**USC Data Privacy Reference Guide**

Questions? Contact the Office of Culture, Ethics, and Compliance (OCEC):
- compliance@usc.edu
- 213-740-8258

---

**“Two Sides of the Same Coin”**

**Data Privacy**
- Governs how data is collected, used, shared, and how to uphold individual’s rights related to their data

**Data Security**
- Refers to measures (e.g., solutions, technologies) to protect data from unauthorized access

---

**Definition**
PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

---

**What is Personal Information (PI)?**

*Not an exhaustive list of examples*

- Name, Alias
- Social Security Number
- Driver’s license
- Passport
- Internet Activity
- Geolocation Data
- Date of Birth
- Place of Birth
- Email Address
- Phone Number
- Address
- Bank Accounts
- Credit Cards
- Financial Info
- Medical Info
- Leave Notices
- Health Plans
- Treatment
- Accommodation
- Diagnosis

---

**Key Privacy Practices**

1. **Only access information necessary to perform your duties**
2. **Only disclose the minimum amount of information necessary to fulfill the intended purpose**
3. **Only disclose information to individuals authorized to receive it**
4. **Protect information in your possession (verbal, written, electronic)**
5. **Safely dispose of information (e.g., shredders)**

---

**Privacy Do’s**

- Confirm communications containing PI are being sent to the appropriate individuals
- Use private areas to discuss PI (not elevators, hallways, or in public)
- Encrypt files when necessary and lock and secure laptops/ portable devices
- Be familiar with USC data privacy and information security policies and procedures
- Report suspected privacy violations to your supervisor or OCEC

---

**Privacy Don’ts**

- Share User ID and passphrases or leave them open for others to see
- Leave laptops, devices, and sensitive data unattended (even for a few seconds!)
- Transfer or process data for unrelated purposes, unless legally required to do so
- Send or forward USC confidential information to personal email accounts
- Click on links or open attachments from suspicious emails or unknown sources

---

**Resources**

- Report Phishing
- Email Encryption
- Confidential Info Brochure (See separate attachment)
- USC Data Privacy Site
- USC Information Security Site

---

**Help & Hotline**
- report.usc.edu
- 213-740-2500
- 800-348-7454

---

**CMIA**
- What is Personal Information (PI)?
- *Not an exhaustive list of examples*

- PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

- Social Security Number
- Driver’s license
- Passport
- Internet Activity
- Geolocation Data
- Date of Birth
- Place of Birth
- Email Address
- Phone Number
- Address
- Bank Accounts
- Credit Cards
- Financial Info
- Medical Info
- Leave Notices
- Health Plans
- Treatment
- Accommodation
- Diagnosis

---

**FERPA**
- **Definition**
- PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

---

**HIPAA**
- **Definition**
- PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

---

**GLBA**
- **Definition**
- PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

---

**GDPR**
- **Definition**
- PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

---

**Privacy Do’s**

- Confirm communications containing PI are being sent to the appropriate individuals
- Use private areas to discuss PI (not elevators, hallways, or in public)
- Encrypt files when necessary and lock and secure laptops/ portable devices
- Be familiar with USC data privacy and information security policies and procedures
- Report suspected privacy violations to your supervisor or OCEC

---

**Privacy Don’ts**

- Share User ID and passphrases or leave them open for others to see
- Leave laptops, devices, and sensitive data unattended (even for a few seconds!)
- Transfer or process data for unrelated purposes, unless legally required to do so
- Send or forward USC confidential information to personal email accounts
- Click on links or open attachments from suspicious emails or unknown sources

---

**USC Data Privacy Site**
- **Definition**
- PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

---

**CMIA**
- **What is Personal Information (PI)?**
- *Not an exhaustive list of examples*

- PI is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular individual.

- Social Security Number
- Driver’s license
- Passport
- Internet Activity
- Geolocation Data
- Date of Birth
- Place of Birth
- Email Address
- Phone Number
- Address
- Bank Accounts
- Credit Cards
- Financial Info
- Medical Info
- Leave Notices
- Health Plans
- Treatment
- Accommodation
- Diagnosis