

MAY 2012

THIS ISSUE

Announcing: The Honest Broker System for Data and Specimens	1
When is medical record pre-screening a research procedure?.....	2
Information Security and Research	3

Announcing: The Honest Broker System for Data and Specimens

Pearlanne Zelarney, MS, Research Data Curator
Ted Wade, PhD, Principal Investigator, Honest Broker System

Honest Broker services allow data and tissue to be used in research while still protecting the confidentiality of research study participants. The National Jewish Health Research Database (RDB) and Biobank already act as an automated Honest Broker Service. The RDB removes personal health identifiers from data/samples and ensures that when they are given to a researcher, it will be very difficult for the researcher to identify the patients directly or indirectly. This process differs from data/sample anonymization in that honest brokers retain a linkage code and are able to provide updated information to the researchers in a de-identified fashion.

When data or samples not normally found in the RDB or the Biobank are necessary for research, an honest broker can provide these data/samples on an individual basis in either a de-identified (all identifiers removed) or a limited data set (dates included) manner. The honest brokers will also work closely with the NJH Human Live Cell Core to provide live cells from donors in a de-identified manner. Researchers will be able to request live cells from donors with broadly defined phenotypes and then, at a later date, use the RDB to further phenotype the subjects.

Both the RDB as an automated honest broker and the honest brokers listed below serve as a well-defined barrier between the research community and protected health information (PHI) collected as part of patient care, thus ensuring confidentiality.

Research on data provided to you by our certified honest brokers ***might qualify as non-human subject research and so not need to be reviewed by the IRB.*** The Service can make this determination for you upon request.

Continued on next page...

CONTACT US

National Jewish Health
Institutional Review Board
1400 Jackson Street
Room M211
Denver, CO 80206-2761

Phone: 303.398.1477
Fax: 303.270.2292

nationaljewishIRB@njhealth.org

Information Security and Research

Bill Hubbard, MA, GISP, GSEC, Security Administrator

Medical research and clinical trials involving human subjects are valuable in finding anything from causal relationships to potential cures for ailments and diseases; National Jewish Health has a tremendous history of success for a variety of medical advances that were assisted by human related medical research. It behooves us, as medical caregivers, to also remember the importance of protecting data and computer systems we use to achieve these medical advances.

The core concepts of Information Security are to mitigate risk to the confidentiality, integrity, and availability of data and systems, and to ensure the business succeeds. In regards to medical research, there are several ways we can work toward these goals, as we are required to do so under HIPAA regulations.

Why do we need to take these steps to protect PHI? Accidents can happen as easily as malicious activity. We, as users, could inadvertently overwrite or erase data. We could store it on a personal device and lose that device, or have it stolen from us. We could accidentally expose PHI on a publically accessible webpage, or fail to encrypt it when sending it over the Internet. All of these mistakes have happened to many organizations and medical institutions.

PHI has also been compromised via criminal behavior: theft of equipment, theft of paper records, unauthorized access to data, or even system compromises via virus or computer intrusions. To date, millions of individuals have been affected by medical entity PHI related compromises, from both malicious activity and accidental disclosure. So how can we help mitigate risk to data and systems we are entrusted with?

First, we need to ensure only authorized personnel have access to confidential data, especially protected health information (PHI). This means

using individual login credentials to systems, not sharing passwords, and making sure managers or business owners have authorized access to confidential data for business needs. This also entails ensuring stored data is accessible only by authorized people. For example, it is much easier to secure PHI on protected network shares and in encrypted backups than on personally owned memory sticks, computers, or cloud storage.

Securing data also means protecting the systems on which the data resides. This means keeping systems up to date on operating system and application patches whenever possible, keeping anti-virus programs current and running, and limiting what other systems or people can access those systems that store, process, or transmit PHI.

Lastly, while following policies and procedures are essential, we also need to use common sense. When using or accessing PHI, ask yourself if the risk involved is low. How likely is it that something could go wrong, or the confidential data get exposed? Can you lower the risk by being more careful about your login credentials? How about limiting access to appropriate staff, or perhaps create a more secure workflow around the data itself?

We need to protect PHI and confidential data not just because it's the law; it's also part of our responsibility as healthcare professionals. Our knowledge, experience and behavior are crucial for not only creating successful research studies, it is also crucial for protecting the systems and confidential data that allows us to perform our research in the first place.

For more information, contact:

Bill Hubbard
hubbardb@njhealth.org
303-398-1829