Sustain and Improve Your Privacy and Information Security Programs

The Higher Education Information Security Council (HEISC) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs.
Introduction
Continual technological change requires continual effort to keep an appropriate balance with privacy. While privacy principles and concerns are not limited to technology, we cannot deny that technology has a direct impact on privacy concerns in higher education. For example, research involving visual data has evolved from using handheld cameras in the late 1800s to drones flying over our campuses; U.S. campus law enforcement added dash cams to squad cars in the 1980s and started moving to body-worn cameras on officers in 2012; institutions’ data has moved from locally managed data centers to globally managed cloud platforms; data administration focus has turned from managing user authentication and access to managing data loss protection; data analytics has moved from building specialized views to today’s capabilities to collect and analyze massive, complex data sets, making it increasingly difficult to deidentify information. These are some of the changes that have pushed social, legal, and political privacy norms and are challenging traditional notions of privacy. These are the continuing challenges of the chief privacy officer (CPO).

The CPO title is commonly used for the senior-most individual in an organization responsible for the privacy department or program.¹ The Higher Education Chief Privacy Officers Working Group has created this resource to serve as a welcome kit for CPOs in higher education. It focuses on privacy considerations in the higher education environment that may differ from the considerations in other industry sectors.

For the purposes of this document, we use the term CPO to refer to the individual or role within a college or university that has primary institutional responsibility for privacy, regardless of actual title. A designated CPO is still relatively new in higher education, and not every institution has one. However, the numbers have been steadily growing since 2002, when the University of Pennsylvania named a chief privacy officer.² The titles of individuals responsible for privacy can vary widely, especially at institutions where a privacy program is nascent or still in the planning stages. Some common titles may include campus privacy officer or university privacy officer, but it is not uncommon to see titles that do not even include the word “privacy.” For example, an institution’s information security officer or legal counsel often assumes or is assigned initial responsibility for institutional privacy.³

The main audience for this document is a CPO or person with primary institutional responsibility for privacy. However, parts of this document may also be useful to:

- An individual staff or faculty member, generally without formal or prior privacy training or experience, who has been asked (or would like to be asked) to take on an institutional privacy role or help plan and shape a privacy program
- An existing privacy officer from another sector entering higher education
- An individual staff or faculty member who would like to get into the privacy field
- Existing privacy staff aspiring to become the head of the privacy unit or program (i.e., someone seeking the traditional title of CPO on campus)
Privacy in Higher Education

Privacy plays a particularly important and complicated role in higher education because of the teaching and learning—and, where applicable—research, patient care, and public service missions of colleges and universities. Moreover, it is a complex and often personal construct that holds important implications for individuals, institutions, and society at large.

Colleges and universities have multiple privacy obligations: they must promote an ethical and respectful community and workplace, where academic and intellectual freedom thrives; they must balance security needs with civil and individual liberties (see table 1), opportunities for using big data analytics, and new technologies, all of which directly affect individuals; they must be good stewards of the troves of personal information they hold, some of it highly sensitive; and finally, they also must comply with numerous and sometime overlapping or inconsistent privacy laws.

Table 1. Liberties predicated on—or partially reliant on—privacy

| Civil liberties | • Freedom of thought, speech, and expression  
|                | • Freedom of social and political activities  
|                | • Freedom of association  
|                | • Limits on authority  
| Individual liberties | • Promotion of individuality  
|                    | • Ability to grow and change  
|                    | • Autonomy and control over self  
|                    | • Ability to control how much is revealed about one’s self |

As individuals—whether as students, faculty, and staff, or as part of an institution’s extended community of alumni, donors, parents, volunteers, athletics fans and event attendees, and many others—we expect the institution to properly safeguard the data it holds about us. But as students, faculty, and staff we are also concerned with having an environment that nurtures student growth and development, as well as free inquiry, independent research, and academic freedom. Privacy is an important condition for meeting both types of expectations, and institutions of higher education therefore play a critical role in the social discourse on privacy.
The Privacy Officer and Privacy Function

Compliance has been the traditional realm of the privacy officer, and this is not uncommon today. The higher education environment also affords the opportunity and challenge to work on privacy matters that are often more abstract and complex. Because the very mission of colleges and universities includes the cultural and philosophical issues that surround academic freedom, student growth and development, and research and discovery, there are many other complex layers for higher education privacy officer engagement.

“Where does privacy live?” is a perennial question, particularly for institutions that are newly forming this function. Privacy overlays an institution’s organizational chart, with each institution anchoring the privacy function differently, depending on the culture and structure of the campus. Typically, privacy is housed within compliance, legal counsel, IT, or an academic administrative office. Regardless of organizational structure, the chief privacy officer will likely collaborate with many other administrative and academic offices to converge on an institutional approach to privacy.4

Within the boundaries set by the law and applicable regulations or contractual requirements, an institution has discretion to develop its approach to privacy. Some of the factors may include:

- Sustaining an environment where faculty and student are free to inquire, experiment, discover, speak, and participate in discourse is without intimidation
- Protecting against and responding to modern-day cybersecurity threats
- Protecting the interests of individuals and assuring they have appropriate influence over data about themselves
- Pursuing opportunities for use of data in medical treatment, research, and student success
- Enabling shared governance

The chief privacy officer plays a key role—if not a leadership role—in defining this institutional balance, often facilitating the conversations around privacy’s import for individuals, the institution, and, by extension, society.

Privacy Context: History, Frameworks, and Laws

Ideally, higher education privacy officers are not narrowly focused on compliance. However, it is important for CPOs to have a good understanding of the history of privacy,5 current privacy frameworks, and laws that have emerged over time. Appendix A provides an overview of some of the most pertinent federal, state, and international privacy laws applicable to higher education; appendix B describes common privacy frameworks and standards; and appendix C provides suggested resources for background reading.
While appendix B describes a number of frameworks used in higher education and other sectors, it is noteworthy that the most well-recognized and influential privacy framework, the Fair Information Practice Principles (FIPPs), was developed in the United States. FIPPs resulted from the 1973 U.S. Department of Health, Education, and Welfare’s seminal report *Records, Computers, and the Rights of Citizens*, which is at the core of the Privacy Act of 1974 and is mirrored in other federal and state laws, as well as in those of many foreign nations and international organizations.

**Key Areas of Focus**
Overlaid on any privacy program are the relationships with other functional roles or offices that deal with a specific aspect of privacy, many of which map to compliance with specific laws (see appendix A). Some typical examples of privacy issues in the higher education context include:

- Student education records and FERPA
- Big data, algorithms, analytics, and responsible use
- Information security monitoring and the privacy impact of surveillance
- Emerging privacy areas such as the Internet of Things (IoT), wearables, drones, location data, and augmented reality
- Open records laws and academic freedom
- Human subjects research and institutional review boards (IRBs)
- Medical schools and/or academic medical centers and HIPAA
- HIPAA on campus (e.g., student health centers, unit-based research)
- International students, scholars, and visitors
- Contractual agreements
- Credit card processing and Payment Card Industry Data Security Standards (PCI DSS), available from the [PCI Security Standards Council](https://www.pcisecuritystandards.org)

**Components of a Privacy Program**
A number of resources describe how to develop a privacy program and the underlying components of such a program. While higher education institutional privacy programs will share many similar components and areas of focus, programs will also be shaped by institutional mission and approach to privacy.

In terms of privacy program development, the International Association of Privacy Professionals (IAPP) has numerous resources, including a book on privacy program management. In addition, EDUCAUSE and NACUA published *Developing a Comprehensive Privacy Program: A Step-By-Step Guide*, written by well-known privacy academic Daniel Solove.
A number of resources describe the typical elements or components of a privacy program. The Federal CIO Council Privacy Committee published the white paper *Best Practices: Elements of a Federal Privacy Program*. Privacy consulting group Nymity offers the Nymity Privacy Management Accountability Framework, which provides a convenient “at a glance” overview of the following 13 privacy management categories, with over 100 potential privacy management activities:

1. Maintain governance structure
2. Maintain personal data inventory
3. Maintain data privacy policy
4. Embed data privacy into operations
5. Maintain training and awareness program
6. Manage information security risk
7. Manage third-party risk
8. Maintain notices
9. Respond to requests and complaints from individuals
10. Monitor for new operational practices
11. Maintain data privacy breach management program
12. Monitor data handling practices
13. Track external criteria

For those just establishing the privacy role on campus, the components needed to create, manage, and sustain a privacy program may seem overwhelming. The table in this 2015 *EDUCAUSE Review* article compares some of the distinctions between a new privacy office and a more mature privacy office. Appendix B also offers additional frameworks and standards, as well as a privacy framework comparison table.

**The Relationship between Privacy and Security**

Understanding how privacy and information security fit together, and how their domains and goals diverge, is critical when establishing a privacy program. Generally, a privacy program focuses on the laws, practices, and norms around how information is collected, used, and disclosed, as well as norms around surveillance and observation (see autonomy privacy in figure 1). An information security program focuses on protecting institutional data and the IT services that support it from cyberattacks and other types of unauthorized disclosure or access. Figure 1 outlines the synergies and distinctions of the privacy and security domains in higher education.
The information security function is critical for information privacy—for protecting personal information (as well as nonpersonal information and infrastructure) from unauthorized access. Yet frequently controls that strengthen information privacy (such as online monitoring) can weaken autonomy privacy. Balancing autonomy privacy interests with information privacy interests, as well as other values and obligations (such as transparency, accountability, functionality, and efficiency), is a unique determination for each institution. Representing privacy in these conversations is a key responsibility of the CPO and argues for maintaining this role as distinct from, but closely partnered with, the chief information security officer, as institutional circumstance allows.

What’s Next?
This primer 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. Part two of the primer will provide a roadmap describing how to create a new privacy program in higher education and how to operationalize it using some of the frameworks, key components, and resources mentioned here. Topics the roadmap will cover include:
• Establishing and formalizing the privacy role/office
• Defining the mission statement and scope of the privacy office
• Planning the first 100 days
• Developing an elevator speech
• Engaging stakeholders and collaborative partners

Acknowledgments
This primer was prepared as a group effort by a number of higher education CPOs passionate about the evolving role of privacy professionals and programs in higher education. We find our profession to be thought provoking and rewarding, and believe that privacy is a pivotal issue in the Digital Age. We hope you will find these recommendations and resources useful in establishing and improving your institution’s privacy programs.

Special thanks go to the following authors of this primer.
• Sol Bermann (University of Michigan–Ann Arbor)
• Susan Blair (University of Florida, emerita)
• Sara Chambers (Indiana University Bloomington)
• Michael Corn (Brandeis University)
• Denise Dolezal (University of California, Santa Cruz)
• Patrick Feehan (Montgomery College)
• Jeff Gassaway (University of New Mexico)
• Lisa Ho (University of California, Berkeley)
• Gary Miller (The College of New Jersey)
• Sarah Morrow (University of New Mexico Health Sciences Center)
• Geoff Nathan (Wayne State University)
• Leonard Nelson (Temple University)
• Jane Rosenthal (Colorado School of Mines)
• Scott Schafer (University Pennsylvania)
• Kent Wada (UCLA)

Additional thanks goes to the following contributors.
• Holly Benton (Duke University)
• Joanna Grama (EDUCAUSE)
• Ann Nagel (University of Washington)
• Lisa Palazzo (Case Western Reserve University)
• Rachel Krinsky Rudnick (University of Connecticut)
• David Sherry (Princeton University)
• Valerie Vogel (EDUCAUSE)
Appendix A: Privacy Laws Applicable to Higher Education

There are myriad privacy-related state, federal, and international laws. This section provides a brief overview of the laws that most higher education CPOs frequently encounter. It is prudent to identify your institution’s subject matter expert in each area to help clarify the application of laws and regulations to a particular privacy matter (e.g., registrar for FERPA, etc.)

Federal Laws

Below is a short list of major federal privacy-related laws that affect colleges and universities:

- **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. Educational records are agency or institution-maintained records containing personally identifiable student and educational data. FERPA applies to primary and secondary schools, colleges and universities, vocational colleges, and state and local educational agencies that receive funds under any program administered by the Department of Education.

- **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. However, education and treatment records defined under FERPA are excluded from coverage under the HIPAA Privacy Rule. This law is often implicated when institutions have a campus medical center or provide health insurance to employees.

- **The Gramm Leach Bliley Act of 1999 (GLBA)**: Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data. This law applies to how institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information.

- **Federal Policy for the Protection of Human Subjects (“Common Rule”)**: Published in 1991 and codified in separate regulations by 15 federal departments and agencies. The “Common Rule” 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. For example, before a developer can collect any information from a student under 13, parental consent is required. This law might apply to higher educational institutions that offer summer programming for students under age 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. Like GLBA, this law applies to how institutions collect, store, and use student financial records.

- **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. The act also requires federal agencies to collect and store only the minimum information that it needs to conduct its business and requires them to give the public notice about any records that it keeps that can be retrieved using a personal identifier (e.g., name or a Social Security number).
• Federal Information Security Management Act of 2002 (FISMA): Designed to protect the security of federal IT systems and the data contained within those systems. This law and its provisions apply to federal agencies and to contractors and affiliates of those agencies (such as educational institutions that receive a grant from a government entity). FISMA requires federal agencies to implement risk-based information security programs that conform to certain national standards.

• Freedom of Information Act (FOIA): Establishes the public’s right to request records from U.S. federal agencies and governs how and when federal agencies must share records with the public.

State Laws
There are many state laws that carry privacy ramifications to be aware of in higher education, including laws about open records, breach notification, protected health information, and even social media. The National Conference on State Legislatures (NCSL) Privacy and Security website is a good starting place to research the privacy-related laws in your state. Additionally, the NCSL tracks Internet privacy laws related to social media, commercial websites, Internet service providers, and private employers.

International Laws
Be aware that many other countries have national privacy laws that may affect international students, and cross-border research that involves data sharing. Choosing to comply with a widely recognized privacy framework will help position your institution well for most jurisdictions.

In July 2016, the European Union reached accord with the United States on Privacy Shield, which imposes obligations on U.S. entities to protect Europeans’ personal data. It reflects the requirements of the European Court of Justice, which ruled the previous Safe Harbor framework invalid. It is unclear whether Privacy Shield applies to colleges and universities, and you should consider discussing this issue with your general counsel.
Appendix B: Privacy Frameworks and Standards

The Fair Information Practice Principles (FIPPs) are the widely accepted framework of defining principles to be used in evaluation and consideration of systems, processes, or programs that affect individual privacy.

Many FIPPS are being strained and challenged by big data and data science, where transparency, individual participation, purpose specification, data minimization, and use limitation are often difficult to operationalize, and may not even be desirable.

FIPPs consist of eight privacy principles:26

1. **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
2. **Individual Participation**: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
3. **Purpose Specification**: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
4. **Data Minimization**: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
5. **Use Limitation**: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
6. **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
7. **Security**: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

In addition, FIPPs privacy principles have been incorporated into a number of different frameworks, although they may not always be the main focus of the framework. For example, NIST Special Publication 800-53 (SP 800-53, Rev. 4), which was first published in 2005, only very recently added privacy controls to the framework.27

Other common standards consulted in both privacy programs and for legislative purposes include:
• **Generally Accepted Privacy Principles**: GAPP is a framework developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). GAPP was developed from a business perspective and is described by AICPA as “designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities.”

• **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**: Originally developed by the Organization for Economic Co-operation (OECD) and Development in 1980, and recently revised in 2013, the “Privacy Guidelines” provide a framework for the international flow of information. The 2013 revisions highlight themes of risk-based privacy program implementation as well as improved interoperability on a global scale.

• **Security and Privacy Controls for Federal Information Systems and Organizations**: This NIST special publication (mentioned above) provides a catalog of security of privacy controls for federal information systems and organizations. The “Privacy Control Catalog” is structured to help organizations comply with applicable federal requirements.

• **Information technology—Security techniques—Privacy framework**: A high-level framework for the protection of personally identifiable information within information and communication information systems developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The standard provides common terminology, roles and responsibilities, safeguarding requirements, and privacy principles.

Table 1 illustrates the similarities among and between many of the privacy frameworks. All generally address the same concerns and focus areas relevant to the proper handling of personally identifiable information. Privacy officers should consider factors such as geography, political and national boundaries, business objectives and needs, commercial grouping, legal and regulatory requirements, and government affiliations when evaluating and selecting a privacy framework to use a foundation to their privacy program.
## Privacy Framework Comparison Table

Table B.1. Comparison of key concepts/principles within the noted frameworks using FIPPs as baseline

<table>
<thead>
<tr>
<th>Framework</th>
<th>Transparency</th>
<th>Individual Participation</th>
<th>Purpose Specification</th>
<th>Data Minimization</th>
<th>Use Limitation</th>
<th>Quality and Integrity</th>
<th>Security</th>
<th>Accountability and Auditing</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPPs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>N/A</td>
</tr>
<tr>
<td>GAPP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Disclosure to third parties</td>
<td></td>
</tr>
<tr>
<td>OECD</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Accountability principle</td>
<td></td>
</tr>
<tr>
<td>ISO</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

### FIPPs
- **Transparency**
- **Individual Participation**
- **Purpose Specification**
- **Data Minimization**
- **Use Limitation**
- **Quality and Integrity**
- **Security**
- **Accountability and Auditing**
- **Other**

### GAPP
- **Notice**
- Choice and consent
- Access
- Collection
- Use, retention, and disposal
- Use, retention, and disposal
- Quality
- Security
- Management
- Monitoring and enforcement

### OECD
- **Openness principle**
- Collection limitation principle
- Collection limitation principle
- Purpose specification principle
- Use limitation principle
- Quality principle
- Security principle
- Accountability principle
- Free flow and legitimate restrictions

### NIST
- **Transparency**
- Individual participation
- Authority and purpose
- Data minimization and retention
- Use limitation
- Data quality and integrity
- Security
- Accountability, audit, and risk management
- N/A

### ISO
- **Openness, transparency, and notice**
- Consent and choice
- Individual participation and access
- Purpose legitimacy and specification
- Collection limitation
- Data minimization
- Use, retention, and disclosure limitation
- Data quality and integrity
- Information security
- Privacy compliance
- Accountability
- N/A
There is no one-size-fits-all privacy standard; however, you can work to adapt existing frameworks and principles or standards, or craft your own, to ensure your framework answers primary privacy questions such as:

- Are privacy and the institution’s privacy risks properly defined and identified?
- Has the institution assigned responsibility and accountability for managing a privacy program?
- Does the institution understand any gaps in privacy management?
- Does the institution monitor privacy management?
- Are students, faculty, and staff properly trained and/or educated?
- Does the institution have an incident response plan?
- Does the institution communicate privacy-related matters and update that material as needed?

Further, the emergence of “big data” is throwing some of these foundational concepts up for renewed debate. New concepts and frameworks are emerging, such as:

- **Privacy Risk Management for Federal Information Systems**: NIST’s draft document describes a privacy risk management framework that provides the basis for the establishment of a common vocabulary to facilitate better understanding of and communication about privacy risks and the effective implementation of privacy principles in federal information systems.
- **White House Precision Medicine Initiative: Privacy and Trust Principles**: This document articulates six main governing principles and lists objectives for each.
- **LACE DELICATE Checklist**: This eight-point checklist is designed to allow educational institutions to better frame and account for ethics and privacy discussions around learning analytics.
- **Data benefit analysis (DBA)**: Authored by members of the Future of Privacy Forum, this white paper offers a framework for a “reasoned analysis to balance big data benefits against privacy risks.” Risks identified through the traditional privacy impact assessment (PIA) must be balanced against the benefits identified through the DBA.
- **Consumer Privacy Bill of Rights**: This document proposes that the Consumer Privacy Bill of Rights apply to commercial uses of personal data—that it “applies FIPPs to an environment in which processing of data about individuals is far more decentralized and pervasive than it was when FIPPs were initially developed.”
Appendix C: Professional Resources

Many resources are available when you need support and guidance, both from colleagues within higher education and more generally in the privacy field.

To connect with the privacy community at large, begin following or subscribing to free mailing lists, newsletters, announcement lists, and blogs, then choose a book or two to expand your knowledge.

Professional Associations

- EDUCAUSE is a nonprofit association whose mission is to advance higher education through the use of information technology.
  - The HE-CPO Working Group ([chart](#), [members](#)) provides a supportive and collaborative environment to share information and speak freely regarding privacy issues, news, laws, concerns, and best practices affecting higher education. Membership is by invitation only; please see the charter for eligibility and contact information.
  - This working group is part of the HEISC that leads the EDUCAUSE Cybersecurity Initiative.
  - The EDUCAUSE Privacy Discussion Group is open to all for discussion of privacy-related topics in the higher education context.

- The IAPP (International Association of Privacy Professionals), the world’s largest global information privacy community, offers a variety of professional certifications, as well as privacy program resources. A special higher education membership rate is available.
  - IAPP Certification Program

- The mission of NACUA (National Association of College and University Attorneys) is to advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve.

Privacy Advocacy Organizations

- EFF (Electronic Frontier Foundation)
- EPIC (Electronic Privacy Information Center)
- PRC (Privacy Rights Clearinghouse)
- WPF (World Privacy Forum)

Legal and Regulatory Resources

FERPA

- Department of Education (ED) and the Department of Health and Human Services (HHS), “HIPAA/FERPA Joint Guidance”
- ED, “Family Policy Compliance Office”
- ED Privacy Technical Assistance Center (PTAC), “PTAC Toolkit”
- ED PTAC training videos
- FERPA/Sherpa student privacy resource center
HIPAA

- HHS Office of the National Coordinator for Health Information Technology (ONC) and Office of Civil Rights (OCR), “Health IT Privacy and Security Resources”
- HHS ONC OCR, “Guide to Privacy and Security of Electronic Health Information”
- Subscribe to the OCR-Privacy-List mailing list

Reading List

Higher Education Focus


General

- IAPP Resource Center, “Intro-level Privacy Books.”
- David Snyder, *The NSA’s “General Warrants”: How the Founding Fathers Fought an 18th Century Version of the President’s Illegal Domestic Spying* (a discussion of privacy’s role in the American Revolution and Fourth Amendment).

Media

Twitter

- @DailyDashboard—Top privacy and data protection news from the IAPP publications team
- @DataPrivacyDay—Data Privacy Day is an international effort held annually on January 28 to create awareness about the importance of privacy and protecting personal information
- @DataPrivacyNtwk—Data privacy and online security consultants, speakers, and resources
- @HEISCouncil—A Twitter feed for the EDUCAUSE Cybersecurity Initiative
- @MKaiserNCSA—The Twitter feed of Michael Kaiser, the executive director of National Cyber Security Alliance; NCSA leads STOP THINK CONNECT, National Cybersecurity Awareness Month, and Data Privacy Day
News

- **Passcode from the Christian Science Monitor**—A modern field guide to security and privacy. Passcode produces smart, groundbreaking journalism focused on security and privacy in the Digital Age.
- **IAPP Daily Dashboard**—A daily newsletter summarizing the day’s top privacy-related stories from around the world with links to the full articles (available via e-mail or online).

Notes

1. Please note that this document is intended for college or university CPOs generally, rather than HIPAA-mandated privacy positions.
2. University of Pennsylvania March 28, 2002, announcement, “First chief privacy officer named.” Also see the *EDUCAUSE Review* article “The Chief Privacy Officer in Higher Education” (May 2015), which provides additional background information.
3. Such individuals must be mindful that they are wearing two related, but distinct, hats.
4. The question “Where does privacy live?” will explored in more detail in part 2 of this primer.
5. This primer provides an overview of privacy and how privacy issues play out in the higher education environment. There are a number of excellent resources discussing privacy concepts generally, from the history and development of modern privacy as both a legal right and a societal norm, to understanding privacy as a social and civil justice issue. Additional resources are listed in appendix C. You can also watch an 8-minute video by PBS Digital Studios about online privacy.
6. Big Data in the Campus Landscape is an ECAR series of papers that introduces the concept of big data; discusses basic infrastructure support issues that may arise, as well as related security, privacy, and compliance issues; and examines current data-curation activities.
7. Examples include UCLA’s Principles of Scholarly Research and Public Records Requests and the University of Wisconsin–Madison Chancellor’s message on academic freedom and open records.
8. Contracts with third parties, cloud services providers, and other vendors generally may include boilerplate privacy-related provisions. However, an institution may prefer to include its own privacy protection statements in third-party contracts.
10. For more information, see the Nymity Privacy Management Accountability Framework website.
11. The Privacy Maturity Model published by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) offers a framework for establishing and assessing privacy program maturity benchmarks.
14. See joint guidance on HIPAA and FERPA to student health records and HHS.gov FERPA and HIPAA FAQ for guidance on this complex overlay of federal regulation.
22. Often called Sunshine Laws, open record laws mandate that certain state records and reports be open to the public for review and inspection.
23. Laws specifying the circumstances under which a breach of personally identifiable information must be disclosed to state residents.
24. Laws specifying how the state must protect medical and mental health records and communicate with patients (in an electronic medium).
25 Laws designed to protect employees and students from being asked to grant third parties such as employers, potential employers, and schools access to their social networking accounts.

26 See this overview of FIPPs.


28 See the American Institute of Certified Public Accountants, *Generally Accepted Privacy Principles*.


30 See NIST Special Publication 800-53 (Rev. 4).


33 See NISTIR 8062 DRAFT Internal Report on Privacy Risk Management for Federal Information Systems, also available as PDF.
