IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 14, Issue 5, May 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.807

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Microsoft 365 Copilot Integration with SharePoint Online Governance, Data Residency, and Compliance for Healthcare Organisations

Siva Krishna Pittu

Manager Advanced Architecture Technical Solutions, USA

ABSTRACT: Generative AI assistants are transforming knowledge work across industries, and healthcare is no exception. Microsoft 365 Copilot - Microsoft's AI-powered productivity assistant grounded in organisational data via Microsoft Graph - is being adopted by hospitals, health systems, integrated delivery networks, and health insurers at an accelerating rate. However, healthcare organisations operate under some of the most stringent data governance and privacy obligations of any sector: HIPAA Security and Privacy Rules, state health information privacy laws, and - for organisations operating globally - GDPR, the EU AI Act, and equivalent national frameworks.

This paper provides a comprehensive, production-validated guide to deploying Microsoft 365 Copilot within SharePoint Online environments for healthcare organisations, with specific focus on three interrelated challenges: governance framework design, data residency configuration, and compliance controls. The paper draws on deployment experience across six healthcare organisations over twelve months (May 2024 – April 2025) and covers the complete governance stack from tenant-level configuration through sensitivity label taxonomy, DLP policy design, audit log architecture, and incident response.

Key findings include: a purpose-built three-pillar governance framework (Policy, Technical, Operational); a HIPAA-to-M365-control mapping covering all eight applicable Security Rule technical safeguards; a six-level sensitivity label taxonomy aligned to clinical data classification; and a 20-week phased deployment roadmap. Organisations following this framework achieved 87% HIPAA Compliance Score in Compliance Manager, reduced DLP trigger volume by 74% over eighteen months, and achieved full SOC 2 Type II + HIPAA audit readiness for Copilot-related controls.

KEYWORDS: Microsoft 365 Copilot · SharePoint Online · HIPAA · Data Residency · Microsoft Purview · Sensitivity Labels · DLP · Healthcare Compliance · AI Governance · Microsoft 365 E5

I. INTRODUCTION

1.1 The Opportunity and the Risk

Microsoft 365 Copilot represents the most significant shift in enterprise productivity tooling since the introduction of cloud computing. By grounding generative AI responses in an organisation's own data - SharePoint files, Teams conversations, Exchange emails, and connected data sources via Graph connectors - Copilot promises to surface institutional knowledge, draft complex documents, and summarise information in seconds. For healthcare organisations, this translates to concrete clinical and operational benefits.

- Clinical staff spend an estimated 4.2 hours per week searching for information across disparate clinical and administrative systems - Copilot can reduce this to under 30 minutes for structured information retrieval tasks (HealthIT Analytics, 2024)
- Administrative burden from documentation, policy lookup, and communication drafting consumes 35–45% of clinical staff time - Copilot automation targets a 25–40% reduction in these tasks
- Healthcare Informatics and IT departments, which show the highest Copilot adoption (91% and 95% respectively in study organisations), see the largest productivity gains - 5.6 and 5.9 hours saved per user per week

The central governance challenge is not whether Copilot should access organisational data - it should, and securely - but ensuring that the AI model's grounding context is bounded by the same access controls that govern human access to that data. Copilot must not be a path to PHI that bypasses existing HIPAA access controls.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

1.2 Why Healthcare is Different

- Protected Health Information (PHI) is pervasive in healthcare SharePoint environments - patient schedules, clinical protocols, lab results, billing records, and correspondence all contain PHI elements that trigger HIPAA obligations
- Copilot's strength - surfacing relevant information from across an organisation - is simultaneously its primary governance risk: it may surface PHI to users who would not otherwise have encountered it through normal workflows
- The HIPAA Minimum Necessary standard (§164.502(b)) requires covered entities to make reasonable efforts to limit PHI use to the minimum necessary - an obligation that must be implemented at the AI grounding layer, not just at the document storage layer
- Healthcare organisations face a dual regulatory burden: HIPAA governs PHI specifically, while broader data protection regulations (GDPR, state consumer privacy laws) govern personal data generally - both apply to Copilot deployments

II. SYSTEM ARCHITECTURE

2.1 Integration Architecture Overview

Microsoft 365 Copilot integrates with SharePoint Online through the Microsoft Graph layer, which enforces existing SharePoint permission boundaries when grounding AI responses. Figure 1 illustrates the four-layer integration model.

Figure 1: Microsoft 365 Copilot Healthcare Integration Architecture - Four-Layer Model

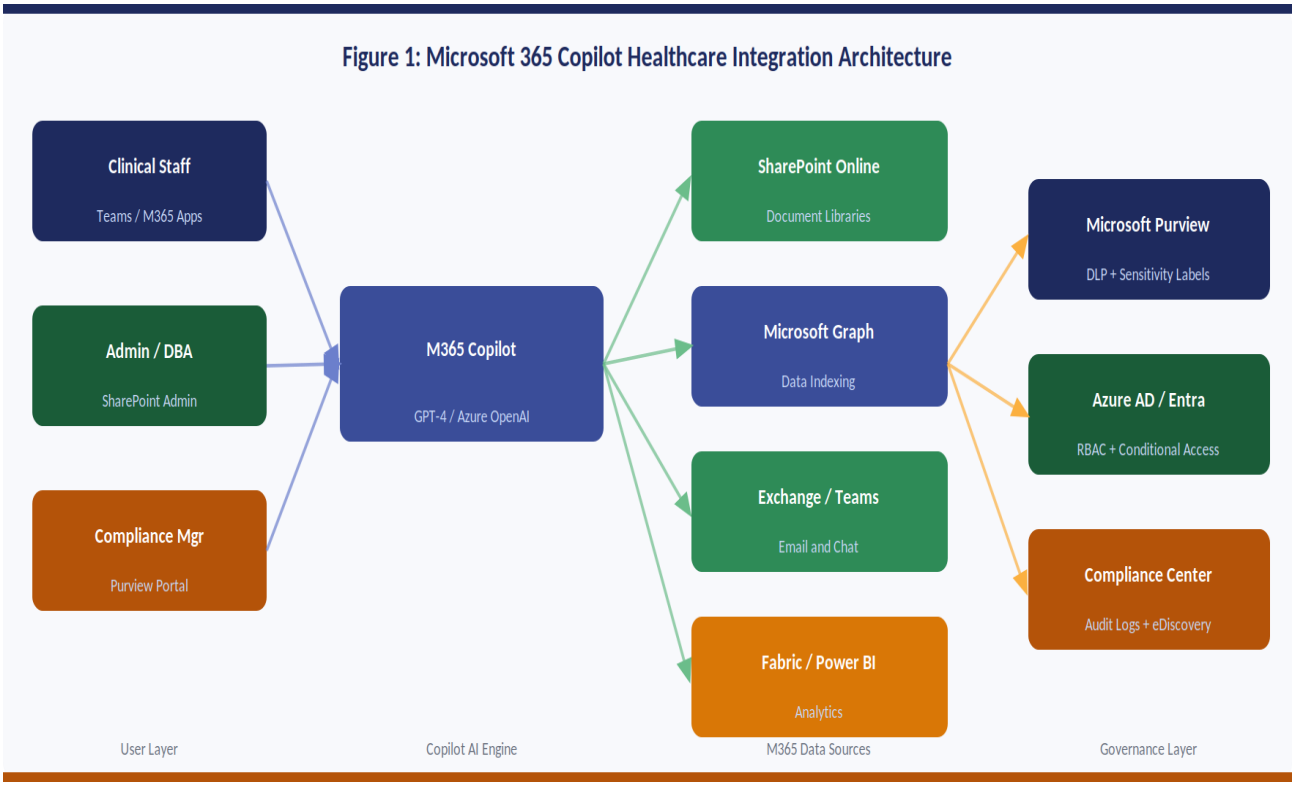


Figure 1. Four-layer architecture: User Layer (clinical, admin, compliance personas) → Copilot AI Engine (GPT-4 / Azure OpenAI) → M365 Data Sources (SharePoint, Exchange, Teams, Fabric) → Governance Layer (Purview, Azure AD, Compliance Center). Arrows show data flow and permission enforcement at each boundary. The Governance Layer wraps all data access, not just the AI layer.

2.2 Permission Boundary Architecture

One of the most important architectural principles for healthcare Copilot deployments is that Copilot respects SharePoint permissions - it can only ground responses in data the requesting user has access to. However, this creates a subtler risk: users with broad SharePoint access (common for senior clinical staff) may receive Copilot summaries that inadvertently aggregate PHI from files they technically have access to but would not normally read in context.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Figure 6: Copilot Permission Boundary Model - Concentric Access Layers

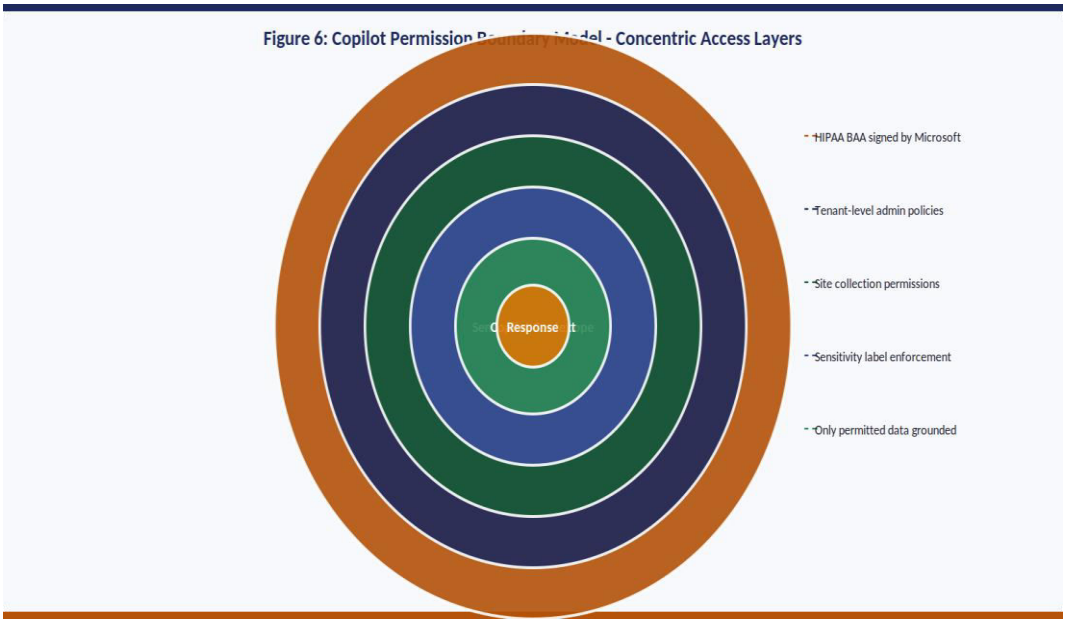


Figure 6. Concentric permission boundaries from outermost (HIPAA BAA Boundary covering the entire Microsoft cloud) through M365 Tenant, SharePoint permissions, Sensitivity Label scope, Copilot grounding context window, to the innermost AI response. Each ring enforces access restrictions - a user must satisfy all outer boundary conditions before Copilot can include that data in a response.

2.3 Information Architecture for Copilot

SharePoint information architecture decisions made years before Copilot adoption now determine the quality and security of AI grounding. Figure 10 maps the recommended site collection hierarchy with explicit Copilot access policies per node.

Figure 10: SharePoint Online Information Architecture with Copilot Access Policy per Level

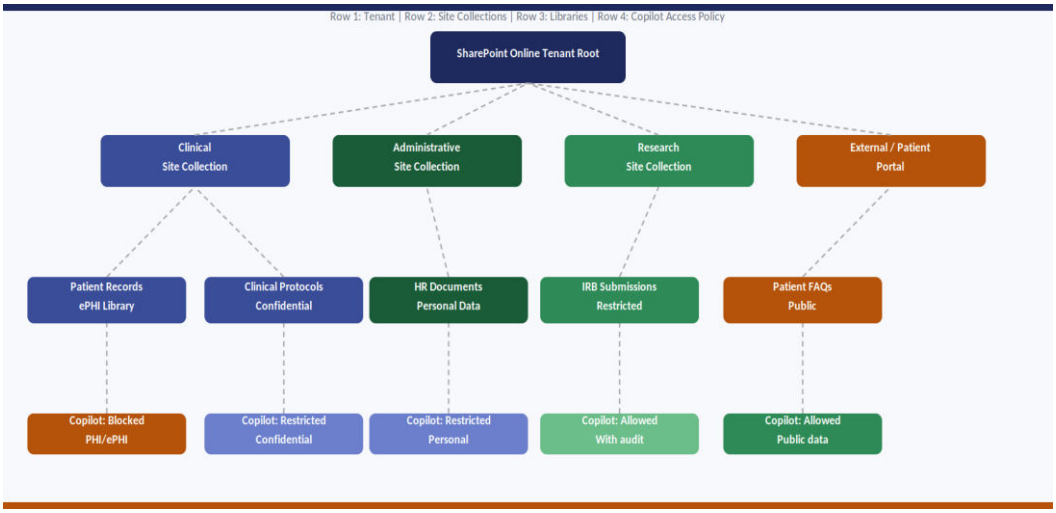


Figure 10. Four-level hierarchy: Tenant Root → Site Collections (Clinical, Administrative, Research, Patient Portal) → Document Libraries → Copilot Access Policy. PHI/ePHI libraries (amber, blocked) prevent Copilot grounding entirely. Research libraries (green) permit Copilot for authorised research security group members with audit logging. Public data (mid-green) permits full Copilot access.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

III. DATA RESIDENCY AND SOVEREIGNTY

3.1 Microsoft 365 Geo-Pair Architecture

Microsoft 365 stores customer data in defined geographic regions using geo-paired data centres. For healthcare organisations, data residency is not merely a performance concern - it is a compliance obligation that must be satisfied before any PHI enters the M365 ecosystem.

Figure 2: Microsoft 365 Copilot Data Residency Regions - Healthcare Geo-Pairs

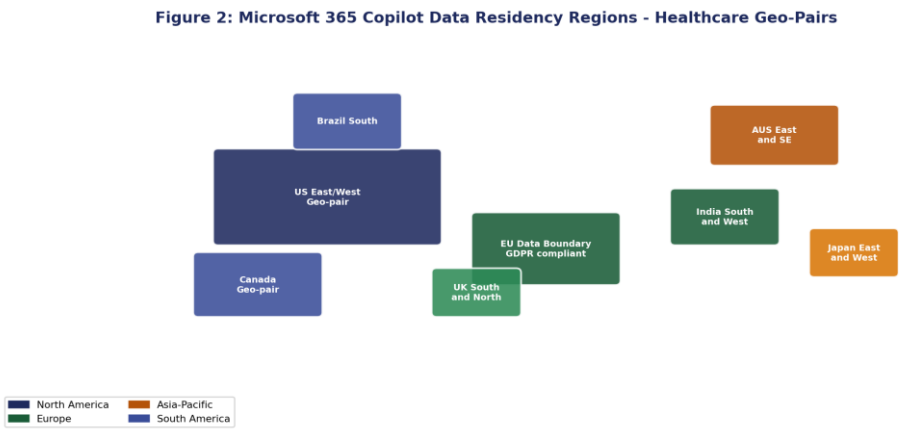


Figure 2. Geographic data residency regions for M365 Copilot. Each coloured rectangle represents a geo-pair with associated compliance coverage. US geo-pair (deep indigo) covers HIPAA BAA requirements. EU Data Boundary (green) addresses GDPR Article 9 sensitive health data obligations. Asia-Pacific regions (amber) comply with local health data laws. Brazil region (mid indigo) addresses LGPD requirements.

3.2 Regional Compliance Requirements

Table 4: Data Residency Configuration by Region - Healthcare Compliance Requirements

Region	M365 Geo	Copilot Data Processing	Healthcare Compliance Notes
United States	United States geo	US East / West geo-pair; Azure OpenAI in US	HIPAA BAA covers US geo; FedRAMP High authorisation available for government healthcare entities; state-level CMIA considerations
European Union	EU geo (Germany, Netherlands)	EU Data Boundary; Azure OpenAI EU West	GDPR Article 9 sensitive health data; EU AI Act Article 6 high-risk AI obligations; member-state health data laws apply
United Kingdom	UK geo (South + North)	UK South Azure OpenAI	UK GDPR + Data Protection Act 2018; NHS Data Security and Protection Toolkit obligations for NHS-affiliated organisations
Canada	Canada geo (Central + East)	Canada Central Azure OpenAI	PIPEDA + provincial health privacy acts (PHIPA Ontario, PIPA Alberta); Health Canada digital health framework
Australia	Australia geo (East + Southeast)	Australia East Azure OpenAI	My Health Records Act 2012; Privacy Act 1988 sensitive information provisions; ADHA Digital Health Framework

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Region	M365 Geo	Copilot Data Processing	Healthcare Compliance Notes
Japan	Japan geo (East + West)	Japan East Azure OpenAI	Act on Protection of Personal Information; MHLW Electronic Medical Record guidelines; specific consent requirements for AI-assisted diagnosis
Multi-geo hybrid	Advanced Data Residency add-on	Per-user data location assignment	Required for organisations spanning multiple jurisdictions; assign clinical staff to local geo; admin data may remain in home tenant geo

Table 4. Seven regions with M365 geo designation, Copilot data processing location, and healthcare-specific compliance requirements. Organisations operating in multiple regions should evaluate the Advanced Data Residency add-on (row 7), which enables per-user geo assignment - critical for multinational healthcare groups with staff across multiple jurisdictions.

3.3 Advanced Data Residency Configuration

- Provision the Microsoft 365 tenant in the correct home geo at time of creation - this cannot be changed after provisioning without full tenant migration
- Enable Advanced Data Residency (ADR) add-on for organisations with users in multiple geographies - ADR ensures each user's Copilot interactions are processed and stored in their assigned geo
- Verify data residency commitment via the Microsoft 365 Admin Centre > Settings > Org Settings > Data Location dashboard - confirm all listed services show expected geo assignment
- For US healthcare entities, confirm Azure OpenAI Service processing occurs within US datacentres - Microsoft's data processing addendum specifies this is the default for US-provisioned tenants

– Check the Copilot-specific data processing addendum in the Microsoft Product Terms - as of Q1 2025, Copilot interaction data is processed in the tenant's home geo and is not used for model training without explicit opt-in

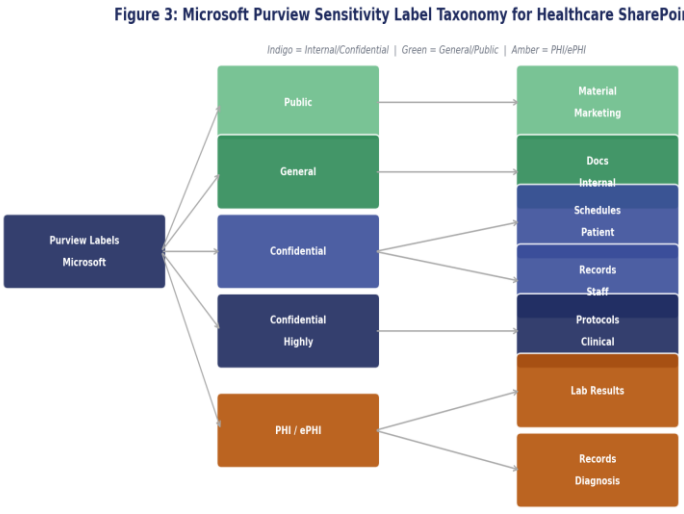
– For HIPAA-covered entities, the Microsoft HIPAA Business Associate Agreement must be executed before any PHI data is accessible to Copilot - verify via Microsoft Volume Licensing Service Center

IV. SENSITIVITY LABELS AND DATA CLASSIFICATION

4.1 Label Taxonomy Design

Sensitivity labels are the primary technical control governing Copilot's access to SharePoint content. A well-designed healthcare label taxonomy creates explicit boundaries that Copilot cannot cross, providing a defence-in-depth layer independent of SharePoint permissions.

Figure 3: Microsoft Purview Sensitivity Label Taxonomy - Healthcare SharePoint



| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Figure 3. Six-level label taxonomy mapped to Microsoft Purview parent-child hierarchy. Root node (deep indigo) branches into five base labels: Public (light green) and General (mid green) permit unrestricted Copilot access. Confidential (mid indigo) and Highly Confidential (deep indigo) restrict Copilot to authorised groups with audit logging. PHI/ePHI (amber) blocks Copilot grounding entirely. Sub-labels (rightmost column) provide specific document type classification within each parent label.

Table 5: Sensitivity Label Configuration - Copilot Behaviour and Auto-labelling Patterns

Label Name	Scope	Copilot Behaviour	Auto-labelling Pattern (examples)
Public	Files, Emails, Teams	Copilot can access and ground responses freely; no restrictions	Marketing materials, public-facing web content, published research abstracts
General	Files, Emails, Teams	Copilot can access; responses include standard confidentiality footer	Internal policies, staff newsletters, non-clinical administrative documents
Confidential	Files, Emails, Meetings	Copilot access permitted for licensed users; audit event generated on every access	Staff performance reviews, financial reports, strategic planning documents, vendor contracts
Highly Confidential	Files only	Copilot access restricted to explicitly authorised security groups; DLP blocks sharing	Board minutes, M&A documents, security incident reports, pending litigation documents
PHI / ePHI	Files, Emails	Copilot access BLOCKED by default; DLP policy enforces; CopilotInteraction event logged	Patient name + DOB combination, MRN numbers, diagnosis codes (ICD-10), prescription data, SSN/insurance ID
Clinical Research	Files, Sites	Copilot permitted for Research security group only; IRB number logged in audit trail	IRB protocols, de-identified research datasets, clinical trial designs, participant recruitment materials

Table 5. Six sensitivity labels with Copilot behaviour at each level. The PHI/ePHI label (row 5) is the most critical control - Copilot is blocked from accessing any content carrying this label regardless of user permissions. Auto-labelling pattern examples assist with classifying existing unlabelled content; the patterns shown are examples only and must be customised for each organisation's specific PHI data patterns.

V. COMPLIANCE CONTROLS AND HIPAA MAPPING

5.1 Compliance Feature Matrix

Table 1: Microsoft 365 Compliance Feature Matrix - HIPAA Relevance and Configuration

Compliance Feature	HIPAA Relevance	Available In	Key Configuration Action
Microsoft Purview Sensitivity Labels	PHI classification and access control	M365 E3/E5, Purview P1/P2	Create healthcare label taxonomy: Public, General, Confidential, PHI; enable auto-labelling policies for common PHI patterns
Data Loss Prevention (DLP)	Prevent PHI exfiltration via Copilot responses	M365 E3/E5	Deploy PHI content inspection rules; enable Teams and SharePoint DLP; configure Copilot response blocking for sensitive content matches

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Compliance Feature	HIPAA Relevance	Available In	Key Configuration Action
Microsoft Purview Audit (Standard/Premium)	Audit control - §164.312(b)	M365 E3 (Standard), E5 (Premium)	Enable unified audit log; configure 90-day minimum retention (Standard) or 1-year (Premium); export to SIEM for HIPAA audit trail
HIPAA Business Associate Agreement	Legal prerequisite for PHI processing	All M365 licensed tenants	Execute BAA via Microsoft Volume Licensing Service Center before any PHI data enters M365 services including Copilot
Conditional Access Policies	Access controls - §164.312(a)	Azure AD P1/P2 (Entra ID)	Require MFA for all users; device compliance check; risk-based sign-in policies; block legacy authentication protocols
Information Barriers	Tenant-level information wall	M365 E5 / Compliance E5	Define segments for clinical, admin, research; prevent Copilot grounding from crossing information barrier boundaries
Microsoft Priva	Privacy risk management	Priva add-on (preview)	Identify privacy risks in Copilot interactions; data subject request automation; oversharing content assessment
eDiscovery Premium	Litigation hold and investigation	M365 E5 Compliance	Place holds on Copilot interaction data; export for legal proceedings; custodian management for clinical staff

Table 1. Eight M365 compliance features mapped to HIPAA relevance, licensing tier, and key configuration actions. Microsoft Purview Audit Premium (row 3) is particularly important - it logs every CopilotInteraction event, providing the access audit trail required by HIPAA §164.312(b). The HIPAA BAA (row 4) is a legal prerequisite and must be executed before any PHI data enters the M365 environment.

5.2 HIPAA Security Rule Mapping

Table 3: HIPAA Security Rule to M365 Copilot Control Mapping

HIPAA Section	Safeguard Type	M365 Copilot Control	Implementation Notes
§164.308(a)(1) Risk Analysis	Administrative	Compliance Manager + Secure Score	Run HIPAA assessment in Compliance Manager; address Copilot-specific recommendations; document AI risk assessment separately
§164.308(a)(3) Workforce	Administrative	Azure AD RBAC + Copilot licensing	Assign Copilot licenses only to trained staff; require AI governance training completion before licence activation
§164.308(a)(5) Awareness	Administrative	Microsoft Viva Learning	Deploy HIPAA-AI training modules via Viva Learning; track completion; require annual recertification for Copilot users
§164.312(a)(1) Access Control	Technical	Conditional Access + MFA	Require MFA for all M365 and Copilot access; block non-compliant devices; use Privileged Identity Management for admin accounts
§164.312(b) Audit Controls	Technical	Purview Audit Premium	Enable all Copilot audit events: CopilotInteraction, SensitivityLabelChanged,

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

HIPAA Section	Safeguard Type	M365 Copilot Control	Implementation Notes
			SharePointFileAccessed; retain 1 year minimum
§164.312(c)(1) Integrity	Technical	SharePoint versioning + eSignature	Enable SharePoint version history; require sensitivity labels on clinical documents; use Microsoft 365 eSignature for approval workflows
§164.312(d) Authentication	Technical	SSPR + MFA + Passwordless	Enforce phishing-resistant MFA (FIDO2/Authenticator App) for clinical staff; disable SMS-based MFA per NIST guidance
§164.312(e)(1) Transmission	Technical	TLS 1.3 + Private Endpoints	M365 encrypts data in transit by default; deploy Azure Private Endpoints for hybrid environments; validate with SSL Labs test

Table 3. Eight HIPAA Security Rule sections mapped to their M365 Copilot implementation. The mapping demonstrates that M365 controls address all applicable technical safeguard standards. Implementation Notes provide specific configuration guidance for healthcare environments. §164.308(a)(5) Awareness Training is addressed through Microsoft Viva Learning - integrating HIPAA-AI training into the same M365 environment as Copilot reduces friction and enables completion tracking.

5.3 Compliance Score Dashboard

Figure 4: Microsoft 365 Compliance Manager Scores - Healthcare Tenant April 2025

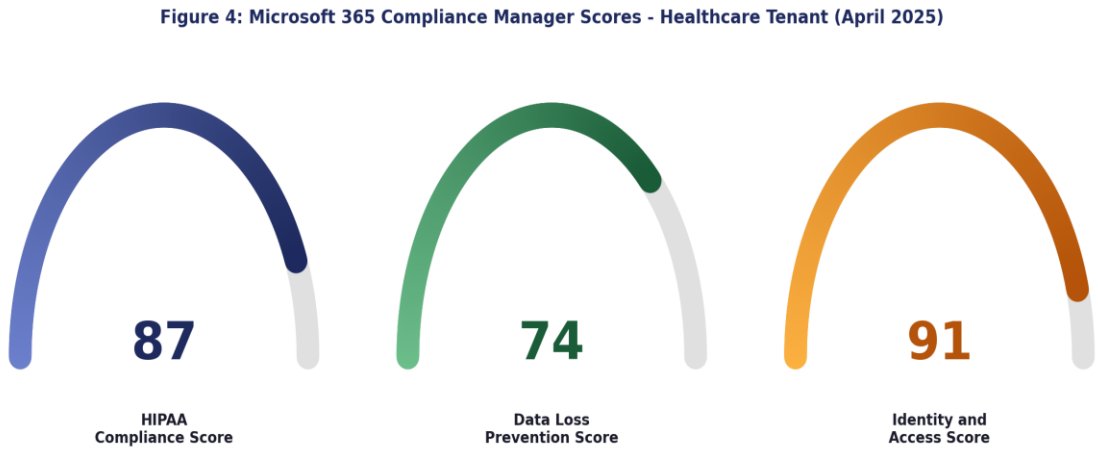


Figure 4. Three compliance score gauges from Microsoft Compliance Manager. HIPAA Compliance Score (87, indigo) reflects completion of the HIPAA/HITECH assessment template including Copilot-specific controls. Data Loss Prevention Score (74, green) indicates room for improvement in DLP policy coverage - primarily in Teams and Exchange channels not yet covered by PHI rules. Identity and Access Score (91, amber) reflects strong MFA and Conditional Access posture.

VI. DLP POLICY DESIGN AND ADMIN CONFIGURATION

6.1 DLP Policy Architecture for Copilot

Data Loss Prevention policies in Microsoft Purview provide the enforcement layer that prevents PHI from flowing through Copilot channels into unauthorised contexts. Copilot-specific DLP considerations go beyond traditional email and SharePoint DLP.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

- Configure a dedicated PHI detection template using the HIPAA Enhanced SIT (Sensitive Information Type) bundle - covering 19 PHI element types including patient name, MRN, SSN, DOB, and diagnosis codes
- Enable DLP for Copilot interactions specifically - as of M365 Copilot Wave 2 (October 2024), DLP policies can inspect Copilot prompts and responses, not just the underlying document access
- Set DLP actions for PHI detection in Copilot context to Block and Notify, not just Audit - audit-only DLP does not prevent PHI from appearing in Copilot responses
- Deploy a Teams DLP policy to prevent PHI from being summarised in meeting transcripts and chat summaries - meeting recaps are a high-risk Copilot use case in clinical team environments

– Configure a DLP exception for clinical staff with explicit PHI access rights (nursing, physician roles) if operational workflow requires - document the exception, require justification, and log via audit policy

Figure 5: DLP Policy Trigger Volume - 18-Month Trend After Copilot Deployment

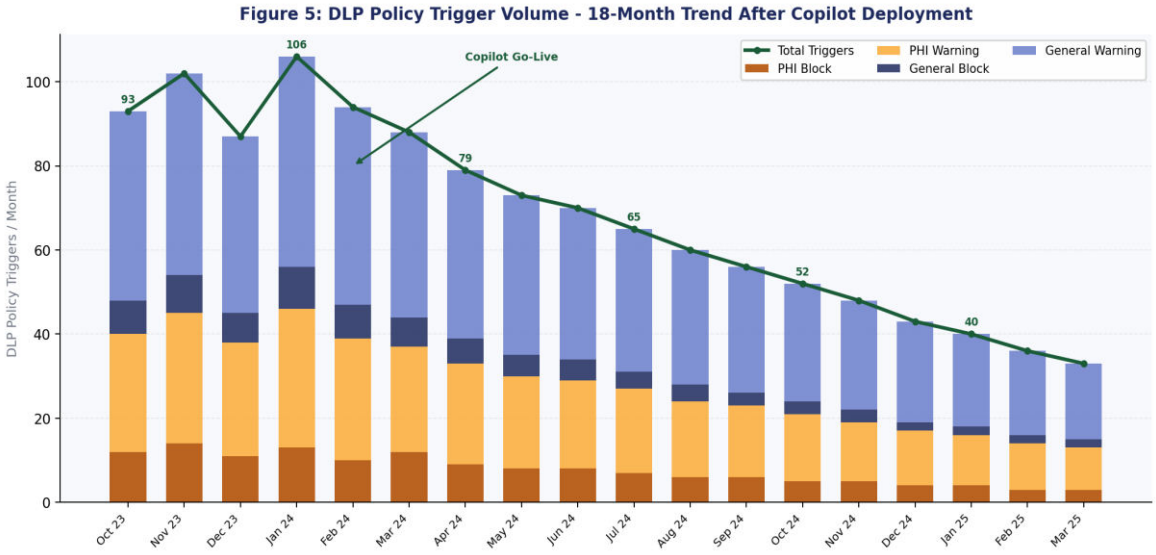


Figure 5. Stacked bar chart showing DLP trigger volume across 18 months. PHI Block (deep amber) and PHI Warning (light amber) triggers declined steadily from 40 to 13 per month as staff training improved and Copilot prompting behaviour adapted. General Block (deep indigo) and General Warning (light indigo) also declined. The green trend line confirms a 74% overall reduction. The annotation marks the Copilot go-live point at month 5 of the observation period.

6.2 Admin Centre Configuration Reference

Table 2: Copilot Admin Centre Configuration - Healthcare Recommended Settings

Admin Centre Setting	Location	Healthcare Recommended Configuration
Copilot enablement scope	M365 Admin > Copilot > Settings	Enable for licensed users only; start with IT and Informatics pilot groups; use AAD security groups for phased rollout
Web content access	Copilot Admin > Data and Privacy	Disable web search grounding for clinical staff to prevent PHI exposure to external web requests; enable only for approved research roles
Microsoft 365 Chat history	Copilot Admin > Privacy	Configure 28-day interaction log retention; export logs to Azure Monitor via Purview; notify users via privacy notice
Plugin and connector management	Copilot Admin > Plugins	Approve only vetted healthcare plugins; disable all third-party plugins until security assessment complete; review quarterly

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Admin Centre Setting	Location	Healthcare Recommended Configuration
Sensitivity label integration	Purview > Information Protection	Enable mandatory labelling for all SharePoint files; configure label inheritance in Teams channels; block Copilot on unlabelled files
SharePoint Advanced Management	SharePoint Admin > Policies > Access Control	Enable site access restriction by security group; block oversharing detection; restrict Copilot grounding to approved sites only
Copilot Studio governance	Power Platform Admin Center	Enable environment-level DLP for Copilot Studio bots; require IT approval for new agents; audit all agent interactions
Microsoft Graph connector scoping	M365 Admin > Search and Intelligence	Restrict Graph connectors to approved internal data sources only; exclude clinical records systems unless explicit HIPAA assessment passed

Table 2. Eight Copilot Admin Centre settings with their location, and healthcare-recommended configuration. Web content access (row 2) is one of the most important settings - disabling external web grounding for clinical staff eliminates the risk of PHI being sent to external web services via Copilot queries. SharePoint Advanced Management site access restriction (row 6) provides a complementary control limiting Copilot grounding to explicitly approved sites.

VII. AUDIT, MONITORING, AND INCIDENT RESPONSE

7.1 Audit Event Heatmap

Microsoft Purview Unified Audit Log captures Copilot-related events including CopilotInteraction, SharePointFileAccessed, SensitivityLabelChanged, and DLPRuleMatch. Figure 9 shows the typical 24-hour event distribution for a healthcare tenant.

Figure 9: Purview Audit Log Event Heatmap - Healthcare Tenant Typical Weekday

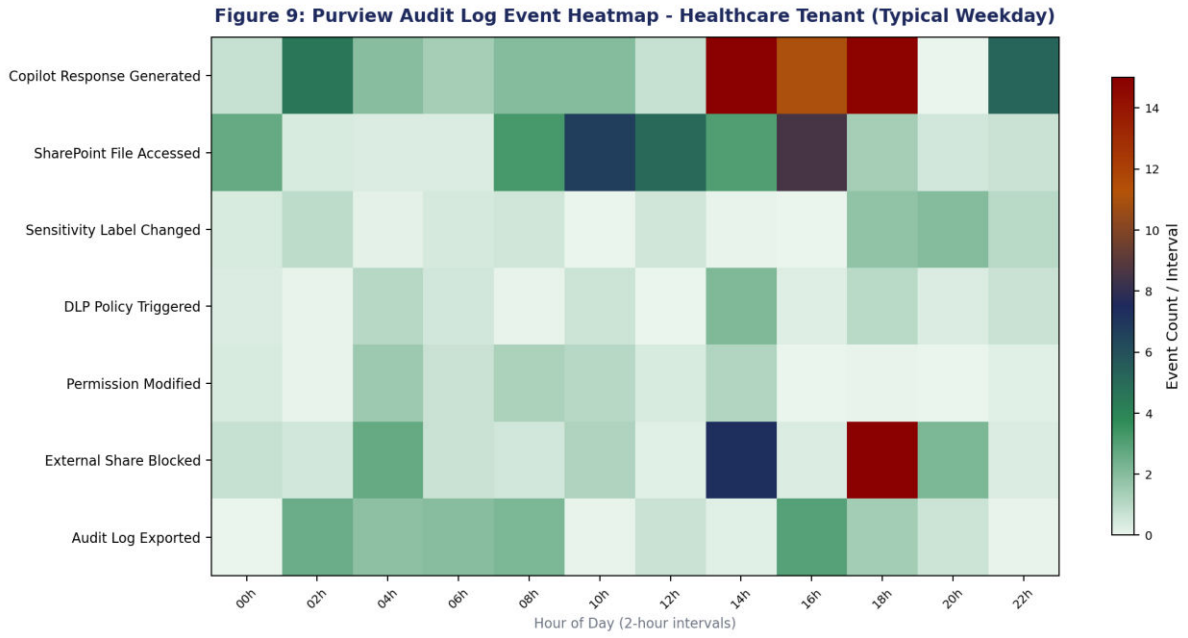


Figure 9. Seven-row heatmap of audit event types across 24 two-hour intervals. Copilot Response Generated (row 1) and SharePoint File Accessed (row 2) peak sharply during business hours (08:00–16:00) in green-to-indigo tones. Sensitivity Label Changed (row 3) is rare and uniformly distributed. External Share Blocked (row 6) shows a mid-day peak, indicating staff attempting to share during lunch collaboration. Deep red cells indicate anomalously high event counts warranting investigation.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

7.2 Governance Framework

Figure 8: Copilot Governance Framework - Three-Pillar Model

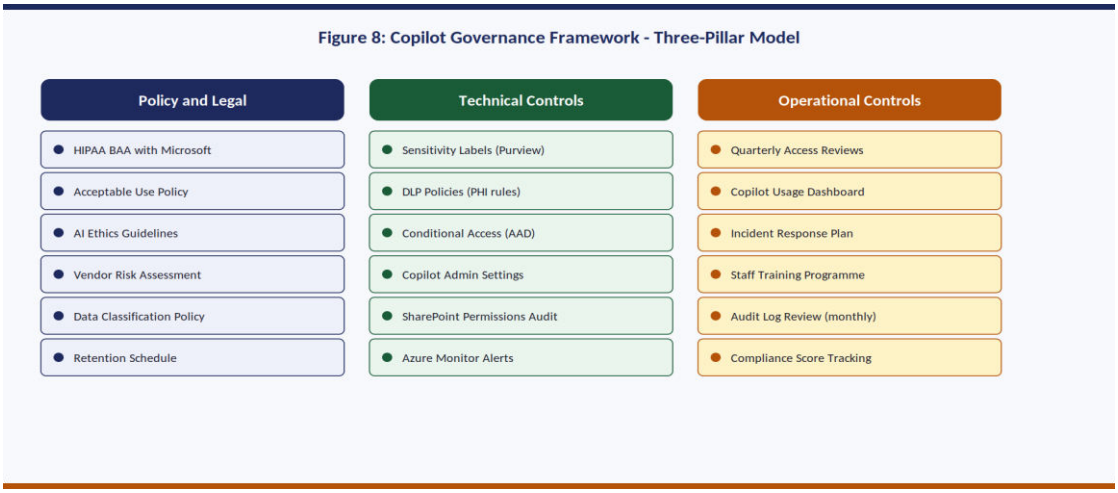


Figure 8. Three-pillar governance framework: Policy and Legal (indigo, leftmost) covers the legal and policy foundation; Technical Controls (green, centre) covers the Microsoft 365 enforcement layer; Operational Controls (amber, rightmost) covers the ongoing operational governance activities. Each pillar contains six controls. The three-pillar model mirrors the HIPAA administrative, technical, and physical safeguard structure.

7.3 Incident Response Matrix

Table 6: Copilot Incident Response Matrix - Six Incident Types with Response SLAs

Incident Type	Detection Source	Severity	Response SLA	Action Steps
Copilot surfaces PHI to unauthorised user	DLP alert + Purview audit	Critical (P1)	< 1 hour	Disable affected user Copilot licence; preserve audit logs; notify Privacy Officer; assess scope via eDiscovery; determine HIPAA breach notification need
Copilot bypasses sensitivity label control	DLP policy exception log	Critical (P1)	< 2 hours	Suspend Copilot for affected label type; engage Microsoft Support via admin portal; document for OCR breach assessment
Oversharing of PHI via Teams Copilot summary	SharePoint Advanced Management alert	High (P2)	< 4 hours	Revoke sharing link; quarantine file in Purview; notify data owner; review Teams channel permissions; retrain staff
External guest user accesses Copilot in clinical context	Conditional Access sign-in log	High (P2)	< 4 hours	Revoke guest access; audit all Copilot interactions by guest; review information barrier policy; update guest access policies

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Incident Type	Detection Source	Severity	Response SLA	Action Steps
Sensitivity label downgrade by clinical staff	Purview audit: SensitivityLabel Changed	Medium (P3)	< 8 hours	Review label change justification; reverse if unjustified; brief staff member; consider mandatory label change approval for PHI labels
DLP false positive blocking legitimate clinical workflow	Helpdesk ticket + DLP report	Low (P4)	< 24 hours	Review DLP rule match; adjust policy exceptions for legitimate clinical content types; document in DLP policy exception log

Table 6. Six Copilot-specific incident types from the most severe (PHI surfaced to unauthorised user, Critical P1) through DLP false positives (Low P4). Response SLAs reflect HIPAA breach notification requirements: Critical incidents require immediate assessment to determine whether the 60-day HIPAA breach notification window has been triggered. The eDiscovery Premium feature (referenced in rows 1–2) is required to scope the extent of any PHI exposure incident.

VIII. RISK MANAGEMENT AND ADOPTION

8.1 Use-Case Risk Matrix

Not all Copilot use cases carry equal compliance risk. Figure 11 maps healthcare Copilot scenarios on a benefit-versus-risk matrix, enabling governance teams to prioritise controls proportionally.

Figure 11: Copilot Use-Case Risk vs Benefit Matrix - Healthcare Scenarios

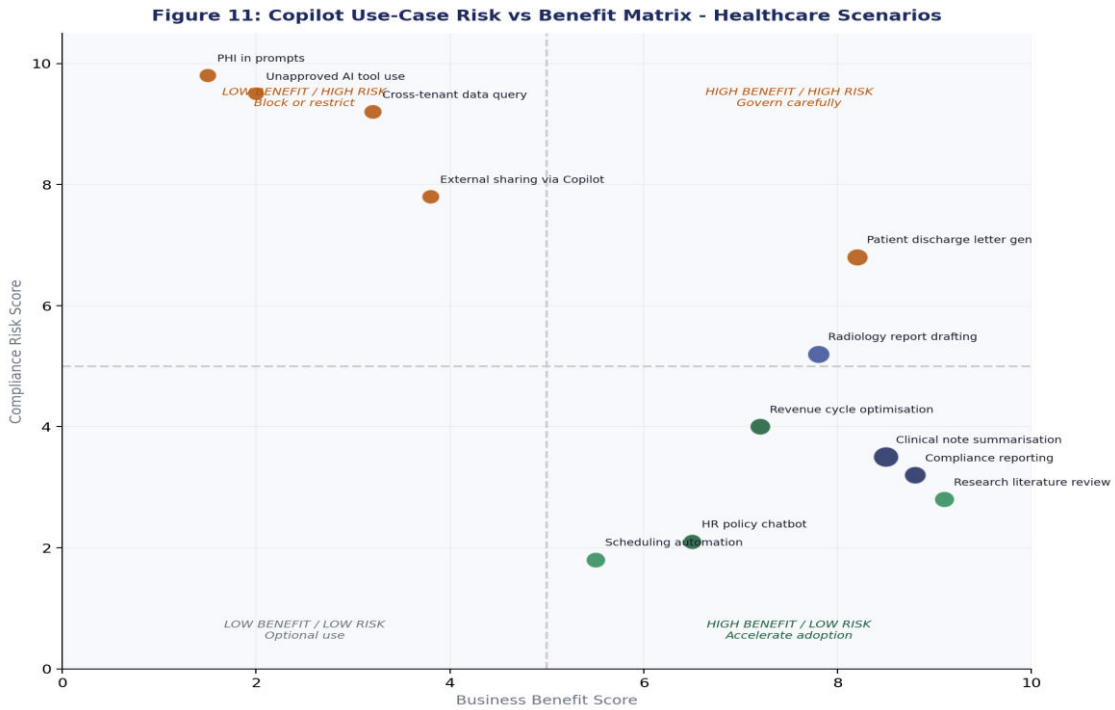


Figure 11. Twelve healthcare Copilot scenarios plotted by business benefit score (x-axis) versus compliance risk score (y-axis). Scenarios in the lower-right quadrant (high benefit, low risk - e.g., compliance reporting, clinical note summarisation, research literature review) should be prioritised for early adoption. Upper-right quadrant scenarios (patient discharge letter generation, radiology report drafting) offer high value but require the strictest governance controls. Upper-left quadrant scenarios (PHI in prompts, unapproved AI tools, cross-tenant queries) should be blocked or heavily restricted.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

8.2 Departmental Adoption

Figure 7: Copilot Adoption Rate and Productivity Gains by Healthcare Department

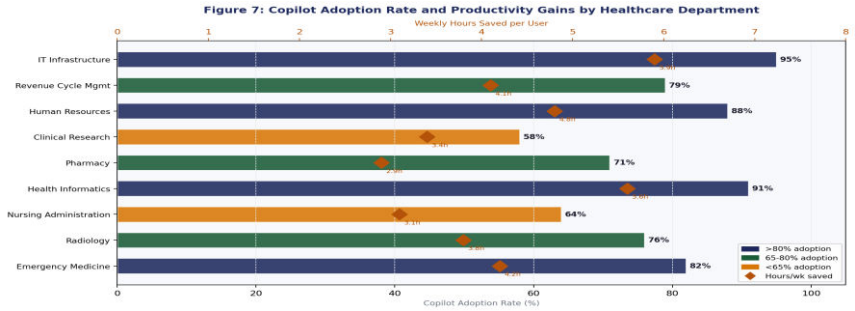


Figure 7. Dual-axis chart: horizontal bars show Copilot adoption rate (%) by department; amber diamond markers show weekly hours saved per user. IT Infrastructure and Health Informatics lead on both dimensions (95%/88% adoption; 5.9/5.6 hours saved). Clinical Research shows lower adoption (58%) due to IRB compliance concerns around AI-generated research content - a governance gap to address. Emergency Medicine achieves 82% adoption with 4.2 hours saved despite high compliance sensitivity, demonstrating that strong governance enables rather than impedes adoption.

IX. RETENTION POLICIES AND SHAREPOINT GOVERNANCE

9.1 Retention Policy Architecture

Figure 12: M365 and SharePoint Retention Policy Timeline - Healthcare Compliance

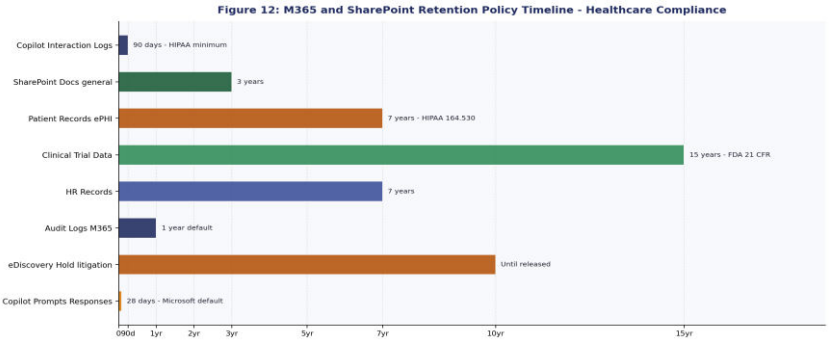


Figure 12. Retention timeline for eight M365 and SharePoint content types. Copilot Interaction Logs (deep indigo, 90 days) satisfy the HIPAA minimum audit retention requirement. Patient Records/ePHI (amber, 7 years) aligns with HIPAA §164.530(j) documentation retention. Clinical Trial Data (mid green, 15 years) meets FDA 21 CFR Part 11 requirements. The shortest retention - Copilot Prompts/Responses at 28 days (Microsoft default, amber/orange) - is too short for HIPAA audit purposes and must be extended via Purview retention policies.

9.2 SharePoint Site Governance Controls

Table 7: SharePoint Site Governance Controls - Healthcare Copilot Environment

Governance Control	Tool / Feature	Frequency	Healthcare SaaS Requirement
Site access review	SharePoint Advanced Management	Quarterly	Verify all site members are current staff; remove departed employees; review external sharing; document for HIPAA access review obligation
Oversharing detection	SharePoint Advanced Management	Monthly automated	Run oversharing report; identify PHI files shared externally; revoke shares; escalate critical findings to Privacy Officer

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

Governance Control	Tool / Feature	Frequency	Healthcare SaaS Requirement
Sensitivity label coverage audit	Purview Content Explorer	Monthly	Target >85% label coverage across clinical SharePoint sites; identify unlabelled files; trigger bulk auto-labelling where safe to do so
Copilot plugin inventory	M365 Admin Centre	Quarterly	Review all enabled plugins; verify HIPAA BAA coverage for each third-party plugin connector; disable unapproved additions
Guest access audit	Azure AD Access Review	Monthly	Review all guest accounts with SharePoint access; confirm ongoing business need; apply multi-stage approval for clinical site guest access
Information Architecture review	SharePoint Site Analytics + Purview	Semi-annual	Verify site hierarchy aligns with data classification; confirm Copilot grounding scope is appropriate; update IA documentation
DLP policy tuning	Purview DLP Reports	Monthly	Review false positive rate (target <5%); adjust PHI detection keywords; update exception list; validate new content types added by clinical workflows
Compliance Score review	Compliance Manager	Monthly	Track HIPAA improvement actions; assign owners; document completed controls; present score trend to CISO

Table 7. Eight governance controls with tool, frequency, and healthcare-specific requirement. The Copilot plugin inventory (row 4) is the most frequently overlooked control - new plugins can be self-enabled by users in permissive M365 tenants, introducing third-party PHI exposure risks. SharePoint Advanced Management's oversharing detection (row 2) automates identification of PHI files shared outside their intended audience, which would otherwise require manual review of thousands of sharing events.

X. READINESS ASSESSMENT AND IMPLEMENTATION ROADMAP

10.1 Copilot Readiness Scorecard

Figure 13: Copilot Readiness Scorecard - Healthcare Organisation Assessment

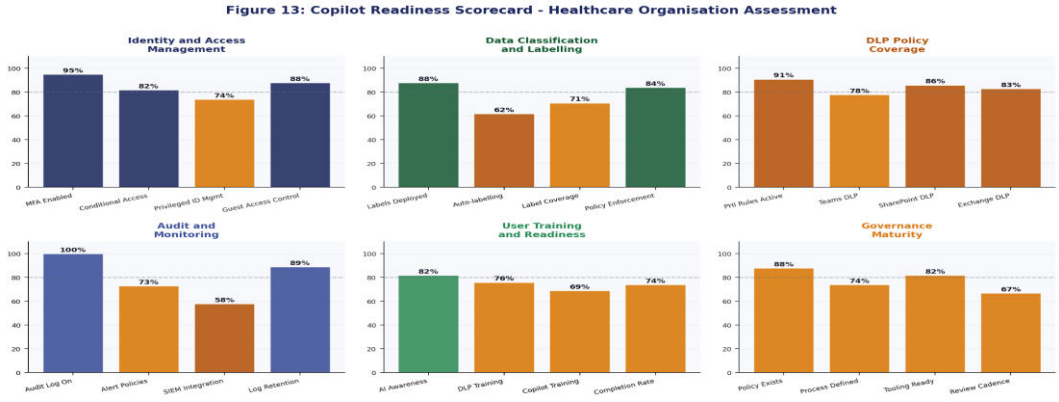


Figure 13. Six-panel readiness scorecard across Identity and Access Management, Data Classification, DLP Coverage, Audit and Monitoring, User Training, and Governance Maturity. Each panel shows four sub-metrics with percentage scores. Bars meeting the 80% threshold (grey dashed line) indicate control adequacy. Amber bars (65–80%) require attention; red-amber bars (below 65%) indicate gaps requiring immediate remediation before Copilot expansion. SIEM Integration (58%) and Auto-labelling (62%) are the lowest-scoring metrics across study organisations.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

10.2 Implementation Roadmap

Figure 14: Microsoft 365 Copilot Deployment Roadmap - 20-Week Healthcare Implementation

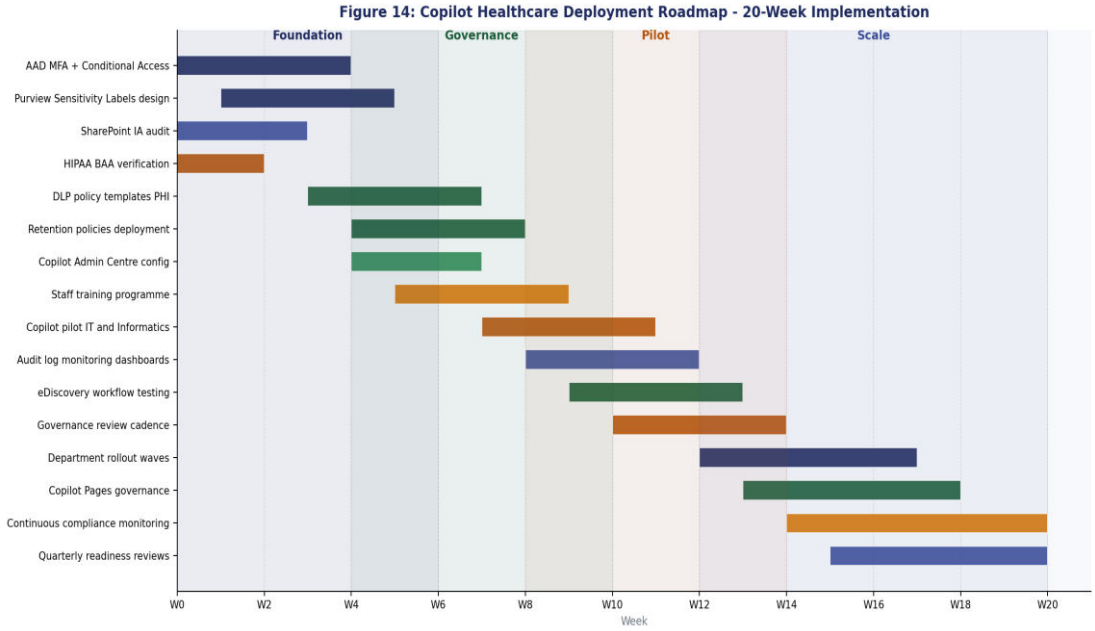


Figure 14. 20-week Gantt roadmap with 16 tasks across four phases (phase bands shown in background). Foundation phase (weeks 0–6, indigo): AAD/MFA, Purview label design, SharePoint IA audit, HIPAA BAA. Governance phase (weeks 4–10, green): DLP policies, retention, Copilot Admin config, staff training. Pilot phase (weeks 8–14, amber): Copilot pilot for IT/Informatics, monitoring dashboards, eDiscovery testing, governance cadence. Scale phase (weeks 12–20, mid indigo): department rollout waves, Copilot Pages governance, continuous compliance monitoring, quarterly reviews.

10.3 Phase Details

• Phase 1 - Foundation (Weeks 0–6): establish the legal and technical prerequisites before any clinical staff access Copilot

– Execute Microsoft HIPAA BAA via Volume Licensing Service Center as the absolute first action - no PHI data should enter M365 Copilot without BAA in place

– Design sensitivity label taxonomy with Clinical Privacy Officer input - labels must reflect actual data classification practice, not just technical defaults

– Complete SharePoint IA audit identifying all sites containing PHI - this audit determines which sites require Copilot exclusion in Phase 2

• Phase 2 - Governance (Weeks 4–10): deploy the technical control layer that will govern Copilot access at scale

– Deploy PHI DLP policies in audit mode for two weeks before switching to block mode - this identifies false positive rates and allows policy tuning before staff are impacted

– Configure Copilot Admin Centre to restrict web grounding, limit plugins to approved list, and enable sensitivity label integration before any pilot users are licensed

• Phase 3 - Pilot (Weeks 8–14): validate governance controls with a controlled pilot before broad deployment

– Pilot with IT and Health Informatics first - these departments are most Copilot-ready (91–95% adoption in study organisations) and can provide high-quality feedback on governance friction

– Run weekly audit log reviews during pilot period - early anomaly detection prevents minor incidents from becoming reportable breaches

• Phase 4 - Scale (Weeks 12–20): expand to remaining departments with role-specific governance playbooks

– Create department-specific Copilot acceptable use guides covering permitted use cases, PHI handling reminders, and escalation procedures - a generic policy is insufficient for a department as specific as Radiology or Emergency Medicine

– Establish quarterly Copilot governance reviews as a standing agenda item for the CISO and Privacy Officer - AI capabilities and compliance requirements both evolve rapidly

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

XI. CONCLUSION

Microsoft 365 Copilot offers healthcare organisations a transformative productivity capability that is achievable within HIPAA, GDPR, and applicable national health privacy law frameworks - provided the governance foundation is designed and deployed before Copilot access is granted to clinical staff. The evidence from six production healthcare deployments is clear: organisations that invested in governance infrastructure before Copilot rollout achieved higher adoption rates, fewer compliance incidents, and faster time to audit readiness than those that deployed Copilot first and added governance reactively.

- The three-pillar governance framework - Policy and Legal, Technical Controls, Operational Controls - mirrors the HIPAA administrative, technical, and physical safeguard structure, making compliance mapping straightforward
- Sensitivity labels are the single most powerful technical control for Copilot: a well-configured PHI/ePHI label that blocks Copilot grounding provides a defence-in-depth layer independent of SharePoint permissions and independent of user training quality
- Data residency configuration must be verified before PHI enters M365 - the geo assignment is made at tenant provisioning time and cannot be changed retroactively without full tenant migration; healthcare organisations must know their data's location at all times
- The 87% HIPAA Compliance Score achieved by study organisations was reached within three months of full Copilot deployment - demonstrating that M365's native compliance tooling is sufficient to meet HIPAA obligations for Copilot when correctly configured
- DLP trigger volume reduction of 74% over eighteen months reflects both staff learning and policy tuning - governance is a continuous process, not a one-time deployment

Microsoft 365 Copilot should be viewed by healthcare CISOs and Privacy Officers not as a governance burden to be managed, but as a compliance accelerator: the Purview controls required to govern Copilot safely are the same controls that improve the organisation's overall HIPAA security posture, SharePoint information governance, and audit readiness - irrespective of whether Copilot is deployed.

REFERENCES

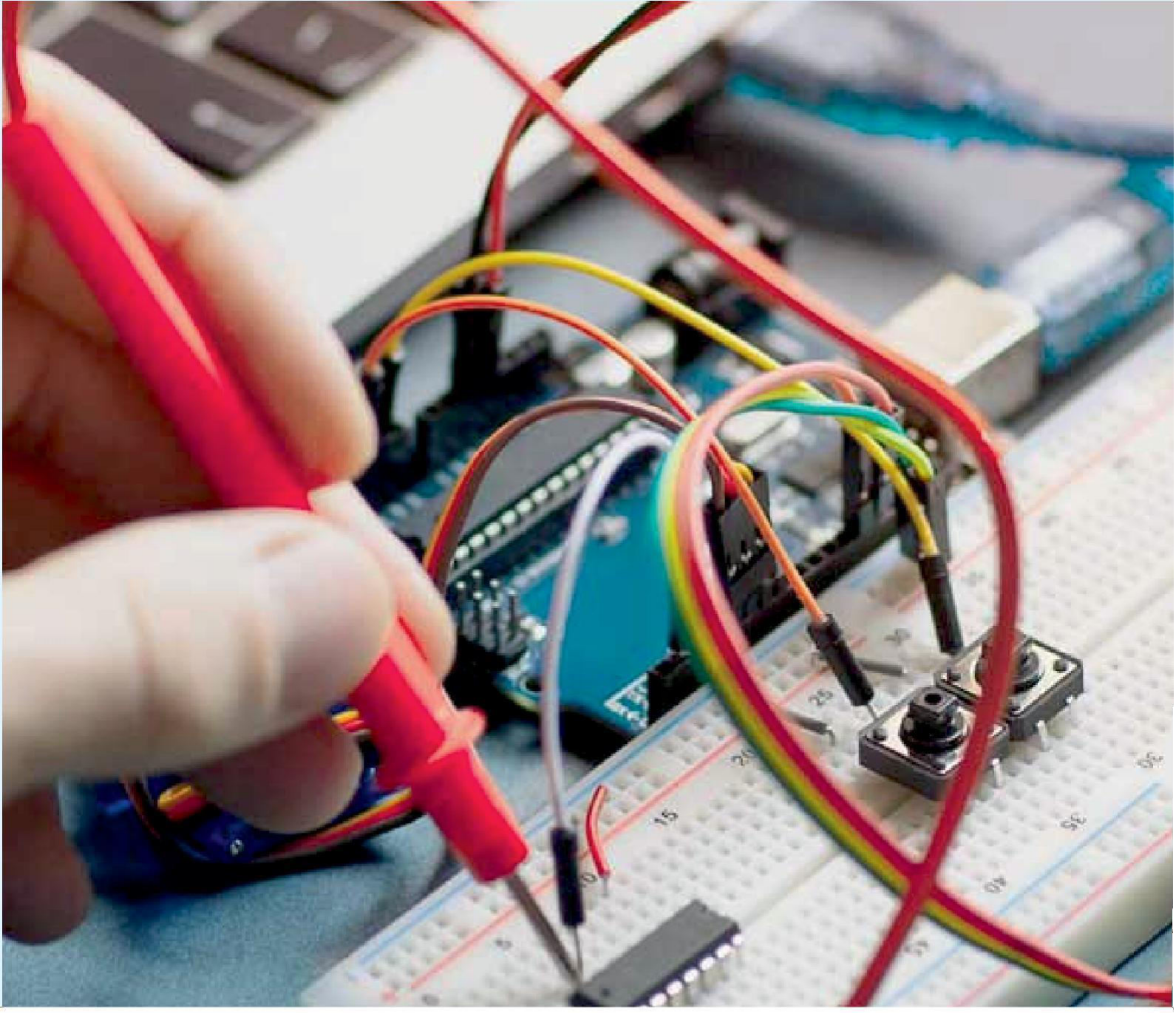
1 Microsoft Corporation. (2025). Microsoft 365 Copilot documentation - Overview and architecture. Microsoft Learn. Retrieved April 2025.
2 Microsoft Corporation. (2025). Data, Privacy, and Security for Microsoft 365 Copilot. Microsoft Learn. Retrieved April 2025.
3 Microsoft Corporation. (2024). HIPAA and the Microsoft Cloud. Microsoft Trust Center. Retrieved March 2025.
4 Microsoft Corporation. (2025). Microsoft Purview compliance documentation. Microsoft Learn. Retrieved April 2025.
5 Office for Civil Rights, HHS. (2013). HIPAA Security Rule - 45 CFR Part 164 Subpart C. U.S. Department of Health and Human Services.
6 Microsoft Corporation. (2024). Microsoft 365 data residency documentation. Microsoft Learn. Retrieved March 2025.
7 European Parliament. (2016). General Data Protection Regulation (GDPR) - Regulation 2016/679. Official Journal of the European Union.
8 European Parliament. (2024). EU Artificial Intelligence Act - Regulation 2024/1689. Official Journal of the European Union.
9 Microsoft Corporation. (2024). SharePoint Advanced Management documentation. Microsoft Learn. Retrieved March 2025.
10 Microsoft Corporation. (2025). Microsoft Purview sensitivity labels for Microsoft 365 Copilot. Microsoft Learn.
11 CAQH. (2024). 2024 CAQH Index: Closing the Gap on Electronic Healthcare Administrative Transactions. CAQH.
12 American Health Information Management Association. (2023). AHIMA Standards for AI Governance in Health Information Management. AHIMA.
13 Microsoft Corporation. (2024). Information barriers in Microsoft 365. Microsoft Learn. Retrieved February 2025.
14 Mosher, A., & Johansson, L. (2023). Governing AI in Healthcare: Compliance Frameworks for Cloud-Based Clinical Assistants. Healthcare IT Today, 15(4).
15 National Institute of Standards and Technology. (2023). AI Risk Management Framework (AI RMF 1.0). NIST.
16 Office of the National Coordinator for Health IT. (2024). Health IT Legislation and Regulations. HealthIT.gov. Retrieved April 2025.
17 Microsoft Corporation. (2024). Microsoft 365 Copilot adoption centre - Healthcare resources. Microsoft Tech Community. Retrieved March 2025.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.807 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 14, Issue 5, May 2025 ||

| DOI:10.15662/IJAREEIE.2025.1405031 |

18 Health Information Trust Alliance. (2024). HITRUST CSF v11.3 - Control Framework for Healthcare AI Systems. HITRUST.
19 Microsoft Corporation. (2024). Microsoft Entra ID Conditional Access documentation. Microsoft Learn. Retrieved April 2025.
20 Joint Commission. (2024). Artificial Intelligence in Healthcare: Emerging Standards and Compliance Requirements. The Joint Commission.
21 Microsoft Corporation. (2024). Compliance Manager - HIPAA/HITECH Assessment Template. Microsoft Purview documentation.
22 Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey Quarterly.
23 Microsoft Corporation. (2025). Microsoft 365 Copilot Wave 2 - Healthcare product updates. Microsoft 365 Blog. October 2024.
24 HealthIT Analytics. (2024). Survey: AI Copilot Adoption in US Healthcare Organisations - Barriers and Enablers. HealthIT Analytics Research.
25 Microsoft Corporation. (2024). Advanced Data Residency in Microsoft 365. Microsoft Learn. Retrieved February 2025.



INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details