# Appendix H: Resources for Secure Remote Use and Access

The HIPAA Security Rule requires all covered entities to protect the EPHI that they use or disclose to business associates, trading partners, or other entities. New technologies, such as remote access and removable media technologies, have significantly simplified the way in which data is transmitted throughout the healthcare industry and created tremendous opportunities for improvements and greater efficiency in the healthcare space. However, these technologies have also increased the risk of loss and unauthorized use and disclosure of this sensitive information. Sensitive information that is accessed by, stored on, or transmitted to or from a remote device needs to be protected so that malicious parties cannot access or alter it. An unauthorized release of sensitive information could damage the trust in an organization, jeopardize its mission, or harm individuals if their personal information has been released.

In December 2006, CMS issued a HIPAA security guidance document, *Remote Use of and Access to Electronic Protected Health Information*, to reinforce some of the ways a covered entity may protect EPHI when it is accessed or used outside of the organization's physical purview. It sets forth some strategies that may be reasonable and appropriate under the HIPAA Security Rule, for covered entities to follow (based upon their individual technological capabilities and operational needs), for offsite use of, or access to, EPHI. This guidance also places significant emphasis on the importance of risk analysis and risk management strategies, policies and procedures, and security awareness and training on the policies and procedures for safeguarding EPHI during its remote access, storage, and transmission.

NIST publications on remote access, storage, and transmission security technologies can be valuable resources to support secure remote use solutions. These publications seek to assist organizations in understanding particular technologies and to provide security considerations and practical, real-world recommendations for implementing and securing these technologies within an organization.

Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, was developed to help teleworkers secure the external devices they use for telework, such as personally owned and third-party privately owned desktop and laptop computers and consumer devices (e.g., cell phones, personal digital assistants). The document focuses specifically on security for telework involving remote access to organizations' nonpublic computing resources by providing:

- Recommendations for securing telework computers' operating systems and applications, as well as home networks that the computers use;
- Basic recommendations for securing consumer devices used for telework;
- Advice on protecting the information stored on telework computers and removable media; and
- Tips on considering the security of a device owned by a third party before deciding whether it should be used for telework.

Special Publication 800-113, *Guide to SSL VPNs*, assists organizations in understanding SSL VPN technologies and in designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. This publication intends to help organizations determine how best to deploy SSL VPNs within their specific network environments by:

- Describing SSL and how it fits within the context of layered network security;
- Presenting a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments; and
- Comparing SSL VPN technology with IPsec VPNs and other VPN solutions.

Special Publication 800-77, *Guide to IPsec VPNs*, assists organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical guidelines on implementing security services based on Internet Protocol Security (IPsec). This publication intends to help organizations determine how best to deploy IPsec VPNs within their specific network environments by:

- Discussing the need for, and types of, network layer security services and how IPsec addresses these services;
- Providing a phased approach to IPsec planning and implementation that can help in achieving successful IPsec deployments;
- Providing specific recommendations relating to configuring cryptography for IPsec;
- Using a case-based approach to show how IPsec can be used to solve common network security issues; and
- Discussing alternatives to IPsec and under what circumstances each may be appropriate.

Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS)*, provides guidelines on the selection and implementation of the TLS protocol while making effective use of Federal Information Processing Standards (FIPS)-approved cryptographic algorithms. TLS provides a mechanism to protect sensitive data during electronic dissemination across the Internet. This guideline:

- Describes the placement of security in each layer of the communications protocol stack, as defined by the OSI Seven Layer Model;
- Provides criteria for developing specific recommendations when selecting, installing and using transport layer security; and
- Discusses client implementation, server, and operational considerations.

Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, assists organizations in understanding storage encryption technologies for end user devices and in planning, implementing, and maintaining storage encryption solutions. The types of end user devices addressed in this document are personal computers (desktops and laptops), consumer devices (e.g., personal digital assistants,

smart phones), and removable storage media (e.g., USB flash drives, memory cards, external hard drives, writeable CDs and DVDs). This publication:

- Provides an overview of the basic concepts of storage encryption for end user devices;
- Provides guidelines on commonly used categories of storage encryption techniques (i.e., full disk, volume and virtual disk, and file/folder), and explains the types of protection they provide;
- Discusses important security elements of a storage encryption deployment, including cryptographic key management and authentication; and
- Examines several use cases which illustrate multiple ways to meet most storage encryption needs.

Draft Special Publication 800-124, *Guidelines on Cell Phone and PDA Security*, provides an overview of cell phone and personal digital assistant (PDA) devices in use today and offers insights for making informed information technology security decisions regarding their treatment. This publication:

- Presents an overview of handheld devices and discusses associated security threats and technology risks;
- Examines the security concerns associated with handheld devices; and
- Discusses user- and organization-oriented measures and safeguards available for mitigating the risks and threats.

All NIST publications are accessible on the public Computer Security Resource Center (CSRC) Web site at http://csrc.nist.gov.

# Appendix I: Telework Security Considerations

Many people *telework*, which is the ability for an organization's employees and contractors to conduct work from locations other than the organization's facilities. Teleworkers use various devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDAs), to read and send email, access Web sites, review and edit documents, and perform many other tasks. Most teleworkers use *remote access*, which is the ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities. Organizations have many options for providing remote access, including virtual private networks, remote system control, and individual application access (e.g., Web-based email).

This appendix provides considerations and tips for securing external devices used for telework and remote access. More detailed information on this topic is available in NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*.

**Before teleworking, users should understand their organization's policies and requirements, as well as appropriate ways of protecting the organization's information that they may access.**

Teleworkers should consult their organization's policies and requirements to provide adequate security to protect the organization's information. Sensitive information that is stored on, or sent to or from, external telework devices needs to be protected so that malicious parties can neither access nor alter it. An unauthorized release of sensitive information could damage the public's trust in an organization, jeopardize the mission of an organization, or harm individuals if their personal information has been released.

**Teleworkers should ensure that all the devices on their wired and wireless home networks are properly secured, as well as the home networks themselves.**

An important part of telework and remote access security is applying security measures to the personal computers (PCs) and consumer devices using the same wired and wireless home networks to which the telework device normally connects. If any of these other devices become infected with malware or are otherwise compromised, they could attack the telework device or eavesdrop on its communications. Teleworkers should also be cautious about allowing others to place devices on the teleworkers' home networks, in case one of these devices is compromised.

Teleworkers should apply security measures to the home networks to which their telework devices normally connect. One example of a security measure is using a broadband router or firewall appliance to prevent computers outside the home network from initiating communications with telework devices on the home network. Another example is ensuring that sensitive information transmitted over a wireless home network is adequately protected through strong encryption.

**Teleworkers should consider the security state of a third-party device before using it for telework.**

Teleworkers often want to perform remote access from third-party devices, such as checking email from a kiosk computer at a conference. However, teleworkers typically do not know if such devices have been secured properly or if they have been compromised. Consequently, a teleworker could use a third-party device infected with malware that steals information from users (e.g., passwords or email messages). Many organizations either forbid third-party devices to be used for remote access or permit only limited use, such as for Web-based email. Teleworkers should consider who is responsible for securing a third-party device and who can access the device before deciding whether or not to use it. Whenever possible, teleworkers should not use publicly accessible third-party devices for telework, and teleworkers should avoid using any third-party devices for performing sensitive functions or accessing sensitive information.

### Secure a Telework PC

Teleworkers who use their own desktop or laptop PCs for telework should secure their operating systems and primary applications.

- Use a combination of security software, such as antivirus and antispyware software, personal firewalls, spam and Web content filtering, and popup blocking, to stop most attacks, particularly malware;
- Restrict who can use the PC by having a separate standard user account for each person, assigning a password to each user account, using the standard user accounts for daily use, and protecting user sessions from unauthorized physical access;
- Ensure that updates and patches are regularly applied to the operating system and primary applications, such as Web browsers, email clients, instant messaging clients, and security software;
- Disable unneeded networking features on the PC and configure wireless networking securely;
- Configure primary applications to filter content and stop other activity that is likely to be malicious;
- Install and use only known and trusted software;
- Configure remote access software based on the organization's requirements and recommendations; and
- Maintain the PC's security on an ongoing basis, such as changing passwords regularly and checking the status of security software periodically.

### Secure consumer devices used for telework, such as cell phones, PDAs, and video game systems

A wide variety of consumer devices exists, and security features available for these devices also vary widely. Some devices offer only a few basic features, whereas others offer sophisticated features similar to those offered by PCs. This does not necessarily imply that more security features are better; in fact, many devices offer more security features because the capabilities they provide (e.g., wireless networking, instant

messaging) make them more susceptible to attack than devices without these capabilities. General recommendations for securing telework devices are as follows:

- Limit access to the device, such as setting a personal identification number (PIN) or password and automatically locking a device after an idle period;
- Disable networking capabilities, such as Bluetooth, except when they are needed;
- Use additional security software, such as antivirus software and personal firewalls, if appropriate;
- Ensure that security updates, if available, are acquired and installed at least monthly, or more frequently; and
- Configure applications to support security (e.g., blocking activity that is likely to be malicious).

**Secure Information**

- Use physical security controls for telework devices and removable media. For example, an organization might require that laptops be physically secured using cable locks when used in hotels, conferences, and other locations where third parties could easily gain physical access to the devices. Organizations may also have physical security requirements for papers and other non-computer media that contain sensitive information and are taken outside the organization's facilities.
- Encrypt files stored on telework devices and removable media such as CDs and flash drives. This prevents attackers from readily gaining access to information in the files. Many options exist for protecting files, including encrypting individual files or folders, volumes, and hard drives. Generally, using an encryption method to protect files also requires the use of an authentication mechanism (e.g., password) to decrypt the files when needed.
- Ensure that information stored on telework devices is backed up. If something adverse happens to a device, such as a hardware, software, or power failure or a natural disaster, the information on the device will be lost unless it has been backed up to another device or removable media. Some organizations permit teleworkers to back up their local files to a centralized system (e.g., through VPN remote access), whereas other organizations recommend that their teleworkers perform local backups (e.g., burning CDs, copying files onto removable media). Teleworkers should perform backups, following their organizations' guidelines, and verify that the backups are valid and complete. It is important that backups on removable media be secured at least as well as the device that they backed up. For example, if a computer is stored in a locked room, then the media also should be in a secured location; if a computer stores its data encrypted, then the backups of that data should also be encrypted.
- Ensure that information is destroyed when it is no longer needed. For example, the organization's files should be removed from a computer scheduled to be retired or from a third-party computer that is temporarily used for remote access. Some remote access methods perform basic information cleanup, such as clearing

Web browser caches that might inadvertently hold sensitive information, but more extensive cleanup typically requires using a special utility, such as a disk-scrubbing program specifically designed to remove all traces of information from a device. Another example of information destruction is shredding telework papers containing sensitive information once the papers are no longer needed.

- Erase information from missing cell phones and PDAs. If a cell phone or PDA is lost or stolen, occasionally its contents can be erased remotely. This prevents an attacker from obtaining any information from the device. The availability of this service depends on the capabilities of the product and the company providing network services for the product.

**Adequately protect remote access-specific authenticators**

- Teleworkers need to ensure that they adequately protect their remote access-specific authenticators, such as passwords, personal identification numbers (PINs), and hardware tokens. Such authenticators should not be stored with the telework computer, nor should multiple authenticators be stored with each other (e.g., a password or PIN should not be written on the back of a hardware token).

**Social Engineering**

- Teleworkers should be aware of how to handle threats involving *social engineering*, which is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. For example, an attacker might approach a teleworker in a coffee shop and ask to use the computer for a minute or offer to help the teleworker with using the computer.
- Teleworkers should be wary of any requests they receive that could lead to a security breach or to the theft of a telework device.

**Handling a Security Breach**

- If a teleworker suspects that a security breach (including loss or theft of materials) has occurred involving a telework device, remote access communications, removable media, or other telework components, the teleworker should immediately follow the organization's policy and procedures for reporting the possible breach. This is particularly important if any of the affected telework components contain sensitive information such as EPHI, so that the potential impact of a security breach is minimized.