PII Protection Checklist and Best Practices

Enable secure, compliant sharing workflows to maintain the privacy of PII and improve collaboration.

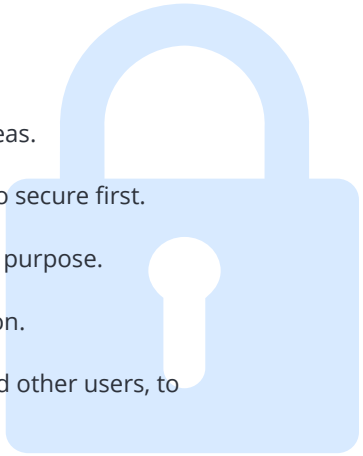
Personally identifiable information (PII) is any data that can be used to identify a specific individual. Along with the more traditional types of PII—such as name, mailing address, email address, date of birth, Social Security number, and phone number—the scope of what is considered PII has broadened to now include IP addresses, login IDs, bank account numbers and even social media posts.

As organizations collect, process, and store PII they must also accept responsibility for protecting this sensitive data. After all, data breaches can occur at all levels of organizational sophistication, but the impacts on the organization are often the same: breaches are costly, time-consuming, and damaging. Remember, one careless employee can result in PII being shared with unauthorized recipients.

Every single organization stores and uses PII, either on their employees or customers. To better understand how your organization may be at risk, consider the security and privacy challenges in the common scenarios below:

- **Employee PII:** HR teams often need to collect PII from new employees before they can begin working and be enrolled in an organization's HR information system. To do so, especially in today's remote work environment, employees may be expected to submit forms containing sensitive data via email. Without end-to-end encryption, PII is at risk of exposure.
- **Customer PII:** As one example, mortgage officers must collect and share customers' data to approve and process loan applications. Despite email being the path of least resistance to share this data, on its own it does not provide the data privacy, ownership, and visibility needed to give customers a positive experience, putting the organization at risk of a breach and facing noncompliance penalties.

Steps to Securing PII



1. **Identify** the types of PII your organization collects, processes, and uses.
2. **Locate** where PII is collected and stored, and the routes it takes to get to those areas.
3. **Classify** PII in terms of sensitivity to help prioritize which systems and processes to secure first.
4. **Establish** an acceptable usage policy that defines who can access PII and for what purpose.
5. **Protect** PII at the object level with data-centric protection via end-to-end encryption.
6. **Provide** seamless technology, accompanied by security training for employees and other users, to ensure they understand how to use your security solutions.

Encryption Checklist

Finding the right encryption solution is a critical step in securing PII both inside your organization and beyond. When evaluating your options, look for data-centric protection that can do the following:

- **Automate Security** — Where applicable, apply rules across all departments and employees to ensure all PII is secure in both emails and documents.
- **Simplify Workflows** — Add an easy-to-use layer of encryption to your organization's existing email and file applications, such as G Suite, without requiring new applications or logins.
- **Boost User Adoption** — Increase adoption of security technology through training and security awareness programs. Source easy security solutions that employees will want to use.
- **Ensure Compliance** — Meet current and future privacy and data protection regulations to avoid non-compliance penalties.
- **Maintain Control** — Deliver persistent data-centric protection, and stay in control of PII no matter where it is shared, by revoking or expiring access, controlling forwarding, and watermarking documents.
- **Enable Collaboration** — Keep PII secure and private while easily allowing safe collaboration with other parties.
- **Enhance Visibility** — Gain access to read receipts and granular tracking to determine who's accessed PII, as well as where and when, to support compliance audits.

Protect and Share PII with Virtru

Virtru unlocks seamless, secure PII sharing workflows to help ensure PII is protected and under your control at all times. Integrated with the applications you already use like Gmail, Google Drive, and Microsoft Outlook, Virtru gives organizations the ability to share sensitive data with ease, while keeping PII private and compliant.

Contact us to learn more about using Virtru to protect PII within your organization. virtru.com/contact-us

virtru

At Virtru, we empower organizations to easily unlock the power of data while maintaining control, everywhere it's stored and shared. Creators of TDF (Trusted Data Format), the open industry standard for persistent data protection, Virtru provides flexible, easy to use, and trusted privacy technologies built on its data protection platform that govern access to data throughout its full lifecycle—from creation to transmission, storage, analysis, and sharing. More than 20,000 organizations of every size and industry trust Virtru for data security and privacy protection. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.