4 TIPS FOR PROTECTING PII

Privacy is a hot-button topic, and alarming revelations about identity theft and data.

As organizations battle to keep personally identifiable information (PII) safe and secure, it becomes more and more apparent that all employees have a role to play in protecting data privacy.

The important thing to remember is that PII is more than just social security numbers and credit card numbers. PII includes any piece of information that can be used individually or in combination to identify a specific person. One-to-one identifiers (e.g., license numbers, finger prints, and insurance policy numbers) can be tied to individuals, but one-to-many identifiers — data points like first names, job titles, city of residence, and last names — can be combined to achieve the same end. In fact, it's estimated that 87% of the U.S. population can be identified using just three pieces of PII: gender, zip code, and birth date.

With that rather startling statistic in mind, it is clear that even seemingly small pieces of data can have value. If you come into contact with, collect, or store PII for coworkers or customers, here are four tips that can help keep PII safe:

1. Use Appropriate Security Safeguards for PII

Clearly, some PII is more sensitive than others. A list of customer names and email addresses doesn't need the same security protections as a list of customer names and credit card numbers. You would naturally want to keep the latter list very secure and only share that information on an as-needed basis. But that doesn't mean the list of names and email addresses should be shared freely with anyone and everyone. It's certainly not information you'd like to put in the hands of competitors, for example.

In order to gauge the level of sensitivity associated with PII, think about the ramifications in the event of a breach. The more sensitive the data, the more intense the protections should be.

2. Only Collect PII You Truly Need

There are a number of reasons an organization might collect data from its customers: for mailing lists (email or snail mail), billing, shipping, etc. Sometimes, as in the case of medical offices, collecting information is simply the starting point of a service relationship. But it's important to think about the information you truly need to have and limit collection to business-critical items. For example, if you're building a mailing list, think about whether you need anything beyond an email address. If you don't do hard-copy mailings or calling campaigns, there's no reason to collect mailing addresses and phone numbers.

Really think about the information you need before you ask for it.

3. Be Smart About Storing PII

Similar to the cautions associated with collecting PII, special considerations should be taken when storing PII. The more PII there is on an organization's network, the more vulnerable that organization is in the event of a breach. So before you store it, consider if it's business critical. If not, securely dispose of it. If so, apply the appropriate safeguards (including physical security measures for paper files and encryption and secure server storage for electronic files). In addition, be sure to revisit stored data and purge that which is out of date or no longer business critical.

4. Apply General Security Best Practices to PII When Appropriate

Keep common-sense best practices in mind when dealing with PII because they add an important layer of security. Password protecting secure systems is a must, as is keeping your passwords private. Do not let unauthorized individuals access secure areas or systems, and don't be too quick to disclose personal data about yourself, your coworkers, or your customers over the phone or on social media.

At the end of the day, it's about recognizing PII and keeping security and privacy top of mind as you use, collect, and store personal data. Also be sure to familiarize yourself with any corporate or industry policies that govern handling of PII.