MPOG DataDirect
Security Checklist and Authorization Form

Thank you for your interest in using MPOGs DataDirect application for Quality Improvement and/or Research Projects at your institution. DataDirect contains limited dataset (protected health information is excluded except for date of service). However, because DataDirect may contain information regarding hospital level quality indicators (i.e. hospital mortality), we ask that approval from the appropriate hospital department (i.e. Quality or Health Information Management) is obtained.

Standard data security processes must be followed when using the application. These are detailed below.

The site's Anesthesiology Quality Champion and/or Practice Leader is responsible for all of the data that is downloaded for their institution from DataDirect. All individuals gaining access to MPOG DataDirect will need to complete and sign the affidavit below. This affidavit affirms that he/she understands the necessary processes and policies to ensure data security. Detailed descriptions of all items on the checklist can be found on the MPOG Security

Use of this data for Research

Anyone downloading data using Data Direct for the purpose of research should follow their institution review board policies.

Please do not hesitate to contact the MPOG with any questions/concerns.

Secure Computer

- Encrypt all mobile workstations (laptops): encrypt computer hard drive using approved tools (described on MPOG website)
- Ensure physical security or encryption of any desktop workstations
- Ensure physical security of servers: Institutional server room with near zero risk of physical theft

Install up to date antivirus programs and strong passwords

- Windows Antivirus Programs:
  - Norton Antivirus
  - Windows Antivirus : Such as Microsoft Security Essentials or commercially available product: http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx
- Mac OS Antivirus Programs:
  - Norton Antivirus
  - ClamXAV (free)
  - McAfee
- Create strong login passwords, not automatic at login (8 characters with 1 capital and 1 number)

Securing Files

- Encrypt and password protect files (Microsoft Excel 2010 or higher, SPSS 21 or higher, ZIP, or RAR)

MPOG DataDirect
Security Checklist and Authorization Form

Sharing File: Use MiShare or secure file-sharing ONLY

- Never share using a portable USB flash drive
- Never store files on public workstations
- Never store files on an unencrypted laptop
- Never store files on a home/personal desktop
- Never store files on a physically unsecured work desktop
- Never store files on Google Drive, Dropbox, or other unapproved web-based file storage systems
- Share files with other institutions using your institutions approved file sharing system (ie MiShare for University of Michigan users. It okay to run files on your computer as long as you have encrypted your hard drive

Authorization

I authorize the use of MPOG DataDirect for quality improvement and/or approved research projects by users who have completed and signed the MPOG DataDirect affidavit.

Authorized Hospital Leader Signature and Printed Name	Date
Role	Institution

Affidavit for MPOG DataDirect Use

I certify that I will:

Ensure computers are secure

- Encrypt all mobile workstations (laptops): encrypt computer hard drive using approved tools (described on MPOG website)
- Ensure physical security or encryption of any desktop workstations
- Not use file/folder encryption in place of hard drive encryption and I know they are not equivalent

Install up to date antivirus programs and strong passwords

Windows Antivirus Programs:

- Norton Antivirus
    - Windows Antivirus : Such as Microsoft Security Essentials or commercially available product: http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx
    - Mac OS Antivirus Programs:
        - Norton Antivirus
        - ClamXAV (free)
        - McAfee
- Create strong login passwords, not automatic at login (8 characters with 1 capital and 1 number)

Secure Files

- Encrypt and password protect files (Microsoft Excel 2010 or higher, SPSS 21 or higher, ZIP, or RAR)

Use Secure Sharing File: Use MiShare or other secure file-sharing ONLY

- Never share using a portable USB flash drive
- Never store files on public workstations
- Never store files on an unencrypted laptop
- Never store files on a home/personal desktop
- Never store files on a physically unsecured work desktop
- Never store files on Google Drive, Dropbox, or other unapproved web-based file storage systems
- Share files with other institutions using your institutions approved file sharing system (ie MiShare for University of Michigan users. It okay to run files on your computer as long as you have encrypted your hard drive
- Not E-mail PHI
- Not give PHI to statistical staff

Affidavit for MPOG DataDirect Use

Off Boarding Processes

- Destroy the data if I leave the MPOG project or institution for which I am working
  - Delete files
  - Empty recycle bin
  - Shred any paper files
- Destroy distributed copies of the data (on research assistant workstations, etc) and maintain only one centralized dataset when the project is completed
- Employ an "off-boarding" process to confirm that data is deleted when a user leaves the project team

I attest that I understand all the PHI security guidelines and will follow them. As a collaborator, I am responsible for the conduct of all members of my team.

DataDirect User Signature	Date
DataDirect User Name	Institution