Penn Medicine's Responsibilities

Securing Cloud Applications / Environments

Penn Medicine uses strategies to secure data and maintain compliance, aiming to protect sensitive information and preserve operational integrity within Cloud environments that are used for various business functions.

As a Penn Medicine Business Owner, you must ensure the Cloud platform handling Penn Medicine data meets these minimum technical controls:

- ✓ **Contracts:** Ensure detailed data sharing agreements are in place with clear security standards before exchanging information. Agreements should include at a minimum, protection measures (encryption, compliance), SLAs, support details (hours, contacts, escalation), disaster recovery, backup procedures, RPO/RTO, audit rights, termination terms (notice, post-termination data handling) and AI usage.
- ✓ **Data Accuracy**: Make sure only data that is correct, reliable, legal, and appropriate is entered into the SaaS application.
- ✓ **Data Relevance**: Only enter or send data into the SaaS application that is necessary for the service you are using. Entering unnecessary data can create risks for us.
- ✓ **Artificial Intelligence (AI)**: Ask the vendor to exclude our data from AI training.
- ✓ **Data Encryption**: Ensure that all data at rest and in transit is encrypted using strong encryption protocols to protect sensitive information from unauthorized access.
- ✓ **Data Protection**: Ensure that all information is kept secure by using strong methods to keep it safe. This includes using encryption, which means turning data into a code that can only be read with the right key, both when it is stored and when it is being sent.
- ✓ **Access**: Make sure only the right people can see and use the data by setting up roles and permissions, so only authorized individuals have access to specific information.
- ✓ **Authentication**: Make sure to set up a Single Sign-On (SSO) system that lets Penn employees use one set of login details for multiple applications. If that's not possible, ensure that users have to go through an extra step to confirm their identity, like using a code sent to their phone, or enforcing strong password rules.
- ✓ **Third-party integrations:** When Penn Medicine's existing tools (like Epic and Cerner) connect with the new SaaS platform, Penn Medicine takes care of the special codes (API Keys) and permissions (access tokens) needed for these connections and checks them regularly to ensure they are still correct. Data shared between the systems should also be taken into consideration.
- ✓ **Incident Response Plan**: Develop and maintain an incident response plan to quickly address and mitigate any security breaches or incidents. Regularly review and update the plan to keep it effective.
- ✓ **Business Continuity:** Create a business continuity plan, which is a strategy to ensure that SaaS-supported operations continue during disruptions or system failures.

Work with your IT Owner or technical lead to ensure these controls are implemented *where feasible*. Following them helps protect the SaaS platforms' integrity, availability, and confidentiality.