CYBER SECURITY

newsletter

DATA PROTECTION

Problem

Our organization handles a great deal of confidential information, including data known as Personally Identifiable Information, commonly called PII or Personal Data. PII is targeted by attackers because it is highly valuable information that can be used for identity theft, fraud or used to attack other organizations. PII is any information that can identify a specific individual, such as Social Security Numbers used in the United States, international passport numbers used in Europe, your drivers license number, or any other personally identifiable information.

Solution

Because this information is so valuable, and because we are committed to protecting the rights and privacy of others, all employees need to take the following steps to protect PII or any other highly confidential information. By following these rules, you help ensure both our organization and information is secure.

1. Authorized Systems: We take extra measures to protect PII and other confidential information. One of those steps is to ensure that such data is stored only on authorized systems. These are systems that have strong security measures, such as strict controls on how they are configured and who can access them. To protect important data, use only authorized systems to enter, process or store PII or other confidential information. Do not enter, process or store PII or other confidential information on any unauthorized systems, such as personal devices.

2. Sharing Data: Another key step to protecting such valuable information is ensuring that only authorized people who have a need to know can access our confidential information or PII. This means these individuals not only have prior management approval to access such data, but they need access to accomplish their job responsibilities, simple curiosity is not sufficient need for access.

Data Protection

Ultimately, it is our data, including PII, that cyber criminals are after. The key to protecting both yourself and our organization is to protect the confidential information you work with every day.

University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Personally Identifiable Information

The concept of Personally Identifiable Information (called Personal Data in Europe) is not new. For thousands of years civilizations have had ways to identify individuals such as their full name, birthplace and birthdate. However, a variety of factors have made this type of information both more valuable and easier to steal.

First, there is far more personal information collected on people then ever before. Every action you take is tracked, such as the clothes your purchase, the phone calls you make or the music you listen to. In addition this information is much easier to associate with specific people as we now have many different identification numbering systems.

Now, you take all this information, then add the fact that there are numerous copies of it stored around the world in digital format, and you begin to understand how easy it is for cyber criminals to steal this information. Once stolen, it can then be use for numerous crimes, including fraud and identity theft. It is because of risks like this that we must take extra steps to protect all Personally Identifiable Information.

3. Mobile Media: Be careful when connecting mobile media to your computer, media such as USB flash drives, memory cards or CDROMs. Only use authorized mobile devices the organization has approved. The concern is it is quite common for worms and viruses to spread via mobile devices. For example if you plug a USB flash drive into an infected computer at home, then bring that same USB flash drive into work, you can accidently infect our entire organization. This is why you do not use mobile media you may have found in the parking lot or received from strangers. In addition, whenever you connect mobile media to your computer make sure you scan all contents on it with current anti-virus before opening any files.

4. Transferring Data: At times you may need to transfer PII or other confidential information to authorized individuals who have a need to know. However, there are tremendous risks to transferring data, such as it getting lost, stolen or even intercepted. For example, if you copy the data to a USB stick and carry it to the office, what happens if you lose that USB flash drive? If you store the information on your laptop, what happens if your laptop is stolen? If you email the information anyone can easily intercept and read it.

As such, if you transfer PII or any other confidential data you should use only secure, authorized methods that support encryption. Do not transfer sensitive data using insecure means, such as email.

5. Data Destruction: A very common way PII and other related data is compromised is by employees simply disposing of the information when it is no longer needed, and then that information is recovered. For example, throwing out an old USB flash drive or donating computers that are no longer used. The problem is these devices often still have sensitive data on them such as PII, data that now anyone can access.

To protect against this danger, all physical and electronic PII and other confidential information 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 physical destroyed or the media should be entirely wiped, ensuring that the information is truly gone and cannot be recovered.