Penn Medicine's Responsibilities

Securing Data Sent to Service Providers / Firms

At Penn Medicine, robust measures are implemented to secure data and ensure compliance when transmitting sensitive information to external service providers involved in key business operations.

As a Penn Medicine Business Owner, you are responsible for ensuring that all externally shared data is protected, closely monitored, and accessible only to those with proper authorization. The following controls must be established when sending data outside the organization:

- ✓ **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, audit rights, and termination terms (notice, post-termination data handling).
- ✓ **Secure Transmission**: Use only approved, secure transmission methods—such as encrypted email, secure file transfer protocols, Kiteworks, or other Penn Medicine-sanctioned data sharing platforms—to safeguard sensitive data in transit. Under no circumstances should data be sent via FTP or unencrypted email.
- ✓ **Data Disposal**: Verify that third parties securely and promptly dispose of data once it is no longer required.
- ✓ **Data Accuracy**: Share only data that is accurate, reliable, legal, and appropriate for its intended purpose.
- ✓ **Data Relevance**: Limit data transfers to only what is necessary for the specific service being provided, minimizing unnecessary risk by avoiding the transmission of extraneous information
- ✓ **Data Protection**: Require third parties to protect all shared information using strong safeguards, including encryption for data at rest and in transit, ensuring only those with the correct decryption key can access the information.
- ✓ **Access Control**: Ensure that the third party enforces strict access controls by assigning roles and permissions so that only properly authorized individuals can view or handle the data.
- ✓ **Training**: Provide regular security training for staff involved in data sharing processes.

Work with the Penn Medicine procurement and contracting department to ensure these controls are contractually covered.