Guide to Security of Clinical Research Data Sets – January 2014

From a risk management perspective there are at least three categories of research projects. Each requires a different approach to information security. The IRB is in the best position to categorize these projects and ensure that investigators understand how to handle each approach:

	Type of project	Principal risks	Controls
1	*Small scale* – generally fewer than 500 research subjects and 5 researchers. Use spreadsheets and small databases primarily. No server application, although files may be shared on file servers among researchers	Lost or stolen unencrypted laptop Lost or stolen unencrypted media Unauthorized access to file shares Unencrypted communications outside the JH network Lost or stolen unencrypted desktop	Every project requires an inventory of private data and an access control list (ACL) to those data. These are embodied in a short ***data management plan***. Risk mitigation can involve eliminating SSN or otherwise de-identifying. Most security breaches of this type can be mitigated by ensuring that data are stored only on file shares or ***encrypted devices***. The PI should require that the team identify machines storing data and ensure that full-disc encryption is in place. For Mac's that means FileVault and for corporate Windows 7 (Bitlocker) and personally owned devices (Checkpoint or TrueCrypt). File sharing tools should be Hopkins-managed or approved. And we recommend ***file shares*** and ***virtual desktops*** as the appropriate settings for sensitive files. Small scale projects should complete the ***Research Security Checklist*** (Item 5. http://www.it.johnshopkins.edu/policies/risk.html).
2	*Medium scale* – these projects resemble their smaller peers yet have greater risk because the number of research subjects or researchers is larger. The second factor is especially important as the number of sharing interactions is likely to be much greater than in 1 above.	Lost or stolen unencrypted laptop Lost or stolen unencrypted media Unauthorized access to file shares Unencrypted communications outside the JH network Lost or stolen unencrypted desktop Insecure file share technologies	All of the controls from above are critical. The principal difference here is that medium scale projects require more attention to complete and updated ***access control lists*** and ***file-sharing*** mechanisms. The team should designate a *security manager* to ensure that the ACL is up-to-date and that approaches to file sharing are appropriate. There should be procedures and ***simple training*** to ensure that insecure sharing mechanisms such as email are avoided. Small scale projects should complete the ***Research Security Checklist*** (Item 5. http://www.it.johnshopkins.edu/policies/risk.html).
3	*Server applications* – there are additional risks for even a small project that requires a Web-based or client/server application for collecting, processing or sharing private information. Whether the tools used are developed internally	Lost or stolen unencrypted laptop Lost or stolen unencrypted back-up media In advertent publication of private data on the Web Network penetration of servers and application servers	Protecting server-based applications is hard. In most cases it requires knowledgeable technical staff and investment of planning and resources into ***analysis***, ***testing*** and ***monitoring***. PI's should commit adequate funding to ensure that these tools are implemented. All such projects must have a ***data management plan***. It should include an informal code validation process, interface tests and server monitoring plan. The ***tools*** and ***procedures*** for each should be documented and

	Type of project	Principal risks	Controls
	or not, there are best practices for managing application, database and web servers.	SQL Injection or cross-site scripting attacks Unauthorized access to application	maintained by a ***designated technical lead.*** All applications with E-PHI should be reviewed for risk and controls, see ***Johns Hopkins Risk/Controls Questionnaire for Restricted Systems*** (Item 2. http://www.it.johnshopkins.edu/policies/risk.html). For any web-facing application, researchers should also conduct a formal ***web security review*** by checking our current Web application standards (http://www.it.johnshopkins.edu/policies/standards.html). We recommend that investigators use Hopkins-managed or approved third party web services for hosting such sites. Managing user authorizations requires an access control list linked electronically to the application interface. There should be an ***access provisioning/termination procedure*** with documented procedures and a designated manager. User authentication credentials are difficult to manage and we therefore recommend ***leveraging authentication*** resources through JHED. If research subjects participate thought the web, tools such as OAuth, OpenID or Facebook Connect may be appropriate. If there are collaborators from other institutions, the project would likely fit in 4 below.
4	*Multi-site collaborations* – multi-site projects often require the most rigorous security planning and review systems and procedures. This is especially true for research "grids" and other large scale data processing systems.	Lost or stolen unencrypted laptop Lost or stolen unencrypted back-up media In advertent publication of private data on the Web Network penetration of servers and application servers SQL Injection or cross-site scripting attacks Unauthorized access to application Sophisticated network penetrations from attackers targeting research labs	All controls in 1-3 above are appropriate here. Many of the principal differences between 3 and 4 involve reconciling different security policies, authorization/authentication approaches, and organizational cultures. For this reason, ***collaboration*** and ***directed training*** are critical to success. Documentation for these types of projects can vary based on size and risk. You should complete the ***Research Security Checklist*** (Item 5. http://www.it.johnshopkins.edu/policies/risk.html) and ***Johns Hopkins Risk/Controls Questionnaire for Restricted Systems*** (Item 2. http://www.it.johnshopkins.edu/policies/risk.html). For research projects that require FISMA/NIST certification we have additional documentation available. Please contact the research office for more information on a FISMA. Further technical questions should be directed to itpolicy@jhu.edu.