

AI in Healthcare: A Case Study in Responsible Workflow Modernization

How healthcare organizations can use AI to reduce administrative burden while protecting ePHI, improving governance, and preserving patient trust

Executive takeaway

AI can help healthcare organizations summarize meetings, draft administrative documents, support referral follow-up, improve patient communication workflows, analyze revenue-cycle trends, and improve operational reporting. But healthcare AI must be implemented with strong ePHI controls, HIPAA-aligned governance, vendor and BAA review, Microsoft 365 permissions cleanup, human review, auditability, backup, cybersecurity, and downtime readiness. AdvancedBITS helps healthcare organizations make AI adoption practical, secure, and governed before expanding use across departments.

Healthcare organizations face a difficult balance. Teams are under pressure to reduce administrative burden, improve responsiveness, manage staffing constraints, support patients, and modernize workflows. At the same time, every improvement must respect privacy, security, compliance, clinical accountability, and patient trust.

AI is not automatically safe because a tool is popular or because a Business Associate Agreement (BAA) exists. The organization must still configure systems properly, govern data access, train users, monitor activity, validate outputs, and document how ePHI is protected. In Microsoft 365 environments, that means SharePoint, Teams, OneDrive, Outlook, sensitivity labels, data loss prevention (DLP), audit logs, identity, endpoint security, and backup all become part of AI readiness.

AdvancedBITS positions AI in healthcare as a responsible workflow modernization opportunity. AI should help teams work faster where appropriate, but it should not bypass human judgment, clinical responsibility, patient communication standards, or HIPAA-aligned safeguards.

Why healthcare AI governance cannot wait

Healthcare is adopting AI faster than it is governing it. Physician use has more than doubled in three years, while independent research shows many organizations still lack controls over the sensitive data those tools touch.

Table 1. Healthcare AI adoption and governance, by the numbers

Finding	Source
81% of physicians now use AI professionally, up from 38% in 2023. The average physician reports 2.3 use cases, up from 1.1.	American Medical Association, 2026 Physician Survey on Augmented Intelligence (March 2026; 1,692 physicians)

Finding	Source
Patient privacy was the only area where more physicians expect AI to cause harm than help (41% versus 13%).	AMA 2026 survey, as reported by Fierce Healthcare (March 2026)
About 17% of healthcare workers admit using unauthorized AI tools, and more than 40% are aware of colleagues doing so.	Wolters Kluwer Health survey of 500+ healthcare workers (December 2025; published January 2026)
60% of healthcare organizations lack controls governing sensitive data used in AI systems. Only 42% use security measures designed for AI, and just 32% have full visibility into unsanctioned AI use.	Proofpoint and Ponemon Institute, 2026 Cyber Insecurity in Healthcare (October 2026; 705 practitioners)
Across industries, 63% of organizations lacked AI governance policies, and shadow AI was involved in 20% of breaches, adding about \$670,000 to average breach cost.	IBM Cost of a Data Breach Report 2025
Healthcare breaches averaged \$7.42 million , the highest of any industry for the 14th consecutive year, and took 279 days to identify and contain.	IBM Cost of a Data Breach Report 2025, as reported by HIPAA Journal
Misuse of AI chatbots ranked #1 on ECRI's Top 10 Health Technology Hazards for 2026.	ECRI (January 2026)

Survey figures are self-reported. The IBM governance and shadow AI figures cover all industries in the study, not healthcare alone.

The AI healthcare reality check

Healthcare AI adoption often begins informally. A staff member asks an AI tool to summarize a policy. A manager uses AI to draft a patient outreach message. A billing team asks for help summarizing denial reasons. A leadership team wants Copilot to search across Microsoft 365. These use cases can create value, but they also introduce risk if the organization has not defined approved tools, data boundaries, and review requirements.

Table 2. Common healthcare AI challenges

Healthcare AI Challenge	What It Looks Like	Why It Matters
Informal AI use	Staff test public or unapproved AI tools for summaries, drafts, documentation, HR, billing, or patient communication.	ePHI, staff data, or sensitive operational information may enter systems without safeguards.
Microsoft 365 oversharing	SharePoint, Teams, OneDrive, and shared mailboxes contain broad permissions or old sharing links.	Copilot-style search may surface content users should not practically access.
Unclear human review	AI-generated patient messages, summaries, or reports are used without defined review ownership.	Accuracy, privacy, and accountability may break down.
Vendor uncertainty	AI, EHR, telehealth, RCM, portal, and SaaS vendors may process sensitive information.	BAA, retention, auditability, training use, and breach obligations must be understood.

Healthcare AI Challenge	What It Looks Like	Why It Matters
Workflow inconsistency	Departments document intake, referrals, outreach, policies, and billing differently.	AI may accelerate inconsistent processes instead of improving them.
Weak recovery posture	Microsoft 365, endpoint, EHR-related exports, and administrative content may not be recoverable quickly.	Ransomware, deletion, or account compromise can disrupt patient service and operations.

Case study: multi-location healthcare practice preparing for AI

Illustrative case study disclosure

This case study is a composite example designed to show how AdvancedBITS can support healthcare AI readiness. It does not describe a named client or disclose confidential client information. No performance results are claimed for the composite practice. All statistics in this document come from independent third-party research and are not AdvancedBITS client outcomes.

A multi-location healthcare practice wanted to use AI to improve administrative documentation, referral follow-up, patient communication drafts, policy search, revenue-cycle reporting, and leadership reporting. The organization used Microsoft 365, Teams, SharePoint, OneDrive, an EHR or practice-management platform, patient communication tools, billing support vendors, and several department-specific SaaS tools.

The executive team saw AI as a practical way to reduce administrative friction. Managers wanted faster meeting summaries and policy search. The outreach team wanted draft content for patient reminders and service-line messages. The billing team wanted to identify patterns in payer correspondence. However, the organization also knew that AI could create risk if ePHI, staff data, or billing details were entered into unapproved tools or surfaced through broad Microsoft 365 permissions.

Table 3. Challenges, actions, and outcomes in the composite practice

Challenge	AdvancedBITS Action	Healthcare Outcome
Unknown AI usage	Interviewed stakeholders and identified where staff were already using or considering AI.	The organization gained a clear baseline of AI exposure and priority use cases.
Microsoft 365 oversharing	Reviewed SharePoint, Teams, OneDrive, guest access, shared links, department sites, and sensitive content locations.	The organization reduced oversharing risk before enabling broader AI search or Copilot workflows.
ePHI handling uncertainty	Mapped workflows where ePHI, claims data, referral information, or patient communication could enter AI-assisted processes.	The organization defined approved, restricted, and prohibited AI data rules.

Challenge	AdvancedBITS Action	Healthcare Outcome
Vendor and BAA gaps	Reviewed AI, EHR-adjacent, telehealth, billing, patient communication, Microsoft 365, backup, and outsourced IT vendors.	Vendor risk became part of the operating model, including BAA, retention, access, and incident review.
Workflow inconsistency	Documented administrative, referral, outreach, billing, and reporting workflows.	AI pilots were focused on workflows mature enough for controlled adoption.
Recovery and resilience concerns	Reviewed Microsoft 365 backup, endpoint protection, MFA, Conditional Access, and incident response readiness.	Leadership received a practical roadmap for resilience before expanding AI adoption.

Where AI helped the healthcare team

In the case study, AI was a controlled workflow support tool. AI was not used to diagnose, treat, make clinical decisions, replace licensed clinical judgment, or send patient-facing communication without review. That boundary matters: ECRI ranks misuse of AI chatbots as the top health technology hazard of 2026 because the tools sound confident even when they are wrong.

Table 4. AI-assisted workflows and human review requirements

Workflow	AI-Assisted Benefit	Human Review Requirement
Administrative meetings	Generated first-pass summaries, action items, and follow-up lists from approved meeting materials.	Managers reviewed accuracy before distribution.
Policy and procedure search	Helped staff find operational procedures, templates, and internal guidance faster.	Content owners validated whether policies were current and applicable.
Referral follow-up	Summarized referral status notes and prepared task lists for staff review.	Referral team confirmed status and next action before patient or provider outreach.
Patient communication drafts	Prepared draft reminders, educational blurbs, and service-line outreach language.	Approved staff reviewed privacy, accuracy, tone, and appropriateness before use.
Revenue-cycle reporting	Summarized denial themes, payer correspondence, and recurring documentation issues.	Billing leadership validated against source records and approved procedures.
Executive reporting	Converted security, vendor, operations, and workflow readiness notes into leadership summaries.	Leadership and compliance owners reviewed findings before decisions.

The AdvancedBITS healthcare AI readiness model

Before healthcare organizations scale AI, they should confirm readiness across data governance, Microsoft 365, identity, vendors, workflows, human review, and resilience.

Table 5. Healthcare AI readiness model

Readiness Domain	Question to Ask	Risk if Ignored	Better Approach
ePHI and data classification	Do we know which workflows may include ePHI, claims data, patient communication, staff data, or sensitive operations data?	AI may process sensitive data without proper controls.	Define data classes, approved use cases, prohibited data, labels, and handling rules.
Microsoft 365 governance	Are SharePoint, Teams, OneDrive, Outlook, DLP, labels, and audit logs ready for AI search?	AI can surface overshared or unmanaged content.	Review access, site ownership, sensitivity labels, DLP, audit logging, retention, and backup.
Vendor and BAA oversight	Do AI and SaaS vendors have appropriate contracts, BAAs, security assurances, and retention terms?	Third-party risk may remain undocumented.	Review BAAs, retention, training use, audit logs, incident terms, and data location.
Human review	Who validates AI-assisted outputs before use?	Drafts may become final without accountability.	Define review owners for patient communication, billing, HR, policies, and reporting.
Workflow maturity	Are processes standardized enough for AI support?	AI may automate inconsistent or unclear workflows.	Map workflows, define owners, standardize inputs, and create escalation paths.
Cyber resilience	Can the organization recover from ransomware, account compromise, or accidental deletion?	AI adoption may depend on systems that are not recoverable.	Review MFA, Conditional Access, endpoint protection, Microsoft 365 backup, restore tests, and incident response.

Microsoft 365 and Copilot considerations

Microsoft 365 Copilot and similar AI tools are powerful because they work across the content a user can already access. That same strength makes permissions, labels, retention, and auditability central to healthcare AI readiness. Copilot respects existing permissions, which means it can also make forgotten, overly broad access much easier to discover.

The evidence suggests this is already happening. In ShareGate's 2026 research, **93%** of IT leaders were confident their Microsoft 365 governance could support AI responsibly, yet **29%** said Copilot or another AI tool had surfaced sensitive internal data that should not have been accessible. The findings are self-reported and the question covered AI tools generally, so they show a governance gap rather than a Copilot-specific failure rate.

Table 6. Microsoft 365 areas to review before AI expansion

Microsoft 365 Area	Healthcare Concern	AdvancedBITS Guidance
SharePoint sites	Department sites may contain ePHI, reports, policies, HR files, and operations documents.	Review site ownership, permissions, sensitivity, retention, and closure rules.

Microsoft 365 Area	Healthcare Concern	AdvancedBITS Guidance
Teams channels	Operational conversations, meeting recordings, and shared files may include sensitive content.	Review membership, guest access, transcripts, recordings, retention, and channel structure.
OneDrive	Users may store working files, exported reports, or draft patient communication outside structured repositories.	Review sharing links, external access, sensitive file locations, and migration to approved workspaces.
Sensitivity labels	ePHI and restricted business content need consistent handling.	Create labels for ePHI, confidential, internal, restricted, and public content where appropriate.
DLP and audit logs	Patient data movement and AI interaction evidence may need review.	Enable DLP policies, audit logging, and review cadence for high-risk workflows.
Backup and recovery	Retention is not the same as recoverability.	Align Microsoft 365 backup, restore testing, and incident response with healthcare-critical content.

A BAA is necessary but not sufficient. Microsoft states that it offers a BAA to covered entity and business associate customers, available by default through its Data Protection Addendum, and that the agreement covers in-scope services. Confirm that each specific AI feature your staff use appears on Microsoft's in-scope list, and remember that the agreement does not configure your tenant, clean up permissions, or train your workforce.

Vendor security and BAA review questions

Healthcare AI vendor review should not stop at whether a vendor is willing to sign a BAA. Organizations should understand how prompts, files, outputs, metadata, logs, transcripts, summaries, and retained content are protected and governed. The scale of third-party exposure is real: the largest healthcare breach of 2025, at Conduent Business Services, involved a business associate and affected 62,224,658 individuals.

Table 7. Vendor review questions

Vendor Review Topic	Question to Ask	Why It Matters
BAA status	Does the vendor create, receive, maintain, or transmit PHI on the organization's behalf?	BAA coverage depends on function, data, and relationship.
Data retention	How long are prompts, uploads, summaries, logs, and outputs retained?	Retained AI artifacts may contain ePHI or sensitive information.
Training use	Will healthcare data be used to train or improve models?	Patient privacy and contractual controls require clarity.
Audit logs	Can the organization review user activity, uploads, exports, and AI interactions?	Auditability supports compliance, investigations, and accountability.
Access controls	Can access be limited by role, department, location, or workflow?	Minimum-necessary access is central to healthcare operations.

Vendor Review Topic	Question to Ask	Why It Matters
Incident commitments	How quickly will the vendor notify the organization after a security incident?	Incident response and breach assessment depend on timely notification.

Why recoverability belongs in an AI plan

AI workflows depend on systems that must stay available. In the Proofpoint and Ponemon research, 97% of healthcare organizations experienced at least one cyberattack in the past 12 months, and 74% of those experiencing the attack types studied reported disruption to patient care. Disruption to normal operations was the largest single cost category, averaging \$1.39 million. ECRI's 2026 hazard list also ranks unpreparedness for a "digital darkness" event, a loss of access to systems and data, second only to AI chatbot misuse. For that reason, the plan below tests restores and downtime procedures before AI use expands.

A practical 90-day healthcare AI readiness plan

Healthcare organizations do not need to solve every AI question at once. A focused 90-day plan can establish governance, identify risk, and test controlled workflows before broad adoption.

Table 8. 90-day roadmap

Timeframe	Priority	Outcome
Days 1 to 30	Inventory AI tools, Microsoft 365 permissions, SharePoint sites, Teams channels, OneDrive sharing, vendors, BAAs, and high-risk healthcare workflows.	Leadership gains visibility into current AI exposure and data risk.
Days 31 to 60	Define AI acceptable use, ePHI handling rules, sensitivity labels, DLP priorities, human review requirements, vendor review criteria, and pilot workflow standards.	The organization creates practical governance for responsible AI adoption.
Days 61 to 90	Pilot controlled AI workflows for administrative summaries, policy search, referral tracking, patient communication drafting, revenue-cycle insights, and executive reporting. Test a Microsoft 365 restore.	The organization tests AI value with human review and measurable productivity indicators.

Measure the pilot so leadership can decide with evidence. Useful indicators include:

- Minutes saved per task compared with the manual baseline
- Share of AI drafts changed or rejected during human review
- Number of unapproved AI tools detected and retired or approved
- DLP policy matches and audit-log findings in AI-assisted workflows
- Time to restore a sample of Microsoft 365 content during a test

The regulatory direction

HIPAA is moving toward more specific, mandatory safeguards. HHS's Office for Civil Rights proposed a Security Rule update on December 27, 2024, published in the Federal Register on January 6, 2025. The proposal would make all implementation specifications required with limited exceptions, require written documentation, and require a technology asset inventory and a network map showing how ePHI moves through systems. Industry summaries also describe required MFA and encryption. As of October 2026 no final rule has been published, and HHS's regulatory agenda projects final action in July 2027. Organizations that map ePHI flows and tighten access now are preparing for AI and for the likely direction of the rule.

Questions healthcare leaders should ask

- Which AI tools are already being used by clinical, administrative, billing, HR, outreach, and leadership teams?
- Which workflows may include ePHI, claims data, staff records, patient communication, or sensitive operations data?
- Are Microsoft 365 permissions ready for AI-powered search or Copilot?
- Do AI and SaaS vendors have appropriate BAAs, retention terms, audit logs, and incident commitments?
- Are SharePoint, Teams, OneDrive, DLP, sensitivity labels, and audit logs configured for healthcare AI use?
- Who must review AI-assisted workflows before output becomes patient-facing, billing-related, HR-related, or executive-facing?
- Can the organization restore Microsoft 365 content after ransomware, accidental deletion, or account compromise?
- Which workflows are mature enough for AI, and which need cleanup first?
- What training do staff need before AI use expands?
- What role should AdvancedBITS play in building the technology foundation?

Where AdvancedBITS fits

AdvancedBITS brings more than 11 years of managed services experience to healthcare organizations building a secure, governed foundation for responsible AI adoption. We do not replace clinical judgment, compliance leadership, or patient-care accountability. We strengthen the technology environment around healthcare operations so teams can use AI more safely and effectively.

Table 9. How AdvancedBITS supports healthcare AI

AdvancedBITS Capability	How It Supports Healthcare AI	Result for the Organization
Microsoft 365 governance	Reviews SharePoint, Teams, OneDrive, Outlook, permissions, sensitivity labels, DLP, retention, audit logs, backup, and Copilot readiness.	The organization reduces oversharing and creates a safer AI search foundation.
AI readiness assessment	Reviews approved tools, ePHI restrictions, use cases, workflow maturity, human review, and adoption plan.	AI adoption becomes governed, practical, and aligned with healthcare obligations.
Vendor and BAA review support	Assesses AI, EHR-adjacent, telehealth, billing, patient portal, Microsoft 365, backup, and outsourced providers.	Third-party risk becomes visible before sensitive data is exposed.
Cybersecurity and identity	Strengthens MFA, Conditional Access, endpoint protection, email security, monitoring, and account recovery.	The organization reduces account compromise and ePHI exposure risk.
Backup and resilience	Reviews Microsoft 365 backup, restore testing, continuity, and incident response readiness.	The organization is better prepared to recover after disruption.
Workflow modernization	Maps referral, intake, billing, administrative, outreach, policy, and reporting workflows for AI readiness.	Teams identify practical automation opportunities without sacrificing accountability.

Closing perspective

AI can help healthcare organizations reduce administrative burden and improve workflow visibility, but only when the technology foundation is ready. Healthcare AI adoption should begin with governance, access control, vendor review, human review, and recoverability, not with uncontrolled experimentation.

AdvancedBITS helps healthcare organizations create that foundation. By aligning Microsoft 365 governance, SharePoint structure, ePHI handling, vendor and BAA oversight, cybersecurity, backup, AI policy, and workflow modernization, healthcare organizations can move from cautious experimentation to responsible adoption with greater confidence. For the security and managed IT side of the same journey, see our companion Healthcare Practice Case Study.

Frequently asked questions

Is it safe for healthcare staff to use AI tools with patient information?

Only approved tools with a BAA, proper configuration, and defined data rules should touch ePHI. Independent research shows 60% of healthcare organizations lack controls governing sensitive data in AI systems, so a written AI acceptable use policy is the first step.

Does a BAA make an AI tool HIPAA compliant?

No. A BAA is a required contract when a vendor handles PHI for you, but you must still configure access, labels, logging, and retention, train staff, and review outputs. Compliance depends on how the tool is deployed and used.

What is shadow AI in healthcare?

Shadow AI is the use of AI tools that the organization has not approved or vetted. A 2025 Wolters Kluwer Health survey found about 17% of healthcare workers admitted using unauthorized AI tools and more than 40% knew colleagues who had.

Is Microsoft 365 Copilot ready for a healthcare practice?

It can be, once permissions, sensitivity labels, DLP, and audit logging are reviewed. Copilot works within existing user access, so overshared SharePoint, Teams, and OneDrive content becomes easier to find. Cleaning up access first is the safest path.

How long does it take to prepare for healthcare AI adoption?

A focused 90-day plan can inventory AI use and permissions, define governance and human review rules, and pilot a few low-risk workflows. Broader adoption then follows from what the pilot shows.

Will AI replace clinical judgment or staff review?

No. In a responsible model AI supports administrative workflows, and a named person reviews outputs before they are used. ECRI ranks misuse of AI chatbots as the top health technology hazard for 2026, which is why human review is a core control.

AdvancedBITS | Business IT Solutions

Secure. Compliant. Outcome-Focused.

Ready to see where your organization stands? Ask for a no-obligation healthcare AI readiness review.

sales@advancedbits.com | www.advancedbits.com | 561-300-3015

Sources

Statistics were checked against the sources below as of October 22, 2026.

1. American Medical Association. 2026 Physician Survey on Augmented Intelligence (March 2026). https://www.ama-assn.org/sites/ama-assn.org/files/2026-03/physician-ai-sentiment-report_0.pdf
2. Fierce Healthcare. AMA: Physicians' use of AI doubled from 2023 to 2026 (March 12, 2026). <https://www.fiercehealthcare.com/ai-and-machine-learning/ama-physicians-use-ai-doubled-2023-2026>
3. Wolters Kluwer Health. Shadow AI: Providers are using unapproved tools to improve workflow (January 22, 2026). <https://www.wolterskluwer.com/en/expert-insights/shadow-ai-providers-are-using-unapproved-tools-to-improve-workflow>
4. Healthcare Dive. 'Shadow AI' use is widespread in healthcare: survey (January 22, 2026). <https://www.healthcaredive.com/news/shadow-unauthorized-ai-/810191/>
5. Proofpoint. Cyber insecurity in healthcare 2026: AI adoption is accelerating (October 13, 2026). <https://www.proofpoint.com/us/blog/thought-leadership/cyber-insecurity-healthcare-2026-ai-adoption-accelerating-governance-needs>

6. Proofpoint and Ponemon Institute. 2026 Study on Cyber Insecurity in Healthcare. <https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report>
7. ThreatMon. IBM's Cost of a Data Breach 2025: The AI Oversight Gap (summary of IBM report). <https://threatmon.io/ibms-cost-of-a-data-breach-2025-the-ai-oversight-gap/>
8. HIPAA Journal. Average Cost of a Healthcare Data Breach Falls to \$7.42 Million (July 30, 2025). <https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-2025/>
9. ECRI. Misuse of AI chatbots tops annual list of health technology hazards (January 21, 2026). <https://home.ecri.org/blogs/ecri-news/misuse-of-ai-chatbots-tops-annual-list-of-health-technology-hazards>
10. ECRI. Top 10 Health Technology Hazards for 2026: Executive Brief. <https://www.draeger.com/Content/Documents/Content/ECRI-Top-10-Health-Technology-Hazards-for-2026-Executive-Brief.pdf>
11. WindowsForum. Microsoft 365 Copilot Data Exposure (summarizing ShareGate's 2026 State of Microsoft 365 research, October 9, 2026). <https://windowsforum.com/news/microsoft-365-copilot-data-exposure-fix-oversharing-and-permission-risks.447824/>
12. HIPAA Journal. Largest Healthcare Data Breaches of 2025 (June 5, 2026). <https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2025/>
13. Microsoft Learn. HIPAA and HITECH Act compliance offering. <https://learn.microsoft.com/en-us/compliance/regulatory/offering-hipaa-hitech>
14. HHS. HIPAA Security Rule NPRM Fact Sheet. <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html>
15. HIPAA Journal. HIPAA Security Rule Update Postponed (July 8, 2026). <https://www.hipaajournal.com/hipaa-security-rule-update-postponed/>
16. VertiComply. HIPAA Security Rule Update: Status October 2026. <https://verticomply.com/blog/hipaa-security-rule-update-2026-status>