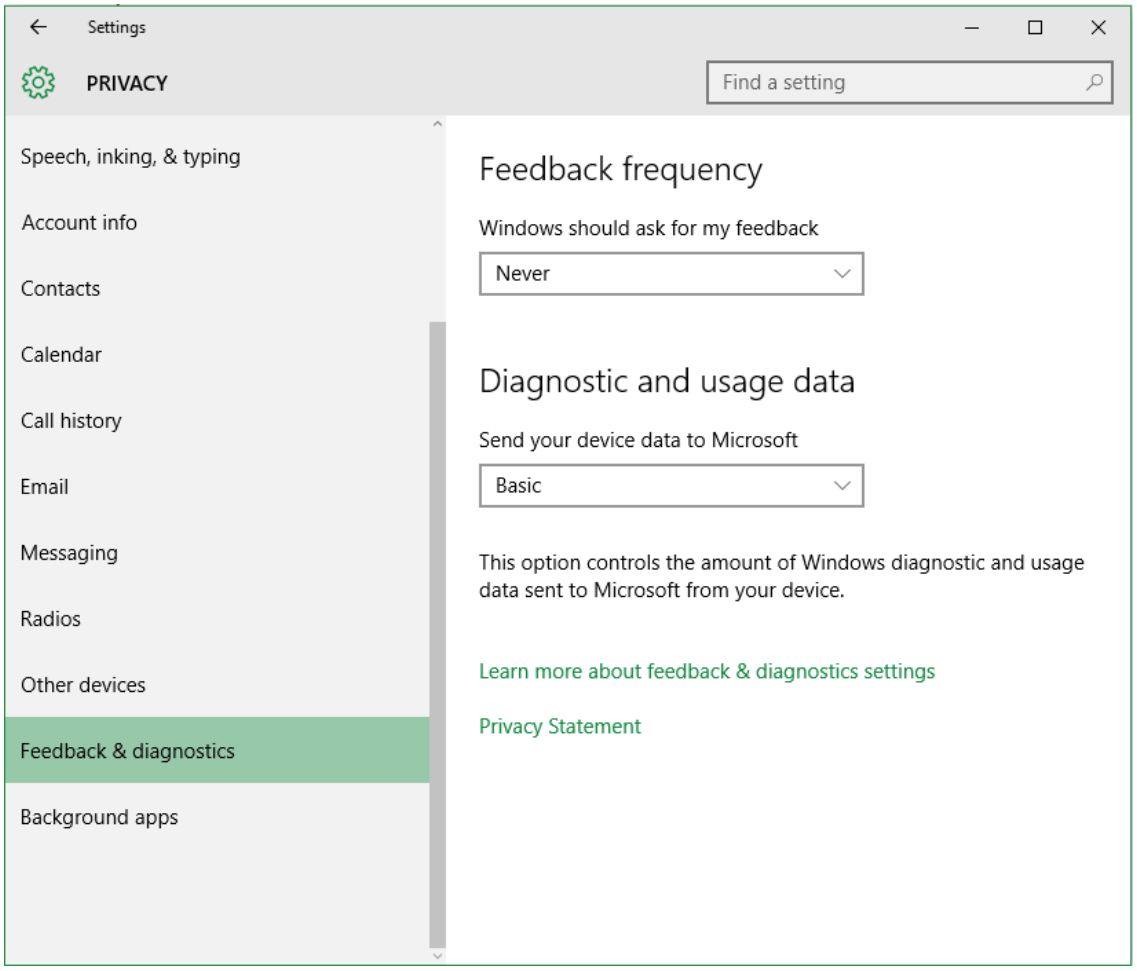
HIPAA beholden entities should immediately navigate to **Settings >Privacy > Speech, inking, & typing**, where they can toggle Cortana on or off. If a grey box appears labeled **Get to know me** appears, that means that Cortana is already disabled. Click on the green box labeled **Stop getting to know me** in order to turn Cortana off.

Any information gathered by Cortana is automatically stored by Microsoft. The organization has not clearly explained how this collection occurs or what steps are taken--if any--to protect it. Is the data anonymized on users' local devices or in Microsoft's

servers? Is the data encrypted before it's sent to Microsoft? Is the data being stored by Microsoft?

These questions raise serious concerns about the way that sensitive information is stored and used by Microsoft. HIPAA-beholden entities cannot risk this potential breach of PHI, so the best course of action is to just turn off the feature entirely.

Next, users should navigate to the **Settings > Privacy > Feedback & diagnostics** menu.



Here, users can limit the amount of feedback sent from their devices to Microsoft by changing the **Feedback frequency** to **Never**. Users can also choose how much **Diagnostic and usage data** they send to Microsoft from this menu. The options here, are **Full**, **Enhanced**, and **Basic**. Users should change the setting to **Basic** to limit the amount of data sent to Microsoft from their devices.

This is where the problem of data sharing comes, though. Users do not have the option of turning **Diagnostic and usage data** off entirely, meaning that there's no way to entirely restrict Microsoft's access here. Again, this does not pose a major problem to most users, but Covered Entities or Business Associates concerned with the privacy of their patients' or clients' PHI have no way to ensure that Microsoft won't have access to this information.

Windows and HIPAA Compliance

The fact that this data sharing must remain active is where the issue of Windows 10's compliance with HIPAA regulation comes into play.

PHI can only be shared lawfully between two organizations if they have executed a Business Associate Agreement. BAAs are meant to guard against liability in the event of a data breach. Both parties must agree that they are beholden to HIPAA. If one of the organizations is responsible for a data breach, a BAA ensures that that organization is the one held responsible.

Although Microsoft signs BAAs with users of its SharePoint cloud-service, the organization does not sign BAAs with users of Windows 10. Combine this with the **Diagnostic and usage data** that must be sent to Microsoft, and users put themselves in a situation where PHI can potentially be transmitted without lawful consent.

According to Microsoft:

> **Basic** data is data that is vital to the operation of Windows. This data helps keep Windows and apps secure, up-to-date, and running properly by letting Microsoft know the capabilities of your device, what is installed, and whether Windows is operating correctly. This option also includes basic error reporting back to Microsoft. **Basic** data includes:
>
> - Configuration data, including the manufacturer of your device, model, number of processors, display size and resolution, date, region and language settings, and other data about the capabilities of the device.
> - The software (including drivers and firmware supplied by device manufacturers), installed on the device.
> - Performance and reliability data, such as how quickly programs respond to input, how many problems you experience with an app or device, or how quickly information is sent or received over a network connection.
> - Network and connection data, such as the device's IP address, number of network connections in use, and data about the networks you connect to, such as mobile networks, Bluetooth, and identifiers (BSSID and SSID), connection requirements and speed of Wi-Fi networks you connect to.
> - Other hardware devices connected to the device.

The vagueness here is cause for concern for HIPAA-beholden entities. One year after the release of Windows 10 and users still don't have a clear understanding of what data is being collected from them.

Microsoft has given users enhanced security from hackers and malware incidents. But the common trend of corporate data collection has put sensitive health data at risk of

exposure just the same. Windows 10 users need to weigh these risks to security against the measures being taken within their own organization to guard the privacy of PHI.

Compliance and security are dynamic parts of any business. They must be adapted to changes in technology and privacy issues as they arise. The process should be uniquely catered to the organization at hand, and the same holds true for users of Windows 10. By limiting the amount of data that Microsoft can access, HIPAA-beholden organizations can keep their privacy in check. Hopefully, further guidance and new service packs from Microsoft will lend some further clarity to the issue. Until that time, users should continue to heavily vet their technology infrastructure to ensure that the PHI they come into contact with stays protected and secure.

Why Compliancy Group?

The former auditors who founded Compliancy Group realized that better HIPAA compliance wouldn't come from better auditing tools. The means to successfully audit across the different components of compliance are well established, but with traditional, fragmented means of implementation, they prove cumbersome and inaccessible to most employees and administrators at organizations facing an audit by HHS.

The Guard accomplishes the task of simplifying HIPAA compliance. It provides clients with a complete tool to Achieve compliance, Illustrate this to their patients, and Maintain that compliance through continued self-assessment. The Guard fosters a continually accessible means of monitoring privacy and security while keeping tabs on policy and procedures in place to eliminate potential breaches.

Since 2012 Compliancy Group has been recognized as the premier solutions to compliance issues faced by healthcare professionals. CRN named The Guard a Top 10 Compliance Tool (2012) and listed Compliancy Group among their Emerging Vendors in 2015. Endorsements by industry leaders such as McGladrey/RSM, the Practice Management Institution, Telehouse, eClinicalWorks, and AOAExcel.

Compliancy Group gives doctors and health care decision-makers confidence that they're HIPAA compliant so that they can focus on running their practice or organizaiton. No client who has used The Guard has ever failed an Office of Civil Rights (OCR) or Centers for Medicare & Medicaid Services (CMS) audit.

Compliancy Group provides partners with a distinction from the myriad of third-party consultants by incorporating The Guard into the services they already provide. Partners maintain the brand and trust they have built with their clients, and add an effective and complete solution to their offerings that comes with a peace of mind absent from other services on the market. The value that Compliancy Group offers to clients and prospects is matched by the highly profitable and recurring revenue stream that partners gain from these relationships.

HIPAA regulations are constantly morphing to accommodate advancements in technology and security, and Compliancy Group is adapting in kind. The Guard is the simple web-based solution that health care professionals need, delivered directly by partners they can trust.

Want more information? Visit us at www.compliancy-group.com

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified