



University at Buffalo
The State University of New York
School of Public Health and Health Professions

POPULATION HEALTH OBSERVATORY



“Dedicated to improving health through population based research.”

SUNY BUFFALO PHO DATA SYSTEM SECURITY PROTOCOL

September 7, 2016

Introduction

The Population Health Observatory (PHO) is a data science research and training center in the School of Public Health and Health Professions (SPHHP). It is staffed primarily by faculty, staff, and students with affiliations with the Department of Biostatistics in the SPHHP. The interdisciplinary research environment involving the PHO and the Department of Biostatistics is very strong. Teams of researchers are formed that include all the multidisciplinary expertise required for each project, and administrative units support these teams. For example, the UB Division of Nephrology and the Department of Biostatistics are currently collaborating under an MOU that supports the recently developed collaboration between Dr. Carter, former director of the PHO and Professor Emeritus, and Nephrology faculty at the Western New York VA and in the UB Department of Family Medicine. It is recognized that the fusion of expertise in biostatistics, nephrology, informatics, and family medicine is needed to produce future advances in the clinical care of CKD patients. This type of cooperation between administrative units enhances the probability of success of the current project and ensures support for follow-up translational work to develop and test strategies for improved clinical care based on the metrics to be developed. Other PHO collaborations follow a similar model of collaborative teamwork that brings the power of data science to health services, health science, and public health investigations that involve Big Data or other quantitatively challenging issues. We are a one-stop-shop for data storage, management, integration, and analysis of large or otherwise challenging databases.

PHO Data Warehouse

Being informatics intensive, our work requires the involvement of staff with expertise in biostatistics and informatics. PHO staff provide data management and data analysis support for project work under Dr. Yu's direction. The PHO is a HIPAA- and FERPA-compliant public health research and informatics center that maintains a data warehouse and data management and analysis system to store, manage, and analyze sensitive data. Databases are well documented by data dictionaries, codebooks, and dataset documentation forms. The PHO data warehouse is maintained on a Dell server that is owned and maintained by SPHHP IT and hosted by Central UBIT. The server has a storage capacity of 7 terabytes with 3.5 terabytes currently available. Storage capacity is scalable and therefore is guaranteed to meet all PHO data warehousing needs.

Physical and Environmental Security of Equipment

The server runs MS Server 2008 and is located securely in the University's CLUB server room, a physically secured interior room with strict environmental controls. Swipe card access to the CLUB Room is required 24/7 for first level entry. A second level of entry requires a password and is alarm protected. The server is locked in a rack for which only two SPHHP IT professionals have keys. Video cameras track traffic around the building and in the internal hallways leading to the CLUB Room. The server runs Symantec Endpoint Protection software for antivirus and firewall protection against intrusions. Two SPHHP IT staff and hundreds of Central UBIT staff provide vulnerability and intrusion detection monitoring. Data are backed up daily to three physically separate sites by Central UBIT. Backups are confirmed by automated email to two SPHHP IT professionals. IBM Trivoli Storage Manager (TSM) is used for data recovery, with duplicate TSM servers at each of the three back up locations. Full disaster recovery within 2-4 hours has been tested and proven with complete server restore. Central UBIT creates all new employee accounts (UBIT name and password) when new hires arrive. Once created, requests for new user accounts to gain permission to the SPHHP servers will be made in writing to the SPHHP IT staff; each request should specify the access level desired for its corresponding account, and should include the usual: name, contact person, and e-mail, as well as other relevant information.

Upon the acceptance of a request and approval by Dr. Yu, the SPHHP IT staff will add an account based on the specifications supplied by the requester. When the new user logs in with their UBIT name and password, access to the requested and approved PHO folder will be available on the K Drive. The data for each project are securely stored and analyzed separate from all other projects and only project staff are authorized to access project data. PHO employees are only allowed to access data as needed to meet project objectives. The warehouse is invisible to all others. All data network connections are dual-linked providing redundancy and essentially guaranteeing 24/7 access to authorized users, and only authorized users. Local support of PHO computers is provided by SPHHP IT professionals. All PHO staff and faculty are regularly retrained in HIPAA regulations.

All project personnel have access to additional high-performance computing resources through the Center for Computational Research (CCR), a leading academic supercomputing facility. The CCR maintains a high-performance computing environment, high-end visualization laboratories, and support staff with expertise in scientific computing, software engineering, parallel computing, grid computing, visualization, advanced database design, and networking.

Physical Security of Records

The physical security of records must be maintained in order to prevent unauthorized access. The following protocol for closing up at the end of each work day will be followed:

- lock all records, memoranda, and documents with confidential data in the storage cabinets
- lock the door to the offices
- issue keys only to individuals who have authorized access to the designated security zone

Security Training

PHO staff will be trained on security and confidentiality procedures before data collection and analysis commences. This training will encapsulate HIPAA regulations. Subsequent to the training, all data collection and analysis operations will be performed according to the security and confidentiality training received. Any further training requested by PHO partners will be evaluated and considered.