From:	Gregory Culler
To:	evpr-info@lists.columbia.edu
Cc:	Purdy, G. Michael; Stiles, Deborah F.; Hescock, Halayn J.; Brenda L. Ruotolo ; Crosswell, Alan; Booth, Jane; ed2513@columbia.edu; at2059@columbia.edu; lm2906@columbia.edu; Bhalodkar, Medha R.; Shea, Steven; Sideli, Robert; lgoldman@columbia.edu
Subject:	IRB Policy Release: Data Security Plans Involving the Storage of Certain Electronic Research Data in Human Subjects Research
Date:	Tuesday, January 08, 2013 5:37:05 PM

IRB Policy Release: Data Security Plans Involving the Storage of Certain Electronic Research Data in Human Subjects Research

The IRB has released a Policy, to be effective February 1, 2013, that provides standards for IRB approval of data security plans involving the storage of certain electronic research data in human subjects research. The Policy applies ONLY to such data that constitute Protected Health Information (PHI) or Personally Identifiable Information (PII) in human subjects research conducted at Columbia University or by Columbia University researchers. The intent of this Policy is to ensure that the protection of the privacy of research subjects and the confidentiality of identifiable research data is in accord with the requirements of HHS, FDA, HIPAA/HITECH and NIH regulations.

Highlighted points from the Policy:

- Any multi-user system that will store human subject data containing PHI or PII must be assessed and certified by the CUMC IT Information Security Office (even if the research is conducted at or by a researcher submitting to the Morningside IRB).
- Any human subject data that contains PHI or PII and is stored on a desktop, laptop, tablet, smartphone, USB drive or other end user device must be protected by a strong password and be encrypted at all times. Please note that this includes any end user device, Columbia owned or personally owned, that connects to a multi-user system that contains PHI and/or PII.
- A new page is being added in the Rascal IRB Module with required questions that will assist the IRB in determining whether your protocol is subject to the Policy.
- The current list of CUMC IT certified systems can be found at https://secure.cumc.columbia.edu/cumcit/secure/security/scp_systems.html
- It is highly encouraged that researchers leverage existing certified systems by making contact with the System Owners listed on the certified systems web page. If you are a researcher who has an environment that is certified and would like to host research studies for additional PIs, please contact the CUMC IT Information Security Office so that the certification status can be confirmed and your willingness to host a compliant multi-user system can be published on the System Certification publishing website.

The Policy in its entirety can be found on the IRB's Policy and Guidance web pages:

CUMC IRB: http://www.cumc.columbia.edu/dept/irb/policies/index.html

Morningside IRB: http://www.columbia.edu/cu/irb/policies/index.html

The IRB and CUMC IT will be hosting several sessions to discuss the Policy. Please join us so that we can help answer any questions that you may have regarding the Policy.

Sessions on the Morningside Campus:

- Jan. 17th, 2:00 to 3:00 pm, Studebaker 367
- Feb. 14th, 1:30 to 2:30 pm, Low Library 212

Sessions on the CUMC Campus (Ampitheatre 7):

- Jan. 24th, 3:30 to 4:30 pm
- Feb. 21st, 3:30 to 4:30 pm

If you have any questions regarding multi-user systems, the CUMC IT certification program or encryption, please send an email to security@mail.cumc.columbia.edu.

If you have any questions regarding the Policy, please send an email to: irboffice@columbia.edu (Medical Center IRB) or askirb@columbia.edu (Morningside IRB).