Privacy

Table of Contents

Getting Started

This chapter of the *Information Security Guide* will serve as a clearinghouse for sharing higher education privacy materials. While privacy is a discipline distinct from information security, sharing privacy information in this resource is appropriate given the many collaborations necessary between higher education information security and privacy programs to ensure the comprehensive protection of institutional data.

The initial process in developing an institutional privacy program is to understand the institution's approach to privacy, understand the different types of data used at the institution, and identify which laws and regulations are applicable to the institution's use of data. You will also want to get to know your stakeholders and other institutional privacy supporters.

Learn more about the General Data Protection Regulation (GDPR) and how it may affect your institution starting in May 2018.

- The General Data Protection Regulation Explained (August 2017 *EDUCAUSE Review* article by Barmak Nassirian)
- GDPR: A Data Regulation to Watch (August 2017 *EDUCAUSE Review* blog by Jaime Tuttle-Santana)
- GDPR: Twelve Steps, Sorted (Jisc blog post)
- Data Protection Reform website (Information Commissioner's Office)
- EU GDPR (EDUCAUSE Library resource page)

Top of page

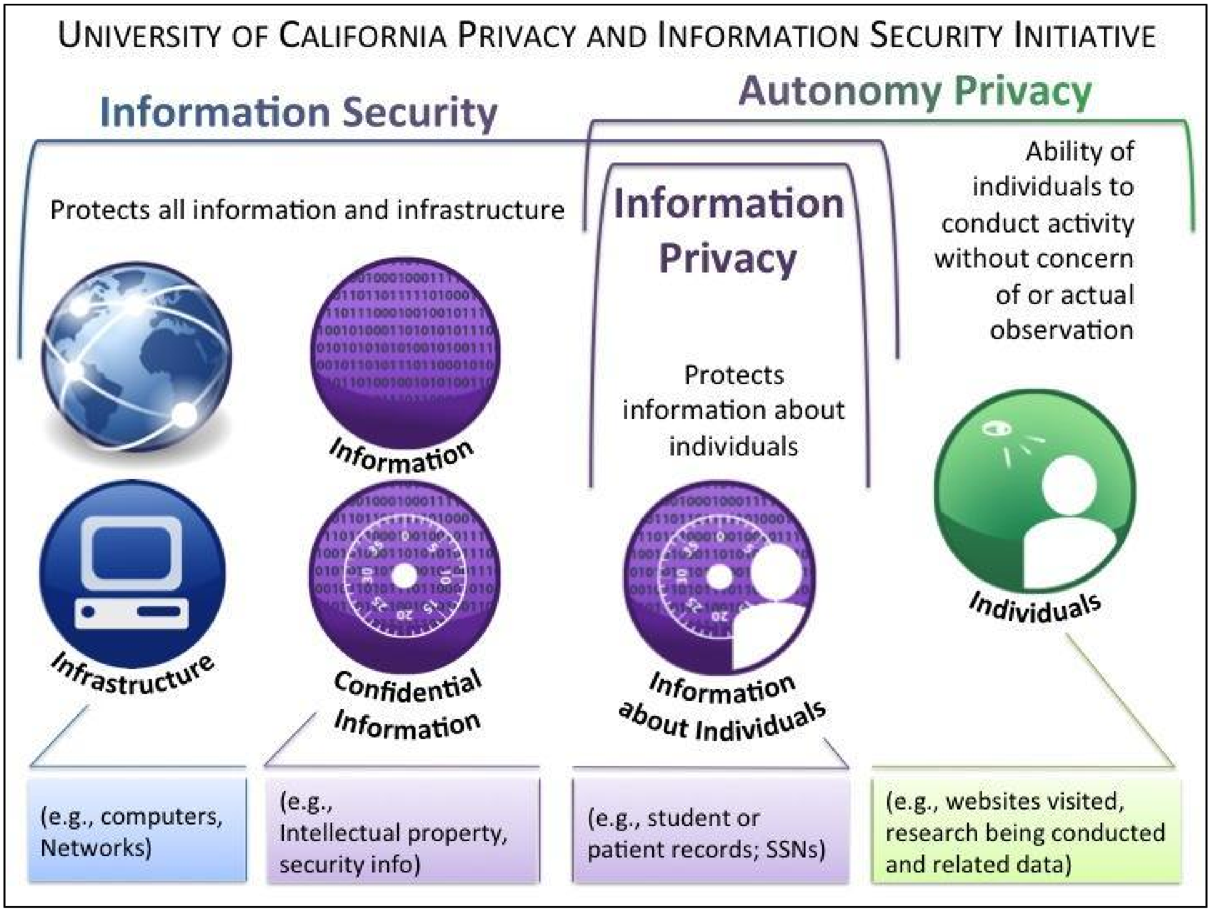
Overview

In the past few years, higher education institutions have begun to hire a growing number of individuals, often called Chief Privacy Officers (CPOs), dedicated to campus privacy and data protection concerns. Higher education institutions collect, store, use, transmit, disclose, and dispose of a wide variety of data every day. The data are varied and include research data, academic data, medical data, financial data, and the personally identifiable data of faculty, staff, students, alumni, and any other person that comes into contact with the institution. Concerns about privacy and data protection have risen in conjunction with the emergence of new technologies, the vast amounts (and variety) of data at play in the higher education environment, and how that data is being used. (See our brief list of the most common federal data protection laws, or visit the Higher Education Compliance Alliance Matrix.)

At the outset, it should be noted that privacy concerns are very different from security concerns, even though the two concepts are often used interchangeably. Information security activities are focused on protecting the confidentiality (i.e., only those authorized to see certain data have access to it), integrity (i.e., the data remains unchanged while it is processed in IT systems), and availability (i.e., data is available/accessible to users when they need it) of data.

Privacy, on the other hand, looks at the privacy rights of individuals and the laws, practices, and norms about how information is collected, used, and disclosed. Within that very broad definition are two concepts:

- Autonomy privacy: The right of an individual to conduct their activities without concern of observation. (This is commonly understood as the "right to be let alone" and to conduct one’s activities without interference from the government or other government-like organizations.)
- Information privacy: The right of an individual to have some control over how their personal information is used. This concept stems from the Fair Information Practice Principles (FIPPs).


UNIVERSITY OF CALIFORNIA PRIVACY AND INFORMATION SECURITY INITIATIVE
Information Security
Autonomy Privacy
Protects all information and infrastructure
Information Privacy
Ability of individuals to conduct activity without concern of or actual observation
Protects information about individuals
Information
Infrastructure
Confidential Information
Information about Individuals
Individuals
(e.g., computers, Networks)
(e.g., Intellectual property, security info)
(e.g., student or patient records; SSNs)
(e.g., websites visited, research being conducted and related data)

Source: UC Berkeley (2016)

In the higher education context, issues around privacy are encountered daily. Consider the following brief examples:

- An institution wishes to install surveillance cameras in its recreational center locker rooms because of increased theft and assaults in these spaces.
- The admissions office wishes to update the institution’s application form and ask students to include their social media account names on their application for admission.
- A faculty member wishes to conduct research on rare diseases and wants to use patient medical records received from the university’s medical center for her research.

All of these examples include privacy issues that need to be addressed. Privacy also contains a compliance component, as there are many laws and regulations that include privacy requirements. In addition to state laws, some of the more well-known federal privacy laws mentioned in the higher education privacy space include:

- The Family Educational Rights and Privacy Act of 1974 (FERPA): Designed to protect students and their families by ensuring the privacy of student educational records.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA): Requires covered entities (typically medical and health insurance providers and their associates) to protect the security and privacy of health records.
- The Gramm Leach Bliley Act of 1999 (GLBA): Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data.
- Federal Policy for the Protection of Human Subjects (“Common Rule”): Published in 1991 and codified in separate regulations by 15 federal departments and agencies, outlines the basic ethical principles (including privacy and confidentiality) in research involving human subjects.
- The Children’s Online Privacy Protection Act (COPPA): Governs the online collection of personal information from children under the age of 13.
- The Fair and Accurate Credit Transaction Act of 2003 (FACTA, or “Red Flags Rule”): Requires entities engaged in certain kinds of consumer financial transactions (predominantly credit transactions) to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft.
- The Privacy Act of 1974: Specifies the rules that a federal agency must follow to collect, use, transfer, and disclose an individual’s personally identifiable information (PII).

As institutions consider privacy issues, a number of responsibilities have evolved for individuals responsible for campus privacy activities and/or programs. Those responsibilities include:

- Establishing privacy policies, notices, standards, and processes with institutional stakeholders.
- Ensuring that the institution complies with applicable state, federal, and international laws, campus policies and procedures, and industry privacy standards.
- Developing and managing privacy awareness education for students, faculty, and staff.
- Serving as a subject matter expert and counseling campus constituents on best practices, new technologies, privacy complaints, potential institution-wide risks, and privacy impacts on institution-wide initiatives.

- Assisting with investigations and responses to campus privacy breaches or incidents.

Note: This chapter of the *Information Security Guide* will serve as a clearinghouse for sharing higher education privacy materials. While privacy is a discipline distinct from information security, sharing privacy information in this resource is appropriate given the many collaborations necessary between higher education information security and privacy programs to ensure the comprehensive protection of institutional data.

Top of page

Welcome Kit and Roadmap for Chief Privacy Officers in Higher Education

The Higher Education Chief Privacy Officers Working Group has created this resource to serve as a **welcome kit** for CPOs in higher education. The CPO Primer (part one) is intended to provide an overview and introductory body of knowledge to help new CPOs (or those new to higher education) better understand their job and the challenges unique to colleges and universities. The main audience for this document is a CPO or person with primary institutional responsibility for privacy. The CPO Primer covers the following topics:

1. Privacy's role in higher education and how the privacy officer and privacy function fit within a college or university's organizational structure
2. Key areas of focus and components of a privacy programs
3. The relationship between (and balance of) privacy and security
4. Basic information about federal, state, and international privacy laws applicable to higher education (appendix A)
5. Common privacy frameworks and standards (appendix B)
6. Professional resources that provide support or guidance and a brief list of recommended readings (appendix C)

The CPO Primer (part two) is intended to build on the guidance offered in the welcome kit and provide a **roadmap** describing how to kick-start or enhance your privacy program in higher education and how to operationalize it using some of the frameworks, key components, and resources mentioned in the welcome kit. In addition to offering ideas for framing your program and activities at the starting gate—as well as at the 100-day and one-year benchmarks—this roadmap offers practical guidance on how to build a program to address day-to-day privacy concerns in a higher education setting.

Top of page

Resources

HEISC Toolkits/Guides

- The Higher Education CPO Primer, Part 1: A Welcome Kit for Chief Privacy Officers in Higher Education (2016)
- The Higher Education CPO Primer, Part 2: A Road Map for Chief Privacy Officers in Higher Education (2017)
- List of Common Federal Data Protection Laws
- Tor (2016)

EDUCAUSE Resources

- EU General Data Protection Regulation (GDPR), EDUCAUSE Library resource page
- Gramm-Leach-Bliley Act (GLBA), EDUCAUSE Library resource page
- "The Chief Privacy Officer in Higher Education," May 2015 *EDUCAUSE Review* article
- "Privacy vs. Privacy," February 2015 *EDUCAUSE Review* blog
- Just in Time Research: Privacy Practices, February 2014 ECAR research report
- Data Privacy Day resource page
- EDUCAUSE Privacy Discussion List
- EDUCAUSE Higher Education Chief Privacy Officers (HE-CPO) Working Group

Initiatives, Collaborations, & Other Resources

- Electronic Frontier Foundation (EFF)
- Electronic Privacy Information Center (EPIC)
- Generally Accepted Privacy Principles (GAPP)
- Higher Education Compliance Alliance Matrix
- International Association of Privacy Professionals (IAPP)
- Privacy Rights Clearinghouse (PRC)
- World Privacy Forum (WPF)

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
ISO/IEC 29100:2011 (privacy framework)	**800-53**: Appendix J	**N/A**	**N/A**	**Cybersecurity Framework:** See methodology to protect privacy and civil liberties.	**45 CFR 160** **45 CFR 164** *(note FERPA interplay in some instances)*

Top of page

? Questions or comments? ℹ Contact us.