QBurst

# Navigating **Microsoft 365** with **Copilot**

Learn how Copilot helped a medical center to improve document management and data security.

## Client

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 U.S. News & World Report ‘Best Hospitals’ list.

## Offering

We implemented Copilot for Microsoft 365, an AI-powered assistant that helps to create, edit, and enhance documents, emails, and other information within Microsoft 365 apps such as Word, Excel, PowerPoint, and Outlook. Copilot generates content based on user input, context, and preferences, while also providing suggestions, feedback, and corrections. Additionally, Copilot assists in finding and utilizing relevant information from multiple sources, including the web, SharePoint, OneDrive, and other Microsoft 365 apps.

## Business Challenges

- The center stored numerous documents across SharePoint, Word, Excel, PowerPoint, and Outlook. These documents were shared with a large group of people. This posed a significant security and privacy risk, as certain documents contained patient records and sensitive information.

- The client struggled to manage outdated, inaccurate, and redundant data within Microsoft 365. This compromised the quality and reliability of information and made it challenging for users to locate and utilize relevant data for their tasks.

- There was a need to enhance document management, security, and data quality while increasing efficiency. Security was paramount and Copilot would be expected to function within a secure and compliant environment that would ensure the safety of sensitive data.

## Our Solution

We implemented Copilot for Microsoft 365 along with several tools and features to secure and govern Copilot usage and data. By following Microsoft's guidelines and best practices, we mitigated potential security risks and ensured proper access controls and resource management. The following tools and features were used to secure and govern Copilot for Microsoft 365.

- Implemented Purview, Intune, and Syntex to secure and govern Copilot usage and data.
- Intune, with its unique capabilities to secure data on devices outside the organization, ensures secure data transfers to various organizations outside the network.
- Implemented the Microsoft Purview compliance portal to configure compliance policies for Copilot and to audit Copilot activities.
- Syntex ensures that Copilot operates within a secure and compliant environment, safeguarding sensitive information and helping the organization maintain robust data security practices.
- Syntex helps lay the groundwork for Copilot by automating mundane tasks, such as extracting information and generating metadata.
- Leveraged Purview, Intune, and Syntex to classify, protect, and manage the data in Microsoft 365 and other cloud environments.
- Followed guidelines and best practices provided by Microsoft to mitigate potential security risks and to ensure proper access control and management of resources.

## Technologies Used

Copilot

Purview

Intune

Syntex

## Business Benefits

- **Improved Document Management and Security:** Copilot for Microsoft 365 significantly improved document management, security, data quality, and efficiency.

- **Enhanced Content Creation and Editing:** Copilot enables users to create and edit documents, emails, and other content quickly and easily. It also helps to find and use information efficiently.

- **Generates Relevant Content:** Copilot helps users enhance written communication by offering suggestions, feedback, and corrections. It also generates content based on user input, context, and preferences.

- **Secured and Governed Copilot Usage:** By leveraging Purview, Intune, and Syntex, the client secured and governed Copilot usage and data, ensuring compliance with regulations and standards such as HIPAA, GDPR, and ISO 27001.

- **Enables Better Data Classification:** Purview, Intune, and Syntex enables the organization to classify, protect, and manage data within Microsoft 365 and other cloud environments, improving search and data discovery.

- **Sensitive Information Protection:** Intune's selective wipe feature protects sensitive information by removing it from applications if a user left the organization or if their device was lost or stolen.

- **Public Kiosk Security:** Intune's single-app and multi-app kiosk modes helps to protect sensitive information even when accessed from public kiosks.

- **Reduced Security and Privacy Risks:** By using these tools and features, the client reduced security and privacy risks and improved the accuracy and reliability of information.