



# TMA Privacy and Civil Liberties Office Information Paper



## BEST PRACTICES FOR SAFEGUARDING LAPTOPS

HIPAA Privacy ♦ March 2011

### **I. Supporting Policies for this Information Paper**

- A. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR Parts 160 and 164) sets forth the requirements for uses and disclosures of protected health information (PHI).
- B. The Department of Defense Health Information Privacy Regulation (DoD 6025.18-R) implements the HIPAA Privacy Rule within the Military Health System (MHS).
- C. The DoD Health Privacy Program Regulation (DoD 5400.11-R) sets forth the requirements for protecting and safeguarding an individual's privacy when collecting, maintaining, using, or disseminating personally identifiable information (PII).
- D. The DoD Health Information Security Regulation (DoD 8580.02-R) implements the HIPAA Privacy Rule within the MHS with regards to the security of PII and PHI.

### **II. Definitions Associated with Best Practices for Laptop Security**

- A. Breach: The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for another than authorized purposes where one or more individuals will be adversely affected.
- B. Military Health System (MHS): All DoD health plans and all DoD healthcare providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by TMA, the Army, the Navy, or the Air Force.
- C. Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual.

- D. Protected Health Information (PHI): Information that is created or received by a covered entity and relates to the past, present, or future physical or mental health of an individual; providing payment for healthcare to an individual; and can be used to identify the individual. It excludes health information in employment records held by a covered entity in its role as employer.
- E. Safeguards: Administrative, physical, and technical actions, measures, policies, and procedures to protect impermissible uses and disclosures of PII and PHI.

### **III. Guidance Regarding Best Practices for Laptop Security:**

Laptops are highly susceptible to loss or theft; therefore, they may be vulnerable to information assurance threats. Employees must be vigilant about protecting laptops and safeguard the information on them. The following are tips and reminders that could help prevent a laptop from being lost or stolen.

- A. Treat your laptop like your wallet. Keep a careful eye on your laptop just as you would your wallet.
- B. Know what data you're transporting. Always know what data you have on your laptop and do not store PII and PHI on laptops or removable storage devices unless authorized. Be prepared to report what data you had stored on your laptop in the event that it's lost or stolen. Keep tabs of any personal data you had on the device, as well, to help mitigate potential cases of identity theft.
- C. Log off. Make it a practice to fully log off your laptop and always remove your Common Access Card (CAC) when the laptop is not in use.
- D. Keep your passwords secure. Passwords should not be written down, yet remembering strong passwords or access numbers can be difficult. However, leaving either in a laptop carrying case or on your laptop is like leaving your keys in your car. If you have written them down, do not store your passwords in the same location as your laptop.
- E. Be aware of your surroundings. When possible, perform work on the laptop in areas under your control and where authorized. Avoid operating the laptop in public places, but when necessary, be aware of your surroundings. Pick an area to work where you have some privacy and don't have to worry about someone looking over your shoulder.
- F. Keep it out of the car. Avoid leaving your laptop in the car. If you must leave it behind in the car, ensure that the car is locked and keep the laptop out of sight. Place it in the trunk and/or hidden under other items.
- G. Keep it locked and out of sight. Whether you're using your laptop in the office, a hotel, or some other public place, a security device can make it more difficult for someone to steal it. Use a laptop security cable and attach it to something immovable or to a heavy piece of furniture. If you don't have a security cable, secure your laptop by locking your office door or by placing it in a locked, secure file cabinet. If you're staying in a hotel, store the laptop in the hotel room safe, if it fits, or keep it well hidden and out of sight.
- H. Pay attention in airports. Always take your laptop as carryon, never as checked baggage. Keep an eye on your laptop as you go through security. Hold onto it until the person in front of you has gone through the metal detector. The confusion and shuffle of security checkpoints provides opportunity for theft.

- I. Keep it off the floor. Whether eating at a coffee shop, attending a conference, at a registration desk, or on public transportation – avoid putting your laptop on the floor. If you must put it down, place it between your feet or up against your leg so that you’re aware of it.
- J. Secure your home network. Make sure your home network is secured with a password. Do not leave it open. Consider unplugging your wireless router when it is not in use. In addition, be wary of using free public wireless connections often available in airports and public locations. Your data could potentially be breached without your knowing.
- K. Beware of viruses. Government-furnished laptops are well-equipped by Information Assurance with the proper security controls configured to provide protection for the information on our laptops. Do not attempt to circumvent these controls. Remember, downloading or installing unauthorized software opens your laptop up to viruses and malware.
- L. Reconnect to the TMA network often. If your laptop has been offline for an extended time, take it back to the office periodically for direct connection to the TMA network. Doing so provides opportunity to ensure all software and protections are current.

#### **IV. Reporting Procedures for Lost, Missing, or Stolen Laptops**

- A. Promptly file a police report if your laptop is lost or stolen. Contact TMA Network Operations at (703) 824-8605 and make arrangements to provide a copy of the police report to them.
- B. For instances of missing laptops that contain PII and/or PHI, the following actions are required:
  - 1. Notify your supervisor immediately upon discovery. If the supervisor is unavailable, contact your Director.
  - 2. Notify United States-Computer Emergency Readiness Team (US-CERT) within one hour: <http://www.forms.us-cert.gov/report/>.
  - 3. Report the breach to the TMA Privacy and Civil Liberties Office within one hour, even though encryption is enabled: [PrivacyOfficerMail@tma.osd.mil](mailto:PrivacyOfficerMail@tma.osd.mil).
  - 4. The TMA Breach Reporting Form is located on the TMA Privacy and Civil Liberties Office web site at: <http://www.tricare.mil/tma/privacy/breach.aspx>.