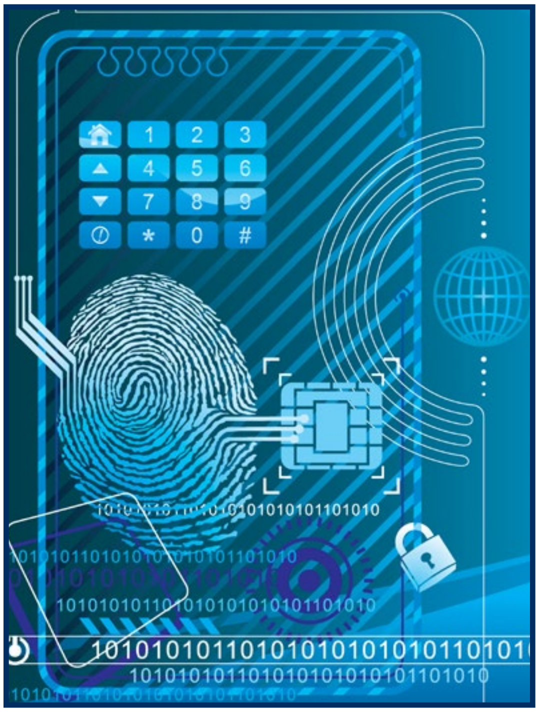
Security Industry Association Privacy Framework



The Security Industry Association (SIA) is committed to protecting privacy when a security solution requires the collection, protection or storage of personally identifiable information (PII). Originally released in 2010 and updated in 2014, the SIA Privacy Framework outlines a core set of principles and best practices the industry is working to implement in the deployment of electronic security technologies protecting people and assets.

Purpose

This SIA Privacy Framework has three intended purposes:

- To identify a set of privacy principles to serve as a guide for manufacturers, integrators and distributors of electronic security technologies (both physical and logical), including but not limited to access control devices, biometrics, CCTV, video analysis, IP-based technology and RFID; [1]
- To inform policymakers about how the security industry protects privacy when collecting, securing and storing PII;
- To help educate end users on the implementation of privacy protections.

SIA Privacy Principles:

1. **Mitigation by Design.** Privacy-enhancing solutions are ideally incorporated during the design phase of electronic security products, services or systems to the maximum extent possible—without increasing the risk of compromising the security provided by the products, services or systems.
2. **Assessment.** Privacy impact assessments help to provide integrators, system owners and managers a methodology to analyze how personally identifiable information is collected, stored, protected, shared and managed—as well as the length of time it is retained and how it is disposed.
3. **Legal Compliance.** An assessment of applicable legal or regulatory requirements, including, but not limited to, the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA) and the HITECH Act, is performed to help monitor compliance with these legal requirements.
4. **Use Limitation.** Work to ensure access to PII captured by a physical or online security system is limited to authorized individuals for authorized purposes.
5. **Database Safeguards.** The database where any PII is collected and stored is protected, including both physical and logical security of the database.
6. **Secure Communications.** Data transmitted between systems or components is protected from unauthorized disclosure, commensurate with risk.
7. **Transparency.** Individuals whose PII may be collected are notified of the reason for collection and how the data may be used.
8. **Breach Notification and Response.** End users adopt a privacy-breach notification plan that includes:
   a. means of determining whether notification is required to individuals with PII in the database

   b. responsive action if a privacy breach does occur

[1] **Note:** This document does not constitute legal advice and is only a guide.

   c. a mitigation procedure to address potential harm from unauthorized disclosure

9. **Data Retention Policy.** End users establish a policy on the retention and disposal of PII—a policy that may include:
   - **a.** for video, a policy establishing a time period for retaining (storing) video for both non-incident and incident video
   - **b.** for a physical access control system (PACS), a policy that dictates when PII is destroyed after an individual is no longer authorized access
   - **c.** for online, deletion of PII once that PII is determined to be no longer relevant
   - **d.** a procedure to ensure that deleted PII is not recoverable
10. **Accountability.** Collaboration between service providers and end users of electronic security systems helps ensure compliance with best practices for privacy protections.

Example Steps to Implement the Framework through a Privacy Impact Assessment (PIA)[2]

Step One
Work to identify information—including PII—that is collected and stored by the physical or online security system, including areas within the system where such data might be stored. Such information could include name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code, certificate/license number, vehicle identifier including license plate, device identifiers and serial numbers, biometric identifiers, photographic facial images or any other unique identifying numbers or characteristics.

Step Two
Follow the Fair Information Practice Principles (FIPPs) in determining how the information collected by the system may be used and protected.

- **Purpose Specification:** Examine why the information is collected so that the system is collecting information that is relevant to achieving the security purpose.
- **Data Minimization:** Limit collection of information to what is determined necessary to achieve the system's security goals.
- **Notice and Awareness:** Determine when and how individuals affected by the security system may be notified of the information collection and its purpose.
- **Data Security:** Examine the potential for both internal and external threats to unauthorized disclosure of PII. Use encryption, mutual authentication and other logical security measures to help protect against potential threats.

Step Three
Determine the controls that are in place, or may be needed, to help minimize risks to collected PII, consistent with the security purpose—and to identify and address points of potential weakness in the collection, sharing and storage of PII.

Step Four
Examine how long and for what reasons collected PII may be retained. Maintain information for the minimum amount of time determined to be necessary, consistent with the security purpose, in order to mitigate the risk of unauthorized disclosure.

Step Five
Determine how and when collected PII may be removed from the system and destroyed to help eliminate potential risks from improperly disposed of PII.

[2] This template is only a guide. It could be modified or expanded depending on the requirements of a specific application. Ideally, a PIA is performed before a system is deployed but the process can also be used to evaluate existing systems, or when an existing system is being considered for upgrade.