Microsoft

A holistic approach to data security, privacy, and compliance for healthcare

Contents

1

Protect health information

Healthcare organizations (HCOs) manage our most personal and sensitive data

Earning and keeping patients' trust is essential, and the reputational risk is enormous. Patient data is under assault from a wide array of threats. Vulnerabilities include external attacks, internal attacks, and inadvertent leakage.

In response to multiple, massive breaches of healthcare data, federal and state governments have stepped in with regulations.

Clinicians endeavor to deliver the best care to patients and coordinate care delivery in this context of heightened and complex vulnerabilities. Digital engagement with patients is also an imperative that introduces its own kind of vulnerabilities. You must defend against hackers, phishing attacks, and a myriad of threats growing in intensity and sophistication every year.

Microsoft understands these risks and what it takes to manage them. Microsoft 365 offers a cloud computing solution with built-in security to help you safeguard protected health information (PHI), keep up with regulatory compliance, and manage data governance for your organization.

The Intelligent Security Graph

Security services from Microsoft 365 are powered by the Intelligent Security Graph. To combat cyberthreats, the Intelligent Security Graph uses advanced analytics to link threat intelligence and security signals from Microsoft and partners. Microsoft operates global services at a massive scale with billions of security signals that power protection layers across the stack. Machine learning models reason over all this intelligence, and the signal and threat insights are widely shared across our products and services. This allows us to detect and respond to threats more quickly and bring actionable alerts and information to our customers for remediation. Our machine learning models are continuously trained and updated with new insights, helping us build more secure products and provide more proactive security.

Where do you start?

This e-book provides insight into security and compliance solutions for organizations like yours to protect the PHI you are the steward of.

2

Why do cybersecurity and compliance matter to healthcare providers?

The healthcare industry is a top target for cybercriminals

In 2018 the healthcare industry again led all others in cybersecurity breaches, claiming more than a quarter of the incidents reported in BakerHostetler's latest Data Security Incident Response Report.[1] Specifically, health information was the second most at-risk type of data in cyber incidents. While social security numbers are the most aggressively attacked data, a full third of potentially compromised records are health information. And it's not just external attacks—55 percent of all incidents involved some kind of insider error or activity, according to the report.

In one recent example, a US-based medical center notified 12,000 patients that an early 2018 phishing attack may have exposed their PHI.[2] In another recent example, a public agency notified 4,882 enrollees treated at one of its locations that their PHI may have been inadvertently mailed to other patients.[3]

[1] Theodore J. Kobus, "BakerHostetler's 5th Annual Data Security Incident Response Report Highlights Collision of Privacy, Cybersecurity and Compliance; Details Efforts to Minimize Risk," BakerHostetler, 2019.

[2] Jim Kinney, "Baystate Health: Info of 12,000 Patients Compromised in Phishing Attack," MassLive, April 8 2019.

[3] Matthew Umstead, "VA Notifying Veterans Whose Personal Information Might Have Been Compromised," Herald, April 8, 2019.

Reported cyberattacks

Over the last few years, according to a research letter in the *Journal of American Medical Association (JAMA) Internal Medicine,* 1,138 breach cases reported to the Health and Human Services (HHS) Office for Civil Rights (OCR) occurred between 2009 and 2017, affecting the PHI of 164 million Americans.[4]

According to this research, phishing attacks were the leading cause of breaches, accounting for 37 percent across all industries. Network intrusions were closely behind at 30 percent, with unpatched servers and remote desktop connections providing easy points of entry for hackers.

[4] "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," U.S. Department of Health and Human Services: Office for Civil Rights, 2017-2019.

Once cybercriminals penetrate a system, their advances often follow a pattern: the attacker tries to gain access to the user's email account (34 percent), roam the network for available data (30 percent), install ransomware (12 percent), or try to obtain a wire transfer to the attacker's account (8 percent). A ransom was paid nearly one in ten times, with an average amount of nearly $29,000. Furthermore, ransomware attacks are on the rise in 2019, with a 195 percent increase of attacks on business targets in Q1 according to a Malwarebytes report.[5]

Attempts to mitigate responses have not been robust enough. On average, 36 days elapse between the time of the initial access and its detection. From there, it typically takes another 10 days to contain the breach.[6]

[5] Jessica Davis, "Ransomware Attacks on Business Targets Increase by 195 percent in Q1," HealthITSecurity, April 26, 2019.

[6] 2019 BakerHostetler Data Security Incident Response Report. Other source: Ponemon Cost of a Data Breach Study, Study of 477 companies, 2017-2018.

Patients' data is protected, however. HCOs must notify the OCR of breaches affecting 500 or more persons.[7] Further, data breaches pose the risk of hefty fines if Health Insurance Portability and Accountability Act of 1996 (HIPAA) patient privacy regulations are violated. In 2018, a cancer clinic in Texas was fined $4.3 million for three data breaches that compromised the PHI of more than 33,500 patients.[8] The OCR faulted the medical system's encryption policies for managing patient data. In the largest HIPAA fine to date, a major health insurer in 2018 paid $16 million to settle claims related to cyberattacks from three years prior that exposed the PHI of nearly 79 million members.[9] In a separate settlement, the affected organization agreed to provide four years of credit monitoring and other services for the impacted consumers.

According to a 2018 Healthcare Information and Management Systems Society (HIMSS) survey, three quarters of healthcare executives and cybersecurity professionals experienced a "recent and significant security incident."[10] According to this survey, the top three attack sources were phishers, negligent insiders, and hackers.

Keeping up with organizational security and compliance is a collective responsibility that sits not only with your IT department but also with the clinicians and medical staff.

To enlist clinicians as stakeholders in the security and compliance journey, you need a solution that's easy to follow as they go about their daily duties.

The threats and key points of vulnerability

One of the top threats to cybersecurity is phishing, and the key points of vulnerability are care coordination, care planning, case management, patient preferences, and data retention and discovery.

[7] HHS Breach Notification Rule, U.S. Department of Health and Human Services.

[8] "Judge Rules in Favor of OCR and Requires a Texas Cancer Center to Pay $4.3 Million in Penalties for HIPAA Violations," U.S. Department of Health and Human Services, June 18, 2018.

[9] "Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History," U.S. Department of Health and Human Services, October 15, 2018.

[10] "2018 HIMSS Cybersecurity Survey," Healthcare Information and Management Systems Society, December 14, 2018.

Phishing

Phishing is the fraudulent practice of sending emails that appear to be from a reputable source to trick individuals into revealing information, including personally identifiable information such as social security numbers. A recent study from *JAMA Network Open* states that the healthcare industry is extremely susceptible to phishing attacks.[11] This report, conducted by a group of physicians, studied the email security practices of six major medical institutions and found that about one in every seven phishing emails ended up being opened by a hospital employee.

According to The Radicati Group, Inc.'s report, 91 percent of cybercrime starts with an email.[12]

HCOs need a workforce equipped to defend against these attacks. A rigorous training and certification program is part of the solution. Of course, everyone is busy, either caring for patients, managing the organization, or other critical tasks. They need to be protected by technologies that apply policies and protections proactively behind the scenes while clinicians focus on the work of delivering the best care they can.

[11] William J. Gordon et al., "Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institution," JAMA Network Open, American Medical Association, March 8, 2019.

[12] "Email Statistics Report, 2018-2022," The Radicati Group, Inc., March 2018. March 2018.

Care coordination

HCO's need to coordinate patient care across a broad care continuum.

Consider the following example: a hospital is preparing to discharge a patient who needs ongoing, facility-based care. The inpatient facility needs to identify a rehabilitation facility to accept the patient. Prospective facilities would need PHI about the patient in order to determine whether they can provide effective care.

The risk exposure increases as the PHI travels to additional facilities for continuum of care. Organizations that transfer and receive patient data need security and data governance solutions that effectively secure communication with the right parties to minimize data breach risks.

Care planning

A provider wants to ensure that their patients have a comprehensive care plan after they've been discharged from the hospital. The provider hires a care planning company as a business associate to develop individualized care plans for these patients.

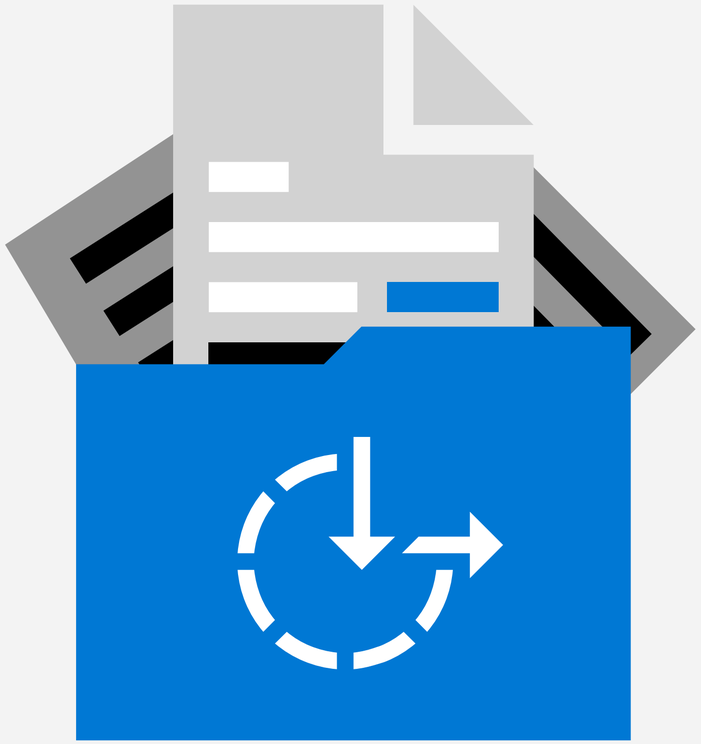
To develop the plan, the care planning company requests pertinent PHI about each patient from their various providers, including hospitals to which they may have been admitted for this or a related condition. Each of these covered entities may disclose the relevant PHI for care planning purposes if consistent with HIPAA and other applicable regulations.

HCOs need technologies that protect PHI in this use case as well.

Case management

Case management is another use case that requires HCOs to control and protect their data—especially as it travels across entities—consistently with the law as well as the trust that patients place in them.

In this example, a health planner hires a healthcare management company to provide semi-monthly nutrition advice and coaching to their diabetic and pre-diabetic members. The care management company, as a business associate of the insurer, must provide appropriate, individualized guidance and ensure that the advice is coordinated with the treatment of each patient's other providers.



Patient preferences about communication and related concerns

According to Aetna's 2018 inaugural Health Ambitions Study, patients want more digital engagement with their caregivers.[13] Among younger consumers ages 18 to 34, 37 percent say digital messaging would be valuable. Among a senior population, 32 percent indicate they want digital messaging. While younger patients prefer digital communications, seniors also want to engage with their caregivers as digital tools become simpler and more prevalent.

Perhaps most surprising in the Aetna Health Ambitions Study is that patient privacy and data security was recognized as the top-ranked concern among consumers about their healthcare—more important than the cost of care.

Data retention and discovery

Some organizations still rely on manual policies and procedures to protect sensitive content and prepare for internal audits, external litigation, regulatory data requests, and data discovery. Whether in a digital or paper format, these policies and procedures too often are irregularly enforced and subject to staff turnover, and occasionally conflicting management objectives and direction. This leads many organizations to keep everything, limiting their ability to quickly find data when they need it and determine whether sensitive information has been, or is being compromised.

[13] "Health Ambitions Study: Research Summary and Data," The Health Section, June 18, 2018.

3

A holistic approach

A reliable system to protect PHI is a business necessity, not a luxury

Current processes have proven insufficient for managing the real-world risks of mass patient record breaches and significant compliance failures. HCOs now must strategically spend funds on efficient, robust, and reliable tool-based process enforcement rather than on the sum of technological remediation, reputational repair, and financial penalties.

A comprehensive approach to data governance, security, and compliance is required to help prevent incidents that could disrupt your patient care and processes. This approach can also support compliance and the documentation needed to demonstrate compliance.

How can you best address these challenges?

Meeting healthcare regulatory requirements and compliance

Microsoft 365 services help you effectively balance meeting regulatory mandates by securing your infrastructure and PHI. By assessing your compliance posture in real time with actionable insights you can improve data protection capabilities and stay current with complex compliance obligations.

Controlling and protecting confidential health and personal data

As PHI data travels from one entity to another, vulnerabilities increase. But you can improve the security and compliance posture of that data in transit without encumbering the clinicians with burdensome bureaucracy or additional steps that add clutter to their experience with fragmented tools and processes. With a comprehensive, integrated, and agile platform, you can protect, govern, and control access to sensitive data.

Adhering to organizational governance policies

Streamlined processes and audit-ready tools let you track data with transparency and accountability. Achieve controlled data flow across the care continuum.

4

Microsoft 365 is uniquely positioned to help with health regulations

Microsoft 365 unifies Windows 10, Office 365, and Enterprise Mobility + Security

This integration helps secure and manage your environment, including supporting compliance.

You can specify that data be kept local within a jurisdiction, complying with regulations and data protection laws that concern data sovereignty and trans-border data flow. Microsoft 365 offers integrated, intelligent tools to provide you better access and help reduce risks. It allows you to govern and protect sensitive and business-critical data while responding to regulatory requests with intelligence and efficiency.

Through enterprise-grade security capabilities, Microsoft 365 empowers you to assess and manage compliance risk, protect personal data, and streamline processes.

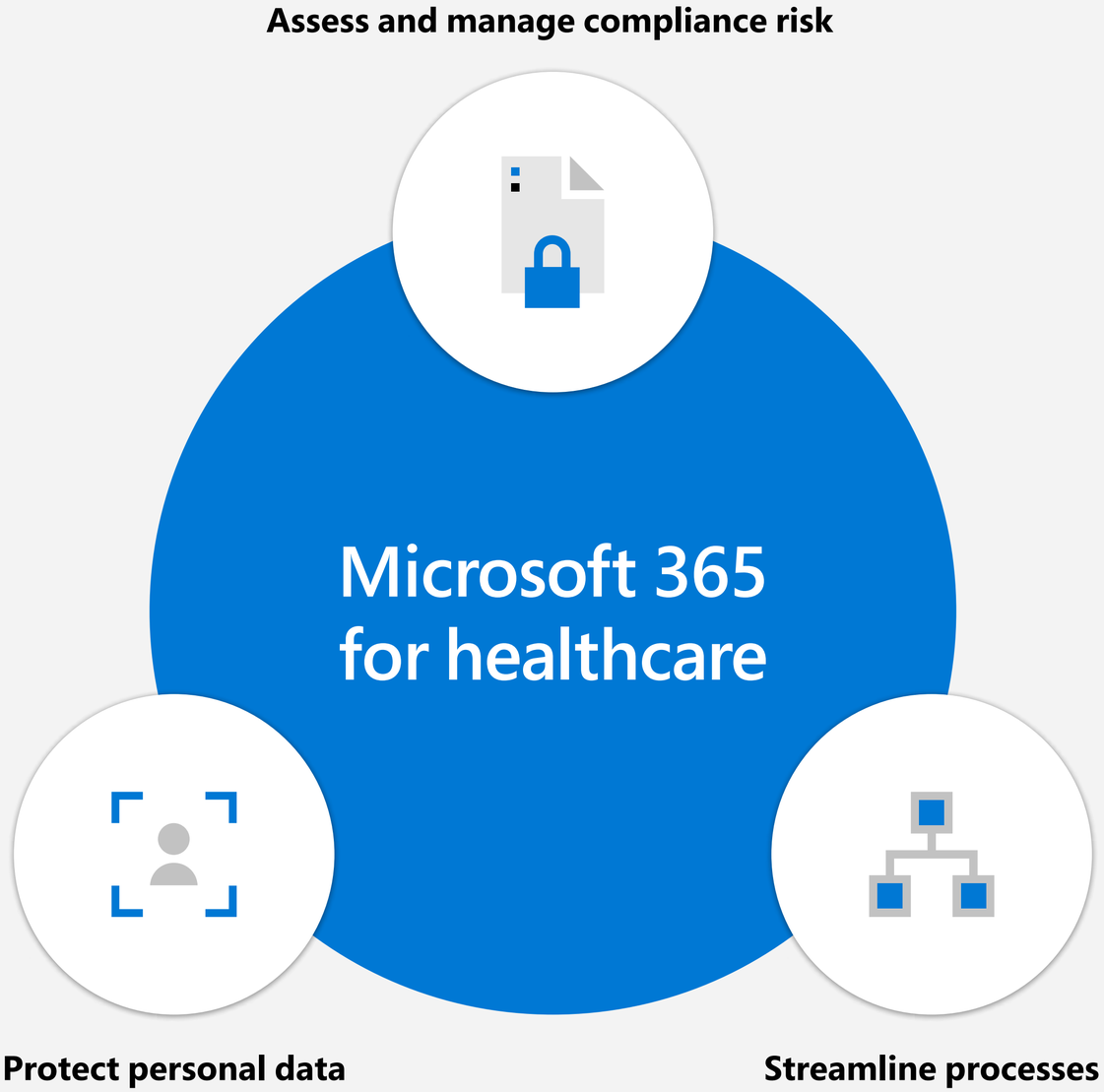


Figure 1: Microsoft 365 provides three critical services for healthcare

Assess and manage compliance risk

Good compliance begins with proper data classification and labeling. That becomes the building block against which your IT team applies governance to manage the data according to its sensitivity. This makes it a more manageable task for your IT department and reduces errors and exposure. Protecting, retaining, or reporting on sensitive data follows more seamlessly when you start with good classification. This also adds agility and accuracy as you respond to audits or your team needs to make data available to regulators. Microsoft 365 provides intelligent tools for data classification and labeling, assigning policies, and managing data subject requests. Furthermore, Microsoft 365 provides ongoing assessment of your compliance posture—including actionable insights to help your organization stay current.

Microsoft 365 helps you assess and manage compliance risk in several ways.

Ongoing risk assessment to demonstrate compliance posture

To help ensure that health records and patient data remain safe and compliant, even in new, complex coordination of care scenarios, you need to continuously assess how your HCO complies with rapidly changing regulatory requirements. When you move your patients' data to a cloud service, it becomes a shared responsibility between your organization and the cloud service provider to protect data and meet compliance obligations.

Performing comprehensive, prioritized risk assessments spanning common workflow scenarios with awareness of organization-specific and common vulnerabilities is crucial to gaining an understanding about the effectiveness of security, compliance, and privacy controls managed by your organization and cloud provider.

Included with Microsoft 365, Compliance Manager provides an intelligent score that reflects your performance against data protection regulatory requirements. Compliance Manager recommends actions to strengthen your data protection capabilities. It also provides built-in collaboration tools to streamline workflows across teams and richly detailed reports of pertinent data for auditing and management purposes.

Microsoft Cloud App Security is a cloud access security broker solution that helps detect use of native and third-party cloud applications. It helps discover cloud apps that are accessed by users, evaluates their risk level, and allows you to manage access based on organizational requirements. Microsoft Cloud App Security can help identify cloud apps for your organization that comply with regulations relevant to you, such as HIPAA, to help meet your compliance goals. More than 16,000 cloud apps have been assessed against more than 75 risk factors, including compliance and industry regulations, which will allow you to govern access accordingly.

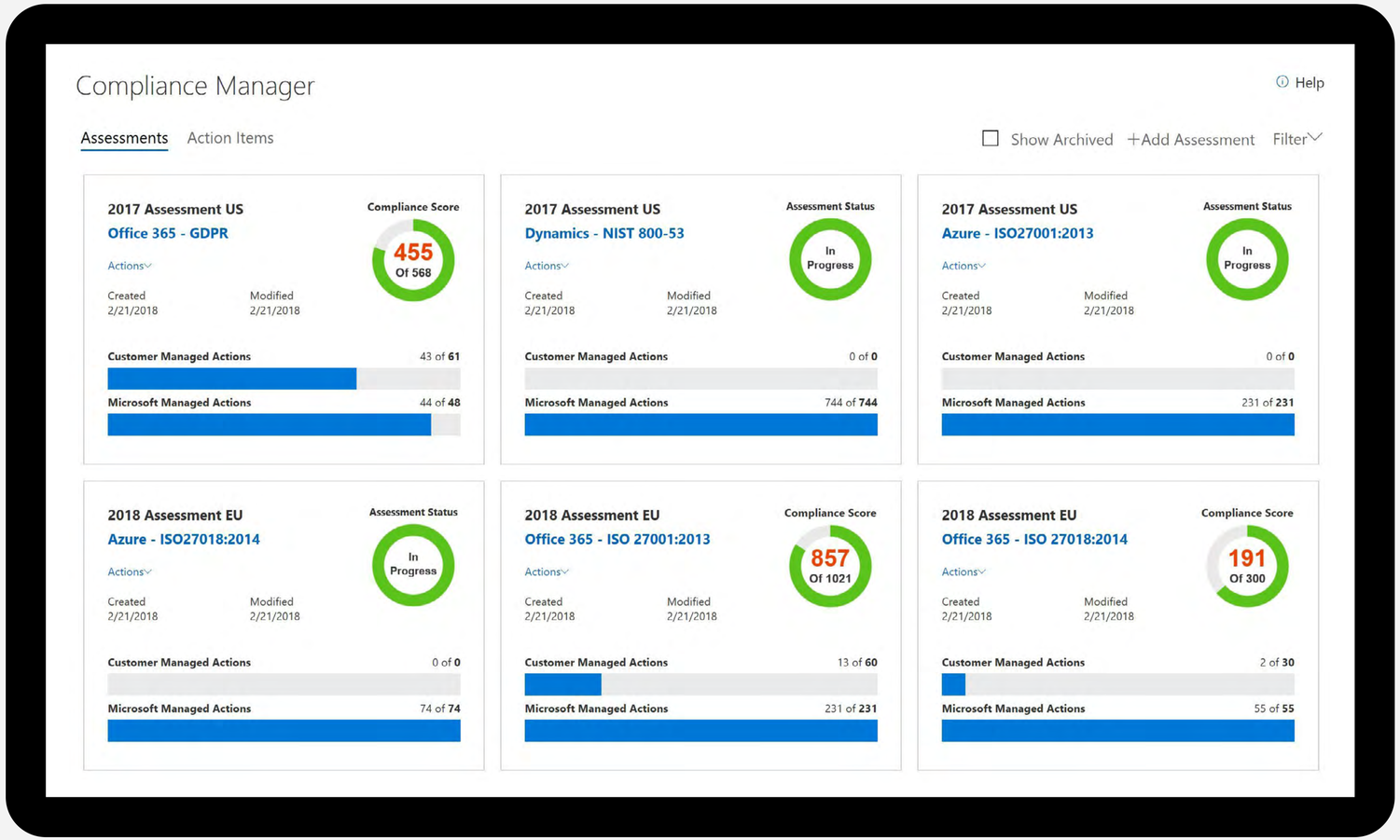


Figure 2: Compliance Manager dashboard with compliance score

Visibility into security posture

With Microsoft Secure Score in the Microsoft 365 security center, you get increased visibility and control over your organization's security posture.

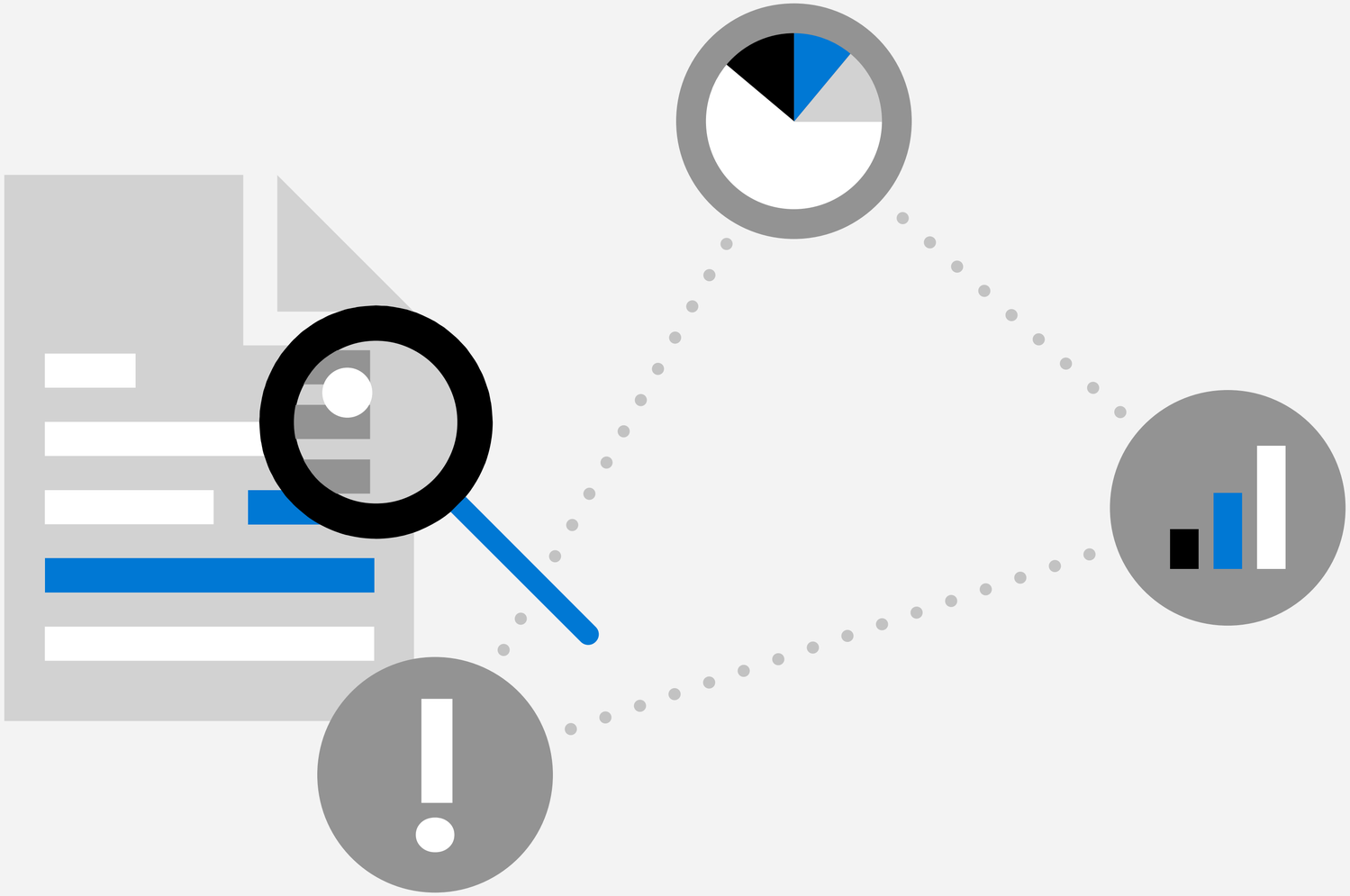
A centralized, real-time dashboard helps you monitor the protection state of care teams, health records, apps, devices, and infrastructure. It delivers a numerical summary of your organizational security posture based on system configuration, user behavior, and other security-related measurements. To improve the score, this dashboard recommends prioritized improvement actions such as enabling multi-factor authentication, turning on auditing, designating less than five global administrators, and much more.

Note: Secure Score is not an absolute measure of how likely you are to experience a breach. Rather, it indicates the extent to which you have adopted controls that can offset the risk of being breached. No service can guarantee that an organization will not be breached. Secure Score shouldn't be interpreted as a guarantee.

Advanced compliance-related tools and resources for best practices

HCOs can use the Microsoft Security and Compliance Blueprint for HIPAA/HITRUST health data and artificial intelligence (AI) to help meet industry compliance requirements. With this blueprint, you have at your fingertips healthcare architectures, deployment guides, control implementation mappings, customer responsibility matrices, threat models, and automations based on industry requirements and regulations.

Microsoft has built the Service Trust Portal (STP) as a public site for publishing audit reports and other compliance-related information related to Microsoft's cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored white papers that provide details on how Microsoft builds and operates our cloud services.



CENTRA

What customers are saying

"Centra boosts quality care compliance scores 24 percent with Microsoft 365 BI tools: in the nine months since we introduced the Power BI dashboard, our overall compliance score increased from 34 to 58 percent. This represents thousands of new touches of improved care provided to our patients."[14]

—Dr. Matthew Johnson
Chief Population Health Officer
Centra Health

[14] "Centra Boosts Quality Care Compliance Scores By 24 Percent With Microsoft 365 Business Intelligence Tools," Microsoft Customer Stories, August 2018.

Protect personal data from internal and external attacks

Clinicians, physicians, and other health workers need to access data from multiple devices, locations, and shared workstations. It's critical to provide timely, convenient, secure access to necessary patient data from virtually anywhere, on various devices, while helping protect against even the most sophisticated attacks.

To help prevent the breach of sensitive health records, patient data, and personal identities, Microsoft 365 provides built-in intelligent capabilities that work together.

Identity and access management

Caregivers, administrators, and staff need to access data from multiple devices, locations, and shared workstations. Today, rather than computer and network infrastructure, end-user identity is the new security perimeter to control who has access to sensitive data; it can help verify that users are authorized before they gain access to apps and data.

Azure Active Directory (Azure AD), Microsoft's identity and access management solution, is designed to help organizations like yours manage users and access privileges to specific systems, patients, and data sets. With Azure AD, you can set policies based on the user, location, device, and app to determine whether the user should be allowed, limited, or blocked from accessing resources.

Azure AD features

Azure Multi-Factor Authentication: two-step verification to safeguard access to data and apps.

Passwordless authentication: Multi-Factor Authentication to allow a user to sign in with a password alternative. The credential is tied to a device that uses biometric authentication (such as facial recognition or fingerprint), non-field communication, or personal identification numbers.

Password protection: a safeguard against using common, compromised passwords through banned password lists and smart lockout features.

Conditional access: manage access to apps based on status and risk level for the user, device, location, or app and apply the appropriate policies and controls.

Identity protection: calculate the risk level of users and sign-in attempts based on behavior and threat signals, analyze security logs, and get alerts on risk events.

Privileged identity management: minimize the attack surface by limiting access for privileged roles to critical operations and monitoring administrator access rights.

Prove users are authorized and secure before granting access to apps, data, and devices.

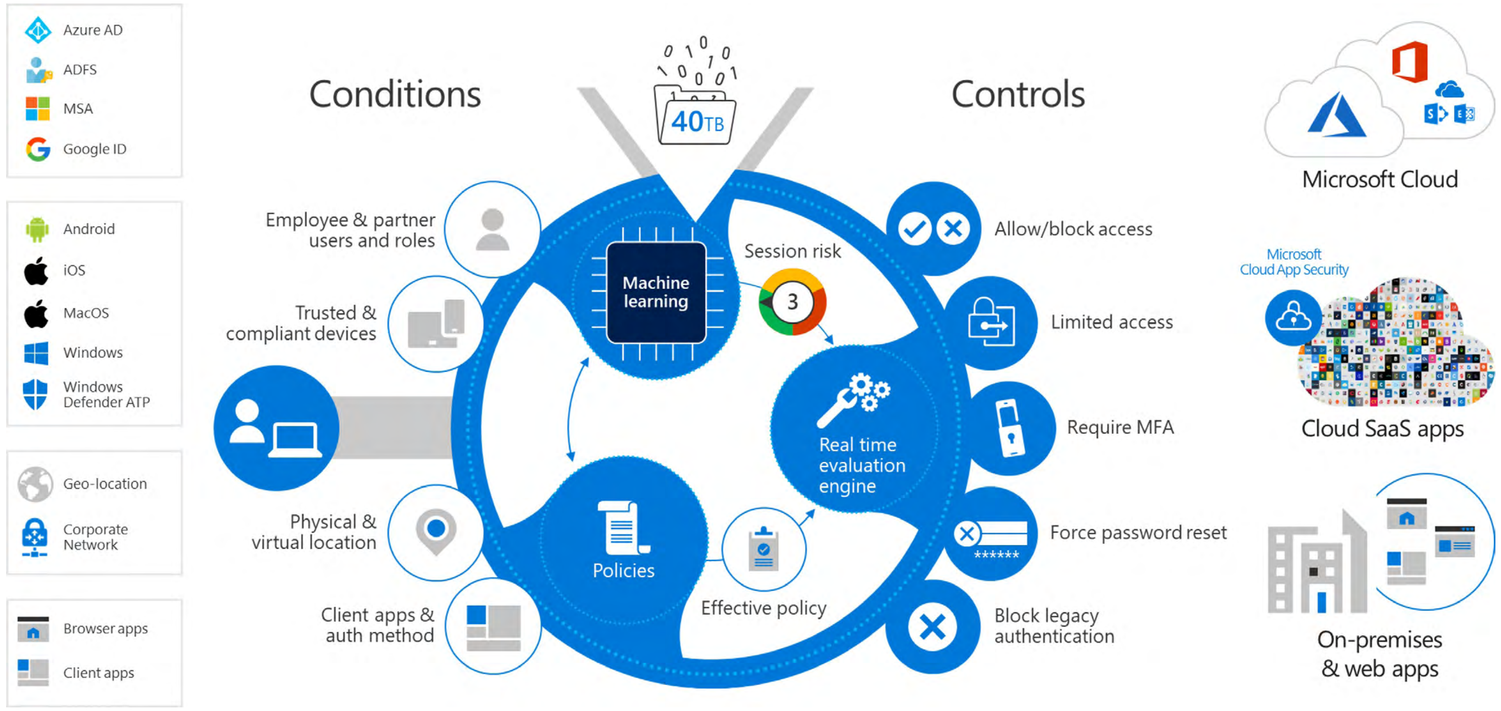


Figure 3: Azure AD features work together to secure and centralize your data.

Advanced Threat Protection

Security breaches and ransomware are a major concern for any HCO, as they can result in stolen patient records and reputational damage. Cybercriminals relentlessly target HCOs, seeking medical, behavioral health, and genetic data of high-net-worth individuals, politicians, celebrities, and the general population. It's ever more vital to keep patient information and other sensitive data secured.

With Microsoft 365, you can implement a comprehensive solution to protect care teams by helping them secure identities, emails, apps, data, and devices. You can apply analytics and intelligence to prevent threats like phishing and zero-day attacks.

Microsoft 365 solutions

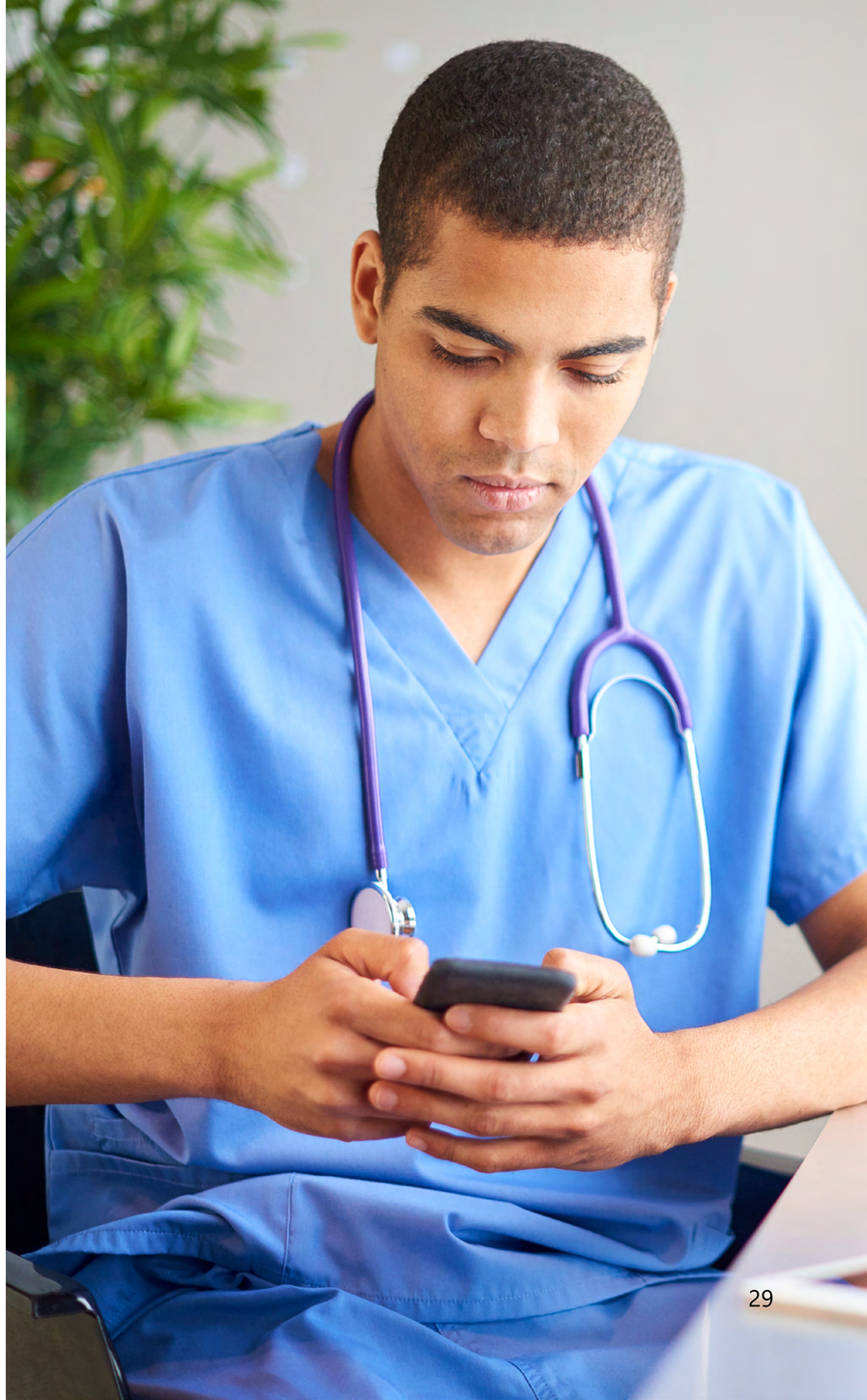
Office 365 Advanced Threat Protection: safeguard your organization against malicious threats posed by email messages, links, and collaboration tools. Additionally, Advanced Threat Protection anti-phishing protection can help protect your organization from malicious impersonation-based phishing and other attacks.

Microsoft Cloud App Security: detect unusual behavior across Microsoft and third-party cloud apps to identify ransomware, compromised users, or rogue apps; analyze high-risk usage; and remediate automatically to limit the risk to your organization.

Azure Advanced Threat Protection: detect, identify, and investigate advanced threats, compromised identities, and malicious insider actions.

Azure AD Identity Protection: configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached.

Microsoft Defender Advanced Threat Protection: built-in, cloud-powered technology includes preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender ATP protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture.



Data encrypted at rest and in transit

Microsoft products and services use industry-standard encryption to protect critical health data, whether it's being accessed by care staff or stored at rest. Microsoft uses some of the strongest, most secure encryption methods, protocols, and algorithms across its products and services to help provide a secure path for data to travel through the infrastructure.

Microsoft 365 managed encryption: Microsoft uses multiple encryption methods, protocols, and ciphers to help provide a secure path for health and patient data to travel across Microsoft 365 services—and to help protect the confidentiality of health records stored within Microsoft 365 services. Service-side technologies encrypt data at rest and in transit. In Microsoft 365, service-side encryption is used by default, so you don't have to configure anything.

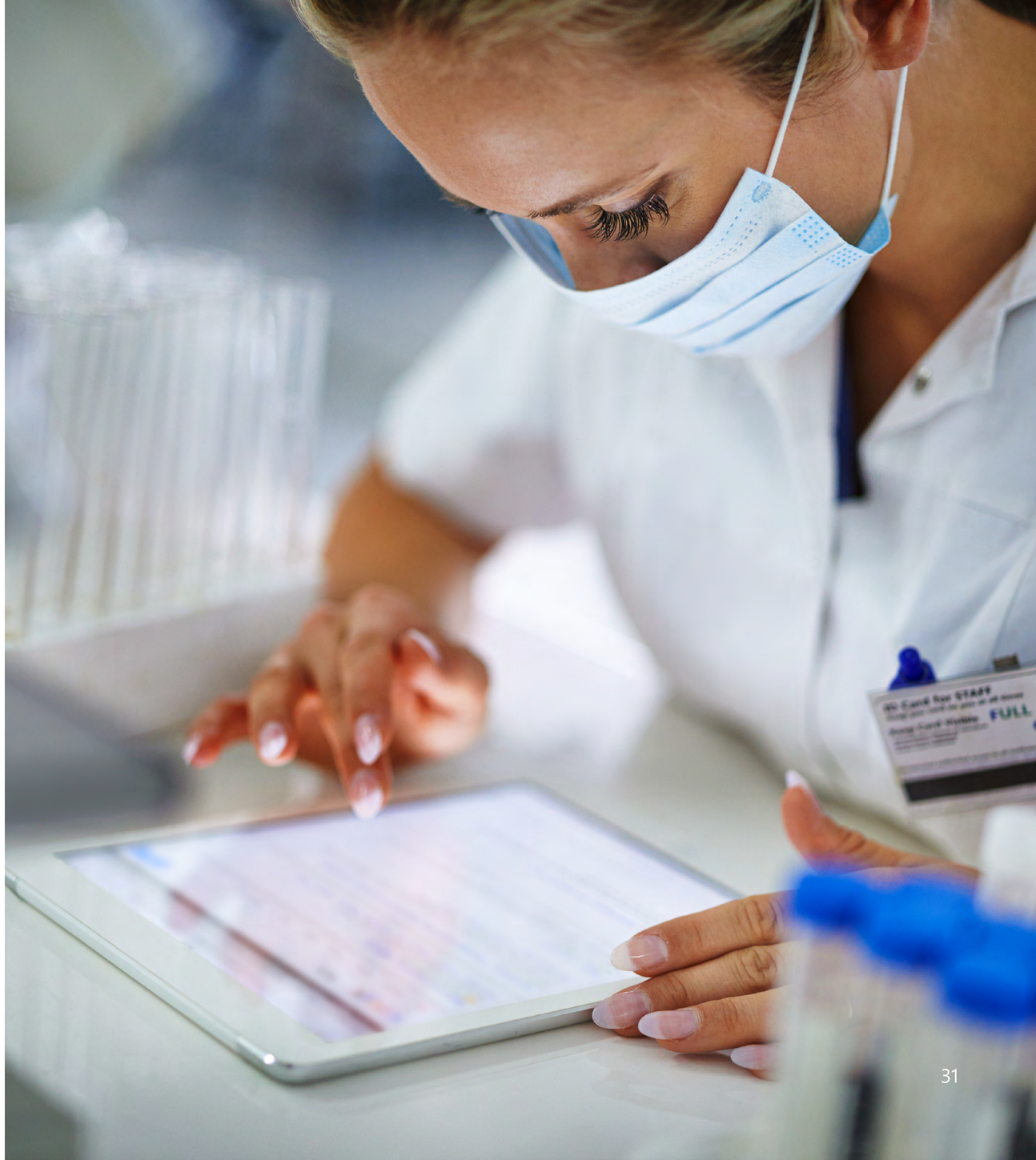
Customer-managed encryption: by adding content-level encryption, you can protect data to help ensure that only authorized health workers can view the protected content. To further mitigate data loss and leakage, you can apply both rights protection and encryption for emails and files in SharePoint Online.

Sutter Health
We Plus You

What customers are saying

"Exchange Online has revitalized our unified email service across Sutter Health. With Office 365 Advanced Threat Protection, the built-in security features are scalable and enable our organization to increase our cyber defense and data protection needs, as well as eliminate the need for network drives."[15]

—Wes Wright
Corporate CTO
Sutter Health



[15] "Sutter Health moves to Office 365 to help strengthen patient care," Microsoft Customer Stories, November 2017.

Streamline data governance processes

A fundamental requirement of complying with data security regulations like HIPAA and HITRUST is the ability to quickly, easily, and accurately identify and classify sensitive data. Rather than relying on manual data classification, AI-based solutions can efficiently recognize patient identifiable content and various types of PHI. Microsoft information protection solutions across Office 365 and Azure provide an integrated classification, labeling, and protection experience. This in turn helps enable persistent governance and protection of your sensitive data across devices, apps, cloud services, and on-premises environments.

Microsoft 365 can help identify sensitive information and define security and controls with integrated e-discovery, classification, labeling, and policy-based protection capabilities, including:

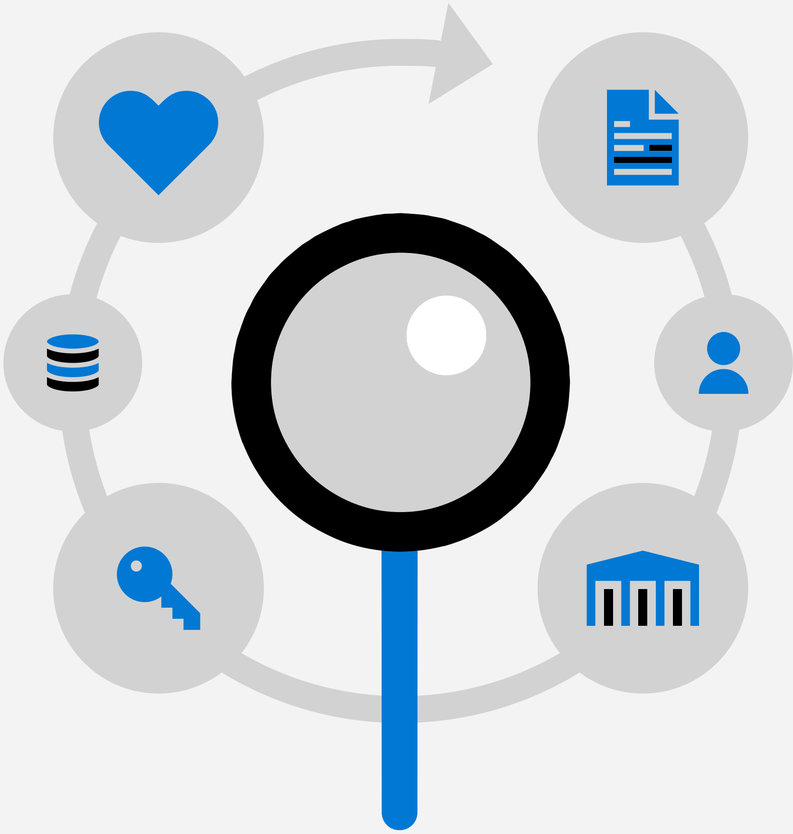
Actionable intelligence with advanced e-discovery

Legal and commercial disputes such as patient complaints, reimbursement, regulatory actions, and malpractice suits require the ability to retain and search relevant health and patient data. The Microsoft 365 E-Discovery and Data Subject Requests capability allows HCOs to quickly access information and reports, and comply with discovery or other data and documentation requests. You can find data across Exchange Online, SharePoint Online, OneDrive for Business (including Teams and Groups), and public folders.

Data classification based on automatic analysis

Automatically classify, protect, and govern sensitive health data. Data classification and protection controls are integrated into Microsoft Office and other common apps, with one-click options that make it easy to label and classify data. Use over 80 predefined sensitive data types or create your own classification and labeling templates to help ensure information protection remains persistent and travels with the data.

There are a range of protection actions you can apply to your sensitive data, and you can define policies to apply varying levels of protection to data based on its sensitivity. Both Azure and Office 365 have data encryption built into the service—for both data at rest and data in transit. You can adopt a multi-layered strategy to protect sensitive data. To protect individual files, for instance, you can apply rights-based permissions so that only intended recipients can access and view the information; enable policy tips that notify users of sensitive information in documents; automatically apply visual marking; and automatically retain, expire, or delete documents based on data governance policies defined by your organization.



This means your data is always identifiable and protected—regardless of where it's stored or with whom it's shared. Microsoft tools and services support information protection and governance, including Advanced Data Governance, Azure Information Protection Premium, Azure AD, and encryption capabilities such as BitLocker, dm-crypt, and Azure Key Vaults.

Automatic classification: classify data based on automatic analysis (such as age, user, type, sensitive data, and user-provided fingerprints).

Intelligent policies: use recommendations based on machine learning and cloud intelligence.

Data preservation: store sensitive data related to any legal matter, or commercial or regulatory dispute, by using In-Place Hold and Litigation Hold.

Data loss prevention

To comply with business standards, industry regulations, and consumer expectations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Data loss prevention (DLP) is a compliance feature of Microsoft 365 that is designed to help you prevent the intentional or accidental exposure of sensitive information—including financial data or PHI such as date of birth, social security numbers, member numbers, diagnoses, tests, documentation, or other health records—to unwanted parties outside your organization.

Sensitive information monitoring

To ensure critical data is in safe hands, HCOs are required to monitor data access, sharing, and usage—and respond quickly to potential abuse or threats. Microsoft 365 can help through increased insight into how care staff are using or distributing health records and patient data.

Rich logs and reporting tools are available to support IT monitoring and analyzing data for compliance and regulatory purposes. You can track activity on shared files, and, if needed, revoke or modify access to shared data. To ensure a timely response, access to data can be revoked either by end users on their own documents or by an administrator on behalf of any user.

Provide transparency by controlling how customer data is accessed

Customer Lockbox can help support compliance needs by demonstrating that you have procedures in place for explicit data access authorization. Customer Lockbox gives you explicit control in the very rare instances when a Microsoft engineer may need access to your content to resolve the issue. It enforces access control through multiple levels of approval within Microsoft, providing just-in-time access with limited and time-bound authorization. Customer Lockbox can help customers meet controls in regulations such as in FEDRAMP.

MJHS

What customers are saying

"We were more than satisfied that Microsoft 365 met our strict standards around security and compliance, in everything from email retention to archiving and e-discovery. We also use Microsoft 365 Advanced Threat Protection which bolsters our defenses against malware and phishing emails."[16]

—Stuare Geller
Vice President of Information Services
MJHS Health System

[16] "MJHS celebrates nearly 110 years of care and innovation with modern Office 365 workplace," Microsoft Customer Stories, December 2016.

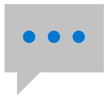
5

Partnering with Microsoft on data security, privacy, and compliance

Microsoft has created new tools and capabilities to help you:

Assess: Microsoft 365 provides tools that allow you to assess and manage compliance from a single location, which supports both a simplification of the compliance process and deeper understanding through actionable insights.

Protect and govern: using information protection and governance solutions, you can automatically protect and govern sensitive data across devices, apps, and cloud services as well as control access to your sensitive data.



Respond: to efficiently respond to regulatory, litigation, and investigation data discovery requests, you can use built-in AI capabilities to find the most relevant data with corresponding audit logging.

Experience more

Learn about Microsoft 365 for health ›

See where your data is located ›

Contact us ›