

Protecting PII: Telework Best Practices

Teleworking and Information Security

Telework presents many benefits to the federal workforce, such as managing commutes, saving taxpayer money by decreasing government real estate, and ensuring continuity of essential government functions in the event of emergencies. While telework allows for greater flexibility in managing our workforce, there are risks to privacy and information security¹ that are inherent with a remote workforce. Information security policies do not change when an employee works from home. It is the duty of the employee to safeguard Sensitive information, including personally identifiable information (PII),² while teleworking.

Safeguarding Sensitive PII

Effective teleworking begins with having a signed telework agreement in place. Work with your supervisor to determine what types of documents are appropriate to take home and what documents should stay secured within the DHS work space. Know the sensitivity of your documents, and make sure they are appropriately marked to help mitigate the risk of unauthorized disclosure.

One of the most effective ways to safeguard documents containing Sensitive PII is to keep electronic documents within the DHS network and to properly secure hard copy documents that you take outside of the DHS work space. Stay within the network by logging in remotely through the DHS Virtual Desktop*, whether you use your DHS-issued laptop or your personal computer. If you choose to work from your personal computer, **do not forward documents to your personal email account** as a way to avoid issues such as slow network connectivity or the inability to print. While there may be instances where you need to send information to an individual's personal account (i.e. job applicant), forwarding unencrypted emails to your own personal email account or sending unencrypted documents outside the DHS network that contain Sensitive PII is considered a privacy incident (or data breach).

If you know you will be teleworking, identify the files you may need to work on in

¹ The Federal Information Security Management Act of 2002 (FISMA) defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, which means guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

² PII is any information that can directly or indirectly lead to the identification of an individual. Sensitive PII is defined as personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

advance, and organize them on your network drive or DHS laptop so that they will be easily accessible to you while teleworking. You may also want to take advantage of DHS-approved collaboration tools, such as SharePoint, to easily access files while teleworking. However, before using SharePoint to store Sensitive PII, make sure your site has been approved for such use and that access is limited to only those individuals whose need for the information is related to his or her official duties. Have a back-up plan in mind in case you experience issues with network connectivity, but never transfer files to your personal computer using thumb drives or other portable electronic devices.















Be able to secure your DHS equipment and information at all times, including while transporting information home or while traveling. If you must leave equipment or documents unattended, secure them (i.e. in the trunk of your car, in a hotel safe, etc.), but only for short periods of time. Inventory your documents before teleworking, and ensure all documents are returned to the office.

Examples of Privacy Incidents Associated with Telework

Know how to recognize a privacy incident and how to report it.

- Sending an email containing Sensitive PII to your personal email account.
- Sending unencrypted Sensitive PII outside the DHS network (i.e., to another agency, to a private sector partner, to a potential hire).
- Allowing family members access to documents containing Sensitive PII.
- Printing documents containing Sensitive PII to your personal printer.
- Using a thumb drive or other device to transfer data (i.e., Sensitive PII) to your personal computer.

***Report any suspected or confirmed privacy incidents
to your supervisor
or your component Help Desk.***

WHEN	DO	DON'T	WHY
Before you telework...	 Plan ahead to ensure that Sensitive documents can be safely accessed remotely. Organize your files so that they are easily accessible via the DHS Virtual Desktop*. Use DHS-approved, portable electronic devices, which are encrypted, thereby adding a layer of protection to your data.	 Don't forward emails to your personal email account or use non-approved portable electronic devices. Have a back-up plan in case you experience issues with network connectivity, but never transfer or download data to your personal computer, personal email account, or to non-encrypted devices.	When you remove data from the DHS network, DHS cannot protect it. There may be instances where you need to send Sensitive PII to job applicants or individuals without DHS accounts, but it must be encrypted. To send it unencrypted is considered a privacy incident.
	 Obtain authorization from your supervisor to take home Sensitive documents, and make sure documents containing Sensitive PII are marked "For Official Use Only" or "Privacy Data." Inventory your hard copy documents when you leave the office and before you return them to the office.	 Don't take Sensitive PII home that you do not need. Limit your removal of Sensitive PII from the office to only that information that is relevant and necessary to the work outlined in your telework agreement.	Hard copy documents are easily lost or misplaced, putting Sensitive PII at risk. Conducting an inventory and properly marking documents helps mitigate the risk of unauthorized disclosure.
Transport of documents ...	 Be able to secure Sensitive data when not in use. If you must leave your laptop or hard copy documents inside a vehicle, lock them in the trunk but only for short periods of time. When traveling, place Sensitive data in a hotel safe when not in use.	 Don't leave your laptop or hard copy documents unattended overnight. Maintain accountability of your data by ensuring documents are secured when not in use.	Failure to maintain accountability of Sensitive PII can lead to loss, theft, or misuse, resulting in a privacy incident.
At home...	 Log in through the DHS Virtual Desktop* Organize your work space at home so that work files are separate from personal files and can be properly safeguarded.	 Don't email or save files containing Sensitive PII to your home computer.  Don't print agency records to your home printer. 	Your home computer, printer, fax, and copier all contain internal storage or "hard drives." Even when these devices are disposed of, the information stored within is vulnerable.
	 Take advantage of DHS collaboration tools such as SharePoint. Do not post Sensitive PII on the DHS intranet, Component intranet sites, SharePoint collaboration sites, shared drives, multi-access calendars, or on the Internet (including social networking sites) that can be accessed by individuals who do not have a "need to know."	 Don't store Sensitive PII on SharePoint unless your site has been approved for such use. Access must be limited to those that have an official need to know.	Collaboration tools provide quick, easy access to data, but without proper security controls, can lead to data winding up in the wrong hands. Sharing Sensitive PII with unauthorized users is considered a privacy incident.
	 Secure your data, and ensure other household members do not have access to it. Organize your work space at home so that government property and information are kept separate from personal property and can be properly safeguarded.	 Don't leave files containing Sensitive data lying out in the open. Never leave Sensitive PII in view of children, spouses, or visitors. Sensitive PII should be secured in locked cabinets and your computer/Blackberry should remain locked when not in use.	Failure to properly secure Sensitive records could result in inadvertent sharing of Sensitive PII.

*Each Component has a different process for accessing the DHS network remotely. Please contact your Help Desk.