QBurst | A High AI-Q™ Company

Navigating Microsoft 365 with Copilot for Enhanced Security and Compliance

Seamless implementation of Microsoft 365 Copilot for a premier US academic medical center, carefully integrating security and governance tools to ensure the powerful AI assistant operated safely within a compliant healthcare environment.

Overview

- **Secure AI Deployment:** Implemented comprehensive governance tools (Purview, Intune, Syntex) to ensure Copilot functioned securely and compliantly, protecting sensitive patient information.
- **Enhanced Efficiency:** Enabled users to leverage Copilot for rapid content creation, editing, and efficient information retrieval across complex systems.
- **Risk Mitigation:** Significantly reduced security and privacy risks associated with managing and sharing sensitive patient data across a large user base.

Client Profile

One of the premier academic medical centers in the United States dedicated to excellence in patient care, education, and research. Consistently ranked among the top 10 hospitals in the US News & World Report 'Best Hospitals' list.

Challenges: Dealing with Distributed, Outdated, and Sensitive Data

- **Security and Privacy Risks:** Wide sharing and manual management of numerous documents across SharePoint, Word, and Outlook posed a high security risk, especially for patient records and sensitive research data.
- **Data Quality and Reliability:** The proliferation of outdated, inaccurate, and redundant data compromises the reliability of information, making it challenging for users to find and utilize relevant data quickly.
- **Compliance Complexity:** Ensuring the use of an advanced AI tool like Copilot to remain compliant with regulations (such as HIPAA) required implementing complex governance and auditing controls.

- **Lack of Control over Devices:** The center needed to secure sensitive data accessed on employee devices outside the primary network.

QBurst Solution: Copilot for Microsoft 365

We implemented Copilot for Microsoft 365, focusing on securing and governing its usage from day one by integrating essential Microsoft compliance and security tools. By strictly following Microsoft's guidelines, we established a secure environment that enabled the medical center to safely harness the power of generative AI.

Microsoft Purview: Configured compliance policies and auditing capabilities for Copilot activities, ensuring the client could monitor and prove regulatory adherence.

Microsoft Intune: Used its unique capabilities to secure data on external devices, enabling secure data transfers outside the organizational network and protecting sensitive information through features like selective wipe.

Microsoft Syntex: This was leveraged to classify, protect, and manage data across the environment, laying the critical groundwork for Copilot by automating mundane tasks like metadata extraction.

Technical Highlights

- **Data Classification and Protection:** Used Purview, Intune, and Syntex to classify and protect data within Microsoft 365, enhancing search capabilities and data discovery.
- **Secure External Access:** Implemented Intune's features to secure data on devices outside the organization and secured public access points via single-app and multi-app kiosk modes.
- **Automated Data Preparation:** Syntex was used to automate information extraction and metadata generation, ensuring Copilot interacts with clean, accurate, and properly tagged data.

- **Compliance Auditing:** The Purview compliance portal was configured to actively audit Copilot activities, providing a complete record for regulatory requirements.

Impact: Streamlining Data for Compliance, Security, and Usability

- **Enhanced Content Creation and Efficiency:** Copilot enabled users to create and edit documents, emails, and content over 50% faster, streamlining administrative and clinical tasks.
- **Improved Document Management and Security:** Leveraging Purview, Intune, and Syntex secured and governed Copilot usage, reducing security and privacy risks by an estimated 40%.
- **Reduced Data Redundancy:** Better data classification and discovery enabled by Purview reduced the instance of outdated, inaccurate, and redundant information, improving data reliability.
- **Sensitive Information Protection:** Intune's capabilities protected sensitive information through selective wipe, safeguarding data even if a user left the organization or lost their device.
- **Compliance Assurance:** The solution ensured continuous compliance with regulations such as HIPAA, GDPR, and ISO 27001.