Thank you, Dixie. I had a few questions regarding these policies that I thought I’d send before the meeting:

1) With regard to the Email, Internet and Telephonic Communications Employee Acknowledgement, it states that all information transmitted by, received from or stored by the MCHS electronic systems are the property of MCHS. Am I correct in then concluding that if a research colleague sends me data from their study via my clinic email (hence, automatically stored on MHCS email servers), MCHS then claims that this data is property of MCHS? Am I also correct in concluding that if I download publicly-available data, for example the Federally-funded 1000 Genomes sequence data, that MCHS claims that these data are the property of MCHS? In the former example, it seems contrary to normal research practices to claim ownership over data collected from an external study. In the latter example, this seems to contradict the 2013 US Supreme Court Association for Molecular Pathology v. Myriad Genetics decision where it specifically states that DNA sequence data existing alone in nature is unpatentable and not property of any institution or corporation. Additionally, it appears to contradict NIH policy which states that these molecular data and calculations performed on those data must remain publicly-available and are not property of individuals nor institutions.

2) With regard to the Computer and Network Access Agreement, it states that research data is to remain confidential and may only be accessed for specified job duties. Does this prohibit publication of research data?

3) With regard to the Cloud Services Acceptable Use policy, internet-based email systems (e.g., Gmail) are considered cloud services. To transfer documents not containing sensitive or protected data to a cloud service will require a request via electronic form and approval. Am I correct in concluding that each time I want to transfer a presentation or PHI-free document (say, a manuscript) to a colleague who uses a Gmail or Hotmail address, I need to submit an electronic form and obtain approval prior to doing so?

4) With regard to the Cloud Services Acceptable Use policy, are the definitions of protected and sensitive data specific to data collected outside United States? As HIPAA was enacted by the US Congress to cover US data, the jurisdiction of HIPAA extends to US data—other countries have their own sets of laws governing data collected outside the US. The Federally-funded repositories from the National Center for Biotechnology Information (NCBI) clearly have taken the position that the laws enacted from foreign governments governing data collected in foreign countries prevails. For example, the following are two examples of “protected or sensitive data” (birthdays with year, month and day) linked to clinical information on the publicly-available NCBI website collected within foreign countries:

https://www.ncbi.nlm.nih.gov/geo/query/acc.cgi?acc=GSM1116511

https://www.ncbi.nlm.nih.gov/geo/query/acc.cgi?acc=GSM198783

It appears as though our MCHS Transnational Policy prohibits interaction with these data without IRB oversight:

From the Marshfield Clinic Transnational Policy:

“Engagement in TNR occurs when a researcher: directly interacts with an international participant, or their identifiable data for research purposes; or is responsible for the conduct of the research at an international site”

“IRB oversight is necessary before an employee of Marshfield Clinic Health System (or an institution for which MCRI IRB is the IRB of record) becomes engaged in TNR.”

Thank you. I believe a high degree of clarity on these policies will serve to ensure complete compliance,

Steve