Security Issues:
The Duke Experience

Lawrence Whitley, Data Manager
Carl Pieper, Core Leader

As we all recognize, there are 2 sources of security issues.

External: As more examples of data security breaches are publicized nationally, the Duke Security/IRB regulations have increased disproportionately.

Internal: As the ADC protocols become more numerous and sophisticated, the need to maintain structure to protect data, particularly PHI data, increases.

External

Duke Security and the IRB have become increasingly aware and more vigilant about security.

Our protocols have moved from Pencil/Paper to
(1) Web Based Collection
(2) Electronic Data Capture (EDC) systems
(3) Eventually, we plan to move to a touchpad-based distributed Client data collection system.

→ Altered security issues. (e.g. paper disappears, but encryption protocols are necessary).

External.

Solutions:

- Malware, Spyware programs updated regularly.
- Windows Server Enterprise Active Directory used - file folder access and database access are all controlled using Active Directory Groups
- File Server and Database Server firewall subnet restrictions – limits the number of potential compromised PCs which can attempt to hack the servers
- Port Services turned off for unnecessary features – reduces security footprint
- Critical Windows Server Patches applied within 72 hours – resolves known security issues quickly
- Servers located inside the PHI network, not internet facing or in the DMZ – limits internet exposure

Internal

Our Center has seen an increase in:

1) # of Protocols
2) # of protocol Consents within the ADC subject protocol
3) # researchers requesting use of the data.

Internal

Data Management Team is developing a Protocol Manager - major portions are completed

Consent drives access.

Without consent,

→ Data not collected (electronically), stored, or entered

→ Retention rules strengthened – as IRB has developed, we have had to change data storage and use for some subjects.

Consent linked to Protocol, Subject data, and Researcher.

So, the data access (e.g. read, write, restricted) is determined by the permissions allowed to the:
Researcher
Protocol
Subject

ALL DRIVEN BY CONSENT.

Internal

PHI data is stored in a separate database for maximum security control
→ Components or Whole database could be encrypted.

Unless the particular Protocol requires it, only de-identified data are analyzed.