CASE STUDY
Enabling Collaboration Among a Fully Remote Workforce

Summary

Challenge
Maintain business continuity for approximately 800 team-based employees from an in-person hospital office environment to a fully remote environment.

Impact

Ensured protection of PHI and PII.

Transitioned seamlessly into a virtual environment allowing for continued operations, as well as collaboration internally and externally with business partners and customers.

Solution
Configured, implemented and deployed Microsoft Teams to approximately 800 workers dispersed across home offices in line with business and compliance requirements of the hospital system.

Trained end users on optimal use of Microsoft Teams for business collaboration.

Implemented security protocols necessary for safe and compliant operations outside of the traditional corporate firewall.

The Business Challenge

When the COVID-19 pandemic started in March 2020, businesses across the nation were forced to shut down offices to mitigate transmission of the virus. Our client, a $1.2B not-for-profit health system, was faced with the challenge of transitioning approximately 800 employees who once worked within their physical hospital offices to dispersed home offices.

This remote set-up would impact end users' ability to collaborate on initiatives and projects for which they traditionally met face-to-face in meeting rooms.

Our client approached Entisys360 to propose a solution that would facilitate collaboration and sharing of information between team members in order to sustain ongoing business imperatives.

The Solution

Entisys360 proposed a phased roll-out of Microsoft Teams starting with features that were easy for end users to learn, then moving to more complex features that required additional infrastructure changes. Based on past experience, Entisys360 understood the three core elements of successful user adoption of a complex product such as Microsoft Teams:

1. **Education**. Including education on Teams features and capabilities, as well as education of security controls and governance available in Teams.

2. **Systems Governance**. Establishing a governance plan with client leadership.

3. **A Phased Deployment**. Implementing teams along with the associated governance measures.

Entisys360 began the engagement with an interactive workshop which served two primary purposes. First, the workshop provided Entisys360 with a clear understanding of the client's business and technical requirements for Microsoft Teams. In order to understand not just the high-level requirements but also the day-to-day user requirements, attendees of the workshop included representatives from all of the major departments within the hospital. The second purpose of the workshop was to educate attendees on Microsoft Teams capabilities, provide a physical demonstration of the product, and answer any questions attendees may have.

Because Microsoft Teams features incorporate the movement of corporate data both internally and externally, governance, security, and compliance were top concerns. During the workshop, Entisys360 gained an understanding of which controls and processes to incorporate into the environment to ensure that corporate data was being protected and that regulatory compliance was met. Some of the security elements that were established as requirements are as follows:

- **DATA LOSS PREVENTION (DLP)** - Like most healthcare organizations, our client was subject to HIPAA regulations that outline the treatment of private and confidential patient information such as social security numbers, addresses, health plan numbers, and medical record numbers among other data. The incorporation of DLP allowed our client to identify where this information was stored and develop policies for the treatment of this information.

- **LEGAL HOLD AND E-DISCOVERY** - The preservation of key data beyond established retention and deletion policies enabling the identification of this data for regulatory or litigation purposes.

- **CONDITIONAL ACCESS POLICIES** - Condition-based policies that verified the identity or users, state of devices and locations from which data was being accessed prior to allowing access to data and applications.

F-210421

Contact us today.
Learn more about how Entisys360 can address your healthcare technology needs through our leading edge advisory and technical solutions. To speak with an Entisys360 healthcare IT services consultant, contact us at **healthcare@entisys360.com**, or visit **entisys360.com/markets/healthcare.**

The Impact

Our understanding of how Microsoft Teams treats external and guest users within a team allowed us to recommend and apply the appropriate policies to allow greater collaboration for our client's employees with its business partners and customers.

Entisys360 also provided structured training courses on the optimal usage of Teams features to ensure that adoption of the product was maintained throughout implementation, and that our client maximized the value they derived from Microsoft Teams. We facilitated two one-hour trainings for 35 client employees in each session, creating super users that extended training to the remaining 800 employees across the organization.

Entisys360 educated and advised our client on the security risks associated with a fully remote workforce. Specifically, as users worked from home, the security perimeter of the organization now extended beyond the corporate firewall. As such, our remote solution comprised a zero-trust security model that challenged users and devices to verify proper rights to data versus the traditional perimeter security model, where remote access to data was far more limited than access from inside the firewall. Based on our recommended security policies, our client has experienced zero security events since implementation of Teams one year ago.

Finally, organizations typically deploy Microsoft Teams without any governance or controls applied, the result of which is the inability to determine how critical data is being shared.

Although the implementation of data loss prevention was not a part of the Phase 1 deployment, Entisys360 was able to illustrate the importance of identifying then safeguarding sensitive data as required by compliance regulations. Our client will pursue a data loss prevention initiative in the near future.