Attachment 8: Confidentiality Procedures

DATE: April 25, 2010

TO: Susan Yurgalevitch, Westat

FROM: Tim Church, Ph.D., Principal Investigator

SUBJECT: OMB Submission for Prostate, Lung, Colorectal and Ovarian (PLCO)
Cancer Screening Trial

The University of Minnesota Assurance of Compliance number is FWA00000312.

Participants in the study are informed in writing that all information regarding their participation is kept private under the Privacy Act, that no written report identifies individuals and that data are published in aggregate form only without any personal identifiers. To assure privacy, we provide secure office space for the storage of study records. The doors are locked at all times and additional building security is in place during the evening and weekends. Access to study files is limited to authorized study personnel only and study files are stored in locked file cabinets or locked file rooms.

The operations and research computer system currently supporting databases maintained for PLCO by the Environmental Health Sciences Health Studies Section is comprised of multiple servers to support file, web, database, mail, application, print and statistical services. Server operating systems are MS Windows 2003 Server, Linux. Desktop systems are MS Windows XP. The entire server system has complete local backup facility and offsite media storage. Servers are housed in an engineered computer room internal to our space with 24x7 keycard controlled access. Internal and external network connections, wiring, routers and firewalls are provided by the University's Networking and Telecommunications Services (NTS). External connections, ports and services are minimized and monitored. System and applications software is kept current and patched on a daily basis. All Linux, MS Windows and Web access is authenticated through individual domain accounts.

Requests for accounts are made by a local authorized staff member, with copies to Systems Manager, Systems Administrator(s), and Study Coordinator. Accounts are closed immediately when staff members depart. NTS has extensive security systems in place to protect the intra-campus internet and NTS provide regular oversight of our systems through activity monitoring, port scanning and periodic site visits. System event and security logs are retained and reviewed daily by system managers.

All University of Minnesota staff members are compliant with our institutional IRB, HIPAA and privacy and data security requirements. Training is thorough, ongoing and recorded. Staff members also complete NIH IRB training