Privacy

Privacy is protecting the personal information of others, not only for legal requirements, but also out of respect for others. Please be sure to follow the steps outlined here and in our overall security program, just as you would want others to take the same steps to protect your privacy.
Technological advances have made it easier than ever before to access and share information. However, these advances have brought tremendous challenges with them. Nowhere is this more evident than in the area of individual privacy and the handling of an individual’s personal information. As part of your routine work duties, you may handle personal information such as someone’s Social Security number, their financial information, their education or employment records or aspects of their health or medical records.

You may not realize it, but federal, state and local laws and regulations require you to protect the privacy of personal information. More importantly, you should safeguard that information out of respect to others. Do what you can to protect their privacy, just as you would want them to protect yours. Here are some steps that you can take to help protect the privacy of others.

**Authorized Systems**

To protect people’s privacy, you should only use authorized systems to enter, process or store their information. These systems have strong security measures in place, such as specialized security software and strict controls on how they are configured and who has access to them. Do not enter, process or store people’s personal information on unauthorized systems, such as your own personal laptop or personal email accounts.

**Sharing Data**

Another step to protecting people’s personal information is ensuring only authorized staff members have access to it. These individuals must have management’s prior approval to access such data. They must also have a need to know, or in other words, they need access to the data to accomplish their job. Simple curiosity is not a sufficient need for access.

**Cloud**

Never store or share people’s personal information on public Internet or cloud services, such as Dropbox, Apple iCloud or Google Drive, unless you have prior authorization from management.

**Transferring Data**

At times, you may need to transfer people’s personal information to authorized individuals. There are numerous risks to transferring data, such losing it, having it stolen or even intercepted. As such, you should only use secure, authorized methods that support encryption when transferring someone’s personal information. Never transfer private data using insecure means, such as using your own personal email account.
Data Destruction

A common way people's personal information is compromised is by employees improperly disposing of the information. For example, when you throw out an old USB flash drive or donate used computers, people's personal information is often still stored on those devices. To protect against this danger, all physical and electronic personal data that is no longer necessary or appropriate to store should be properly destroyed, shredded or rendered unreadable. For digital media, such as hard drives or USB flash drives, this means they should either be physically destroyed or the media should be securely wiped, ensuring the information is truly gone and cannot be recovered.

By protecting people's privacy, you help ensure our organization is compliant and demonstrate our organization's respect for others. If you have any questions about the types of information you should protect, how best to secure it or believe any of our information has been compromised, please contact the help desk or the information security team.

Technology's Impact on Privacy

The concept of privacy is not new. Organizations have collected and stored information on individuals for centuries. What has made this issue so different today is technology. Technology has not only made it possible for organizations to collect much more information on individuals, but made it easy to track specific individuals over the years as well.

In addition, technology has also made it much easier for individuals to illegally access, copy and distribute that very same information. This is why it has become so much more difficult (and important) for organizations like ours to actively identify and protect any and all private information we collect. You play a key part in protecting that private information. Only through your secure actions can we protect the privacy of others.