west protect℠

SAFE
Security Awareness For Everyone

Tip Sheet

Data Privacy and the PII Lifecycle

When you visit the bank or the doctor, you must provide them with personal information. Things like your name, address, date of birth, and Social Security Number. This information is valuable because it provides the key to your identity. If a criminal got hold of this data, they could use it to hack into your accounts, impersonate you, or steal from you. That's why you want the companies you do business with to keep your personal data safe.

But if your job involves handling other people's personal data, then it's your responsibility to handle it with the same strict privacy that you expect for your own data. That's why it's essential to understand what personally identifiable information is and how to keep it secure.

What is PII?

Under the Gramm-Leach-Bliley Act (GLBA), Personally Identifiable Information (PII) is defined as Name, Address, Phone number, Social Security Number (SSN), Driver's license number or other government-issued ID numbers. It also includes financial data like Bank account numbers, Credit or debit card numbers, Credit history or credit scores, Income and account balances, and Transaction histories. And other sensitive data such as Any information provided on applications for financial products or services; Details of services provided by the financial institution; Information from consumer reports, such as credit reports; and Information collected during online activities, like usernames and passwords for financial accounts

Protecting PII

Personal information must be protected and handled securely at every stage of its life cycle. That includes when the data is at rest (stored, saved), when it's in transit (emailed, file transfers/file sharing), and when the data is in use (accessing, processing).

- **Data at rest:** When data is at rest, it's crucial to use encrypted storage devices and cloud accounts. Access to the data should be restricted to only those who need it.
- **Data in transit:** When data is in transit, PII should be encrypted and sent only to authorized individuals.
- **Data in use:** When PII is in use, employees should only access the data they need to perform their duties. They should not attempt to view any PII beyond their proper access level. Employees should refrain from discussing or sharing any PII with unauthorized people.

PII is the key to identity. When you handle PII as part of your job, it's your responsibility to keep other people's data secure. So if you collect it, protect it! Local privacy laws may vary, so follow your organization's policies and procedures.

Unfortunately, cyberattacks are now part of life. It seems we hear about it almost every day. To hackers and criminals, all of our private data, even our healthcare data, is just another commodity to be sold.

By carefully handling the data you are entrusted with, taking precautions, and practicing good cyber hygiene, you can help protect yourself, your customers, and your company—inspiring trust and enhancing reputation and growth, which are always good for business.

What's the Difference between Privacy and Security?

Security **refers to the ways we protect ourselves, our property and personal information. It's the first level of defense against unwanted intruders.**

Privacy **is our ability to control access to our personal information.**

Data Privacy Week

January 27-31, 2025