Privacy by Design: Product Development Guidelines for Engineers & Product Managers

Purpose:

The purpose of this document is to provide our development teams with high level principles and concepts relating to privacy and data protection. Becoming familiar with these principles and concepts will allow you to design into our products, systems, and services features and functionalities (Privacy by Design) that will make it easier for Cisco, customers and users to comply with and/or enforce legal and business requirements to protect personally identifiable information ("PII" – defined below). As a result, privacy becomes an essential component being delivered and is not bolted on as an add-on, after the fact.

Privacy by Design has become a key market differentiator in today’s cyberworld, particularly as the number of available cloud applications has multiplied and more people are concerned about what information is being collected about them, who has access to their PII, and how such PII is protected. Some examples of applications and services offered by Cisco include: HealthPresence, uni, WebEx, WebEx mail, QUAD, FlipShare, FlipPro, and Eos.

There are additional and separate policy and guidelines covering Cisco’s privacy and data protection practices relating to the collection and processing of PII of customers, prospective customers, online visitors, employees and other parties, which can be found on Privacy Central.

Key Concepts:

Privacy: Privacy is an individual’s expectation that organizations will use their personal information in limited ways and protect it from disclosure to unauthorized parties.

User Data: User Data includes any data that is collected directly from a user (e.g., entered by the user via an application’s user interface); any data about a user that is gathered indirectly (e.g., document metadata); any data about a user’s usage behavior (e.g. logs or history); and any data relating to a user’s system (e.g., system configuration, IP address).

Anonymous Data: In some instances, we may collect non-personal or anonymous data such as usage tracking, how frequently errors are encountered, device information or system configuration. Typically, this information is used to determine how customers are interacting with a solution and to assist with improving it. An
example of anonymous user data is system information, such as a user’s hardware configuration.

**Pseudonymous Data**: Pseudonymous Data is unique information that does not identify a specific person, but could be associated with an individual. Examples include unique identifiers, biometric information, non-personal usage profiles, browser cookies, or search histories.

**What is Personally Identifiable Information (PII)**: PII means any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains, or from which identification or contact information of an individual person can be derived. PII includes, but is not limited to:

- Contact information (name, email address, phone, postal address);
- Forms of identification (social security number, driver’s license, passport, fingerprints);
- Demographic information (age, gender, ethnicity, religious affiliation, sexual orientation, criminal records);
- Occupational information (job title, company name, industry);
- Health care information (plans, providers, history, insurance, genetic information);
- Financial information (bank and credit/debit card account numbers, purchase history, credit records); and
- Online activity (IP address, cookies, flash cookies, login credentials).

**Sensitive PII**: Sensitive PII is a subset of PII considered to be so important to the individual that it must be specially protected. Sensitive PII includes, but is not limited to:

- Credit card numbers and bank account information;
- Government-issued identifiers such as Social Security Numbers and drivers’ license numbers;
- Data that could be used to discriminate (e.g., race, ethnic origin, religious or philosophical beliefs, political opinions, trade union memberships, sexual lifestyle, physical or mental health);
- Data that could be used to facilitate identity theft (e.g., mother’s maiden name);
• Data that could be used to permit access to a customer's account (e.g., passwords or PINs); and
• Customer's real-time location.

An important note regarding Sensitive PII: To be clear, privacy concerns apply to all User Data—anonymous, pseudonymous, personally-identifiable or otherwise—not just to Sensitive PII. However, Sensitive PII carries additional compliance obligations and the potential for the most damaging consequences.

Collection & Retention Considerations:

Reduce the Amount of Data Collected: Avoid collecting sensitive data and only collect information that is absolutely necessary for the purpose of the collection.

Architects, developers, and administrators of data collection systems should constantly ask:
  • “Do I need to collect this data?”
  • “Do I have a valid business purpose?”
  • “Will customers support my business purpose?”

The answers must explicitly address both the primary use of the customer’s data (such as providing the feature or service the customer is requesting) and any planned secondary use (such as marketing analysis).

Reduce the Retention Period: Do not retain customer data for any period longer than necessary to accomplish the intended business purpose or required by law. The longer the data is retained, the higher the likelihood of accidental disclosure, theft, and the data growing stale.

Reduce the Sensitivity of the Data: Data exposure can be minimized by reducing the sensitivity of the stored data. When data becomes less sensitive, security requirements for storing and transferring the data may be reduced.

Reduce the Precision: For example, if a customer phone number is to be used for statistical analysis, retain only a subset of the digits such as the area code.

Convert the Form of the Data: For example, when using the customer's IP address to determine location for statistical analysis, discard the IP address after mapping it to a city or town.
Collection Considerations:

There are many ways to introduce data into a system: input fields are one obvious way, but packet inspection, port scanning, browser cookies, and various types of data mining are just some of the alternatives.

When determining whether your project involves collecting User Data, keep in mind that products and services can collect data without explicitly asking users to enter it. For example, Microsoft Office documents routinely contain users’ names in the file’s metadata.

Also keep in mind that users may provide PII, even if your project does not ask for it—open-ended input fields, password fields, and password reminder fields are just some of the ways that your project may inadvertently collect sensitive information.

Our product / service should be designed to provide customer with a notice and a choice of whether to provide the PII and whether the PII can be transferred from the customer’s system or shared with third parties. Self-regulatory standards have been developed by leading industry associations to apply consumer-friendly best practices to the collection and use of PII in certain scenarios, including online data collection, behavioral advertising and video surveillance/digital signage. For reference, please see the links provided in the "Other Resources" section below.

Notice: All notices should be written in clear, easy-to-read language. The Notice should:

• Explain the PII that we collect;
• How we will use it;
• With whom we will share it; and
• How we will safeguard it.

Notice must be given before or at the point PII is collected and should include instructions as to where the customer can get additional information (e.g., a link to the privacy statement).

Choice: Individuals must be given a choice as to whether their PII may be used in a way other than the purpose for which it was disclosed. For example, when registering a product, a customer supplies his address, phone number and email address so we can process the registration - a primary use. We must provide the customer with a choice as to whether this information may be used for any communication beyond the product registration (such as marketing) - a secondary use.
Consent: Consent can take the form of "opt-in" or "opt-out." "Opt-in" means "Yes, I agree" while "opt-out" means "No, I do not agree." To be considered an "opt-in," the default for the query must be "no" or "null" and the individual must take an affirmative action to say "yes."

Security & Integrity Considerations:

Data Security: Reasonable steps should be taken to protect PII from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Preventive measures include:

- Access controls;
- Encryption in transfer and storage;
- Physical security;
- Disaster recovery; and
- Auditing.

Cisco's Information Security organization (InfoSec) has established policies and procedures to minimize security risks to PII. Third parties involved with the processing and storage of PII are also subject to these policies and need to be evaluated through the applicable InfoSec review process.

Sensitive PII requires additional care and security measures such as encryption.

Limit Access to "Need to Know": Access to PII should be limited to those who have a legitimate business purpose for accessing the data. In addition, those employees should only be given access to the smallest amount of PII needed to achieve the specific business purpose. Access must be revoked if access to the data is no longer required as part of the employee’s job function.

Data Integrity: Reasonable steps must be taken to ensure that PII is accurate, complete, and relevant for its intended use. Detective and corrective processes should be put in place to monitor and minimize inaccuracies through routine checks on systems that contain PII. Additionally, because PII may be stored in multiple systems and databases, those systems must be designed to ensure that PII (including customer preferences) remains accurate when data is merged or replicated from one system to another.

Registration of Databases containing PII: A number of countries (including the EU) require registration of databases containing PII with the appropriate legal authority. In support of this, you need to register your databases(s) in the internal "Personal Data Registry."
Customer Access & Control: The customer should have the ability to view, update, and remove/deactivate his/her PII at will without restriction. This can be implemented with the customer having direct access to apply updates or by proxy with confirmation.

Transfer & Disclosure: PII may only be shared with or transmitted to third parties to accomplish their intended business purpose and as stated in the Notice provided to the customer. If you are not aware of the intended business purpose, it is likely that the disclosure is inappropriate and has not been authorized. Whenever possible, take steps to make the PII anonymous before transfer or disclosure.

Disposal: If we no longer need the information or if the information becomes obsolete, destroy or remove it as soon as possible. PII that is no longer useful should be disposed of in a secure and appropriate manner (i.e. using encryption disk erasure or paper shredders).

Anonymous & Pseudonymous Data

For anonymous and pseudonymous data, the guidance is as follows:

- Even if this information will not be used to identify the user, best practice is to follow an opt-in approach before collecting it. See Example 3 in Exhibit B.
- At a minimum, this collection practice should be disclosed in the online privacy supplement, along with providing users the opportunity to opt-out of the collection.

Special Considerations: Financial & Medical Information:

Due to the sensitive nature of the information, special consideration should be given to financial and medical information.

Financial Information (Credit Cards): There are significant risks and onerous data security compliance requirements associated with collecting and storing credit card information. The preferred approach is to outsource the acceptance, processing, transmission and storage of cardholder data to a third party rather than performing it internally. Any such third party must enter into an agreement (which should include a Cisco standard Data Use and Protection Agreement) that obligates the third party to comply with applicable data security standards, Cisco's policies, and any information security standards or applicable laws as required by Cisco. In addition, the third party must complete a review and audit by InfoSec.
In the event cardholder data will be received, stored, processed or transmitted internally, the "Payment Cardholder Data Handling and Protection Policy" addresses the handling and protection requirements to prevent unauthorized disclosure or misuse of cardholder data and to ensure compliance with legislation, regulations and data security standards.

Financial Information (Financial Institutions): The Gramm-Leach-Bliley Act provides protections for consumers' personal financial information held by financial institutions (i.e., companies providing financial products and services to consumers, including but not limited to: lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, and collecting consumer debts.)

Notice: Consumers must be provided privacy notices that explain the institution’s information-sharing practices. In turn, consumers must be given the right to limit some - but not all - sharing of their information.

Security: Safeguards must be designed, implemented and maintained to protect consumer information.

Medical Information: HIPAA (Health Information Portability and Accountability Act) provides national standards for protecting the privacy of protected health information (PHI).

PHI is individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, paper, or oral). The 18 PHI identifiers are set out in Exhibit A. In the event that Cisco will host, use or store PHI (either internally or via a third party) in connection with services performed for a healthcare customer, please contact the Customer Compliance Team to initiate the technical review process.

Notice: Individuals must be provided notice regarding the uses of their PHI.

Patient Access: Individuals must have the right to correct any inaccurate PHI.

Confidentiality of Communications: Reasonable steps must be taken to ensure the confidentiality of communications with individuals.

Disclosures and Documentation: Steps must be taken to keep track of disclosures of PHI and document privacy policies and procedures.
Security: Three types of security safeguards are required:

- Administrative (policies and procedures must be in place to show compliance with the act);
- Physical (physical access must be controlled to protect against inappropriate access to protected data); and
- Technical (access to computer systems must be controlled and controls must be in place entities to protect communications containing electronically transferred PHI from being intercepted by anyone other than the intended recipient.)

SUPPORTING DOCUMENTATION

Specific Examples Implementing these Guidelines:
Examples using these Guidelines are set out in Exhibit B.

Best Practices for Cloud Computing Solutions:
Best practices for data protection and security for services hosted in the cloud are outlined in Exhibit C.

Other Resources
- Privacy Central
- Personal Database Registry
- Cardholder Data Handling and Protection Policy
- Your legal contact
- Privacy team email alias
- Infosec
- Industry Self-Regulatory Standards:
  - Behavioral Advertising
  - Online Data Collection
  - Video Surveillance / Digital Signage - Center for Democracy & Technology (CDT) and Point of Purchase Association International (POPAI)
EXHIBIT A

Protected Health Information under HIPAA

Protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. PHI that is linked based on the following list of 18 identifiers must be treated with special care according to HIPAA:

1. Names

2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000

3. Dates (other than year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

4. Phone numbers

5. Fax numbers

6. Electronic mail addresses

7. Social Security numbers

8. Medical record numbers

9. Health plan beneficiary numbers

10. Account numbers

11. Certificate/license numbers

12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;

14. Web Uniform Resource Locators (URLs)

15. Internet Protocol (IP) address numbers

16. Biometric identifiers, including finger, retinal and voice prints

17. Full face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)
EXHIBIT B

Examples for Privacy by Design: Product Development Guidelines for Engineers

Example 1: Transferring PII to and from Customer’s System

Notice and Consent:
Must provide Prominent Notice and get Explicit Opt-In Consent prior to transfer of PII from customer’s system

Must provide Prominent Notice and get Explicit Consent if PII being transferred will be used for secondary purposes such as marketing

Must have Explicit Opt-In Consent if Sensitive PII (e.g., credit card number) being transferred will be retained at the Company for future use by the customer

Must provide customer with access to Cisco online privacy statement

Should clearly distinguish in User Interface (UI) between optional and required data

Should not use free-form text fields (e.g., scrolling text boxes) when a defined field (e.g., pre-populated list box) can be used instead. If free-form text fields are used, they should be accompanied by a privacy warning directly in the UI

Data Security and Integrity:
Must transfer Sensitive PII to or from a customer’s system over the Internet using a secure method that helps prevent unauthorized access

Should transfer non-Sensitive PII to or from a customer’s system over the Internet using a secure method that helps prevent unauthorized access

Should not use methods of form submission that potentially expose data in a Web form intended for, or likely to result in, the collection of PII

Must only transfer minimum amount of data to achieve business purpose

Should only transfer customer specific data like GUIDs, computer serial numbers, or user IDs if essential to business purpose

Should use data validation controls to filter out inconsistent, incomplete, or incorrect PII

Should mask passwords or pins when collecting or displaying this information

Should suppress a majority of the digits when displaying a credit card number that has been stored

Customer Access and Control:
Customer must be able to control automatic collection and transfer of PII

Customer should be able to remove hidden PII prior to transfer

Must follow the requirements in Scenario 6 if data will be transferred to and stored at the Company
Example 2: Storing PII on the Customer’s System

Notice and Consent:
- Must provide the customer with notice and get consent prior to storage of Sensitive PII
- Must provide the customer with Prominent Notice and get Explicit Opt-In Consent when storing PII in a persistent cookie
- Should provide at a minimum a Notice that specifies what data is stored and what controls are available prior to storing Hidden PII
- Should make it clear to customers if PII could be accessed by other users

Data Security and Integrity:
- Must store Sensitive PII using appropriate security mechanisms that help prevent unauthorized access
- Should identify or provide appropriate security mechanisms that will help the customer prevent unauthorized access to stored Non-Sensitive PII
- Must encrypt PII when stored in a persistent cookie
- Must restrict access to Sensitive PII by default unless the customer has authorized such access
- Should restrict access to stored non-Sensitive PII by default
- Should avoid persisting Sensitive PII on the customer’s system whenever possible
- Must store Sensitive PII using appropriate security mechanisms that help prevent unauthorized access
- Should identify or provide appropriate security mechanisms that will help the customer prevent unauthorized access to stored Non-Sensitive PII
- Must encrypt PII when stored in a persistent cookie
- Must restrict access to Sensitive PII by default unless the customer has authorized such access
- Should restrict access to stored non-Sensitive PII by default
- Should avoid persisting Sensitive PII on the customer’s system whenever possible
- Should persist PII for the shortest time possible to meet the business purpose

Customer Access and Control:
- Customer should be able to control whether PII is stored
- Customer should be able to delete any PII that was stored on the customer’s system, including Hidden PII
- Customer must be able to view and edit stored PII they entered
**Example 3: Transferring Anonymous or Pseudonymous Data from the Customer's System**

**Notice and Consent:**
Must provide the customer with Prominent Notice and get Explicit Consent prior to collection and transfer

**Customer Access and Controls:**
Customer must be able to stop subsequent collection and transfer

Should highlight applicable controls in the Notice

**Example 4: Installing Software on a Customer’s System**

**Notice and Consent:**
Must provide the customer with Prominent Notice and get Explicit Consent prior to installation of any software on a customer’s system, including automatic updates

**Data Security and Integrity:**
Should digitally sign software with a certificate from a well-known, trusted certification authority to help ensure integrity

**Customer Access and Controls:**
Should use standard mechanisms for installing software so that customers have control over installing and uninstalling the software

Should provide Customer with a mechanism to track the automatic updates that have been installed and provide Customer a means to stop subsequent updates

**Example 5: Storing and Processing User Data at the Company**

**Notice and Consent:**
Must provide Customer appropriate notice and obtained appropriate consent prior to using data

**Data Security and Integrity:**
Must only store minimum amount of data necessary to achieve business purpose

Must store PII using appropriate security mechanisms to help prevent unauthorized access

Must restrict PII access to those with a need to know

Must maintain integrity of the data

Must store PII for the shortest time necessary to achieve the business purpose

Should provide a mechanism to audit access to PII
Should aggregate stored data to reduce sensitivity wherever possible

Customer Access and Controls:
- Must provide a secure mechanism for customers to access and correct stored PII
- Must authenticate customers via a Company Approved process before collecting, displaying, or modifying PII or contact preferences
- Must limit access to those with a valid business need
- Should only provide access to records and data fields necessary to accomplish the business purpose
- Must revoke access if no longer required as part of an employee or agent's job function or when the agent's contract has ended
- Should provide a mechanism to audit access to PII

**Example 6: Server Deployment**

**Notice and Consent:**
- Must get Explicit Opt-In Consent from an Application or System Administrator prior to transfer of data from the server over the Internet
- Must disclose any known privacy implications for server features (e.g., in a deployment guide)
- Should consider identifying or providing a mechanism for the enterprise to display a privacy statement to its end users

**Enterprise Controls:**
- Must identify or provide a mechanism that allows a System Administrator to restrict overall access to data stores, such as files, databases, or the registry, which contain User Data
- Must identify or provide a mechanism that allows an Application Administrator to protect stored User Data from unauthorized Instance Administrators
- Must identify or provide a mechanism for an Instance Administrator to protect stored User Data
- Should provide or identify a mechanism to help an Instance Administrator prevent disclosure of User Data
- Should provide or identify a mechanism such as group policy that allows an Application or System Administrator to manage distribution of data outside of the organization or firewall
- Must provide System Administrator the ability to override decisions made by Application Administrators
Security is a priority concern for many customers and a strong driver for cloud service providers to follow best practices for handling and storing customer data. A multilevel security model should be used for the cloud computing solution that maximizes data security and protection and helps ensure service continuity. Best practices include:

- Securing data at rest through blind encryption so only the customer can decrypt the data stored in the cloud, and storing data in a limited number of known systems to support complete removal when needed
- Securing data in motion via transport security measures, strict password policies and user authentication, and network security
- Data segregation of the customer's data from that of other customers
- Architecture considerations to include software code reviews, host hardening and high-availability practices
- Stringent personnel guidelines, including administrative policies and procedures, to ensure only authorized personnel have access to customer PII.
- Obtaining third party accreditation (for example, SAS-70 Type II and ISO-27001)