



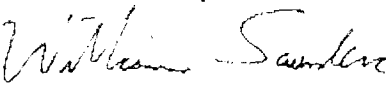
DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

7500 Security Boulevard  
Baltimore, MD 21244-1850

Date: July 7, 2006

To: Individuals with Current Data Use Agreements

From: William D. Saunders   
Deputy Director, Office of Research, Development, and Information

Subject: Privacy and Security Reminder

The Centers for Medicare & Medicaid Services (CMS) wants to remind you of your obligation to follow all Federal laws and CMS requirements regarding confidentiality, disclosure and use of personally identifiable and proprietary information (See Data Use Agreements, Privacy Act and/or Privacy Rule.)

Data and information are to be used only for the purpose(s) approved in your data use agreement. You are required to have appropriate administrative, physical, and technical safeguards in place to protect confidentiality, integrity and availability of protected information. It is critical that these safeguards include laptop computers and/or removable storage containing individually identifiable information if used for CMS project work. Laptops and removable storage ("thumb drives," external hard drives, CD-ROMs, etc.) are particularly vulnerable to theft and loss. Even computer servers and desktop computers are susceptible to theft. We expect that you will use passwords, personal identification numbers (PINs), user identification names, biotechnology (like retinal or fingerprint scans), or digital signatures or smart tokens technology to assure that only authorized persons can access information/data. You should remove private information that you don't need to do your job from your lap top and/or removable storage. If you must use personally identifiable information, that data should be encrypted in a way to ensure that it won't be accessible and usable by unauthorized persons. CMS intends to expand the use of data encryption for data security on data files that are provided to you. You should not access private information using a web browser on a public computer, such as at a library, hotel, or internet café. If you do access private information using a web browser, be sure to "clean up" any temporary files created during your use of that computer. In the course of an internet session, web browsers like Internet Explorer create temporary files to store the graphics and data that are displayed on your screen. Many of these temporary files can remain on your computer after you walk away, which can be a problem if you have accessed private information.

You should perform an internal and external risk assessment to identify and address vulnerabilities. Weaknesses or gaps in your security program should be quick remedied. Your organization should train its staff annually on responsibilities and consequences of failing to secure and protect personally identifiable and proprietary information. In addition, you should notify CMS immediately if you find or suspect any security breach involving personally identifiable information. You also are required to return or destroy all individually identifiable information once your data use agreement expires.

We don't think of these steps as "nice to do" actions. They are your responsibilities, and are found in various laws, regulations and policies, and there are penalties for non-compliance. We consider breaches of security and privacy evidence that you are non-compliant with the terms of your data use agreement. Failure to follow the terms of CMS data use agreements could lead to termination of systems access privileges and/or adverse action up to and including criminal penalties.

Thank you for your efforts and your attention and action in the important task of protecting personally identifiable information.