The Higher Education Chief Privacy Officer Primer, Part 2

A Roadmap for Chief Privacy Officers in Higher Education

HEISC Working Group Paper

AUGUST 2017

HIGHER EDUCATION INFORMATION SECURITY COUNCIL

EDUCAUSE

Table of Contents

Introduction 3

First Things First 4

What Is Your Job Description? 4

What Are Your Resources? 6

What Is Your Mission? 7

What Is Your Privacy Elevator Speech? 7

The First 100 Days 7

Get to Know Your Stakeholders and Collaborators 8

Conduct an Environmental Scan of Information Use and Data Policies 9

Refine Your Elevator Speech 12

The First Year 13

What's Next? 16

Acknowledgments 17

Appendix A: Some Notes on a Good Privacy Elevator Speech 19

Appendix B: Data Inventory Template 22

Appendix C: Additional Resources 23

Privacy Impact Assessment Templates 23

Privacy Program Maturity Models 23

Appendix D: Growing as a CPO in Higher Education 24

Conferences and Networking Opportunities 24

Paying It Forward 25

This second part of the primer on chief privacy officers in higher education provides a roadmap for those who are new to the role of privacy leadership or new to a campus environment.

Introduction

Welcome to the world of higher education privacy!

In August 2016, the Higher Education Chief Privacy Officers Working Group created The Higher Education CPO Primer, Part 1: A Welcome Kit for Chief Privacy Officers in Higher Education. The purpose of the welcome kit was to focus on privacy considerations in the higher education environment that may differ from those in other industry sectors. This document 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.

The roadmap is designed primarily for those currently in higher education who are new to the CPO or privacy leadership role. As noted in the welcome kit, the titles of individuals responsible for privacy can vary widely, especially at institutions where a privacy program or the privacy function is still new or in the early stages of development. While the roadmap's focus is providing advice to someone already in higher education who is new to the privacy role, part of this document may also be useful to a seasoned CPO or privacy professional who may be new to the higher education sector.

As the privacy profession gains traction globally across industries, the CPO in higher education is emerging as a specialized privacy practitioner who handles issues and concerns unique to the college and university setting, for example:

- Student health centers may be required to comply with FERPA[1] with respect to the health records of their student patients and with the HIPAA[2] Privacy Rule with respect to the health records of their nonstudent patient populations. The higher education CPO may be advising the university on the differences between HIPAA and FERPA regarding limitations for disclosures for public health or research.

- Universities often act as Internet service providers for the campus community, not only to carry on the institution's administrative operations but also for students and others living in campus housing and for researchers conducting politically, socially, or economically sensitive studies. The higher education CPO may be guiding the university in establishing appropriate practices to keep data secure while protecting the privacy of community members.
- Public colleges and universities may ask their CPOs to weigh in or make determinations on the appropriate balance of privacy, transparency, and public interest in their disclosures of research for Public Records Act obligations.
- Institutional review boards may consult with their CPO on whether a research activity will cause greater than minimal privacy risk and how the Common Rule's requirements intersect with FERPA or HIPAA.

To orient you to your role in addressing these higher education privacy challenges, this document is organized into the following sections:

- A privacy program roadmap, focusing on privacy program activities that you will want to consider at the outset and at the 100-day and one-year benchmarks
- Guidance on how to deliver a compelling elevator speech about privacy (Appendix A)
- Guidance on how to create a data inventory (Appendix B)
- Guidance on conducting a privacy impact assessment (PIA) (Appendix C)
- Guidance on how to grow in your role as a higher education CPO, including professional resources and a brief list of recommended readings (Appendix D)

First Things First

Now that you've been hired, what are some of the first things you should consider? This list offers suggestions on how to take stock of your new role and function before jumping in.

What Is Your Job Description?

You probably read the job description when you were applying, but now that you're here, pull it out and read it again, with an eye toward using it to guide your future actions. Figure out if you have any authority—directly, or through your unit—to oversee privacy awareness efforts or to engage others in order to

influence the privacy culture of your institution. Examine the following factors and consider how privacy was described to you on hire, as well as what you know about how privacy fits at your institution in relation to any partners.

- What does the job description emphasize?
- Whom do you report to, and what group are you a part of? This may influence how you approach your duties, your authority to make decisions or implement change, and how others view your role.
  - Are you co-located with another unit, and, if so, what is the culture of that unit? This may impact how others see you.
  - Are you part of IT, information security, audit, compliance, ethics, legal, risk management, or some combination of these? It helps to understand the philosophy that underpins your position as you start to develop your privacy function.
  - Where is information security in the organizational chart? If you are not part of that department, you'll need to find out where they are pretty quickly and determine how to partner with them.
  - Are you an academic or administrative unit?
  - Is there a policy office, and, if so, are you part of the office?
- What is the scope of your authority? Do you have authority across the entire institution or only in certain departments? Are there other domain-specific privacy officers whom you may need to work with on campus (e.g., a HIPAA privacy officer or FERPA specialist)?
- Do you have shared responsibility for incident response or breach notifications at your institution? It is important to understand the incident-response process at your college or university.
- Does anyone report directly to you? If so, what are their job duties, and how can you best work together to create and maintain a successful privacy program or department?
- Do you have responsibility for existing policy or procedures, or do you ensure compliance through the activities of other units?
- Do you have responsibility for training on relevant policies and procedures, or does another unit manage this?

What Are Your Resources?

Take the time to understand the direct and indirect resources that you have at your disposal to influence campus privacy activities. Important resources include:

- **Staff:** Do you have full-time, part-time, or partial support? Working in higher education does have its perks in terms of access to student labor. Find out if you have access to a work-study or internship program. Students seeking credit or experience can be a valuable resource if you need website work performed, information turned into presentations, or basic document or forms design. Student workers can also plug you into the level of student knowledge (or lack thereof) on privacy issues and on how to best increase student awareness.
- **Budget:** Do you have a budget for privacy activities such as outreach or design and development? Will you be able to provide incentives, training tools, or communication tools for reaching out to your community? Now is also the time to find out if you have a personal professional development budget so that you can keep your own skills sharp in order to bolster your program.
- **Communities, Partners, and Allies:** Is there an existing privacy advisory group or committee on campus? If so, consider how to contribute (e.g., lead or interact with it). If there isn't such an advisory group, now is the time to start considering who should be on such a group to advance the campus privacy program. Do you have access to any other existing communities on campus, and can you partner with them to brainstorm and share information about privacy activities? Such communities could include, for example, department liaisons in legal, risk management, compliance, audit, or information security offices; governance groups; policy committees; data administration groups; records management groups; or research-based committees like an IRB.
- **Compliance Tools:** What campus tools are available that you can use to track privacy issues? Do these tools have the potential to collect data for metrics down the road? Some examples may include a learning management system or tools used for case management, IT GRC compliance, incident tracking, or ethics reporting. If you don't have access to an established tool, consider how you are going to track institutional privacy issues and projects, as well as metrics, for your program. Even a spreadsheet can be a useful tool to communicate the extent of your privacy activities.[3]

What Is Your Mission?

Knowing your institution's mission, as well as the privacy office's mission, will help you develop the primary drivers of your privacy program. Keep in mind that privacy values may differ from campus to campus. While it may be helpful to research other privacy office mission statements, make sure you take the time to explore your institution's campus culture and existing attitudes toward privacy.

- How will your privacy office mission support the institution's mission? Does your mission include the concepts of information privacy, academic freedom, and autonomy privacy?
- Is this a functionally established, vibrant activity or a newly identified activity that requires grooming?

What Is Your Privacy Elevator Speech?

If you were to ask a group of people what privacy meant to them, you would likely get a different answer from each person. When some people think of privacy they think of data compromises; some envision ubiquitous surveillance and Big Brother; others may have something else in mind. The broad range of possible definitions for privacy makes it challenging to demonstrate why privacy warrants the allocation of scarce resources. Your privacy elevator speech should crisply convey what you do to protect the privacy of people whose data are collected and used by the university and why this protection is important. Your elevator speech will hopefully provide that "aha" moment to help others recognize why privacy is crucial in the higher education environment. A long, detailed explanation won't accomplish this. Instead, you need a sound bite—something that will immediately resonate with people and that can be conveyed in the time it takes to share an elevator ride.

See Appendix A for suggested tips as you begin to develop an elevator speech about privacy for your institution. An example is provided.

The First 100 Days

The first 100 days is often used as a metric of progress for new administrations and programs. This is because the first 100 days is a time of transition, which can be a very challenging time for leaders.[4] Use this time to establish yourself as the new campus privacy leader and build collaborative relationships that will assist you throughout your tenure at your institution.

Get to Know Your Stakeholders and Collaborators

There are a number of campus stakeholders you should get to know immediately. Introduce yourself right away to the campus chief information security officer (CISO), chief information officer (CIO), and general counsel, as well as leaders of internal audit, records management, procurement, public records (if applicable to your institution), campus policy, ethics, and compliance. At institutions where the CPO function is new, keep in mind that some or all of these stakeholders may have been responsible previously for some privacy functions, either formally or informally. For instance, the registrar may be the campus data steward for student records and most likely has significant knowledge and expertise about the privacy requirements of FERPA. Even though higher education tends to encourage a very collaborative working environment, it is always helpful to be mindful of your approach to avoid stepping on another person's toes.

During the first 100 days, most CPOs will be in discovery mode. You'll be meeting with campus stakeholders and potential collaborators. You'll be joining any existing privacy advisory committees or working groups—or thinking about how to create them. At the same time, you'll be doing an initial environmental scan to identify highest risks and quick wins and beginning to plan your data inventory approach by learning who the data stewards and custodians are. And you'll be refining your elevator speech that reflects your privacy program's mission, resources, and activities.

Plan to introduce yourself to faculty leadership and student government leaders. Both of these groups are integral to life on campus, and you can meet with the leaders of each group to see if there are already campus privacy champions who might be able to assist you with your privacy program and its initiatives. Also introduce yourself to deans and department heads, functional leaders responsible for stewardship of records (e.g., registrar, employee benefits, HR, wellness centers, archivist, athletics leaders), and IT personnel in charge of campus-wide data systems.

Although the roles that support privacy may be located in expected departmental units (CIO, CISO, general counsel, audit), sometimes roles involving privacy are not as evident. Campuses with hospitals or medical centers will have a privacy officer who manages the privacy requirements of HIPAA. Student health centers have different considerations for treatment records under FERPA.[5] Universities are frequently "hybrid covered entities" under HIPAA and require that distinctions be drawn between HIPAA-covered and non-HIPAA-covered parts of the institution. As a campus privacy officer, you may find yourself working with medical center privacy officers to manage disclosure of health information to

researchers and others in academic parts of the institution in compliance with HIPAA, FERPA, and the Common Rule for Protection of Human Subjects.[6] Policy institutes, IRBs, or researchers who work with a lot of personally identifiable information (PII) (e.g., in sociology, psychology, medicine, music therapy) are also stakeholders who might have privacy expertise to share or a role to play in the institution's privacy program. Additionally, archived data can be found everywhere, and space/facilities management might be able to help you find and identify where paper records or historical files are stored.

As you meet your stakeholders and future collaborators, identify the privacy champions you want to leverage for your program, as well as campus leaders and administrators who may not understand the distinct role of protecting privacy and may need more care and persuasion before they understand the importance of privacy to the institution and become privacy champions.

Conduct an Environmental Scan of Information Use and Data Policies

You already understand that there is a lot of data in motion at higher education institutions. In addition to data collected on employees (and their families if employment benefits are provided), students, and applicants, institutions hold data on alumni, donors, and people who purchase services from the institution (such as concert and athletic events tickets or meal plans). If the institution conducts any sort of community outreach or research, then it will collect data about those activities and who makes use of them. Find out about the different types of data collected on campus and understand if there is a data life-cycle plan in place for how those data are collected, used, maintained, and destroyed (see figure 1). In essence, you need to create a data inventory (see Appendix B).

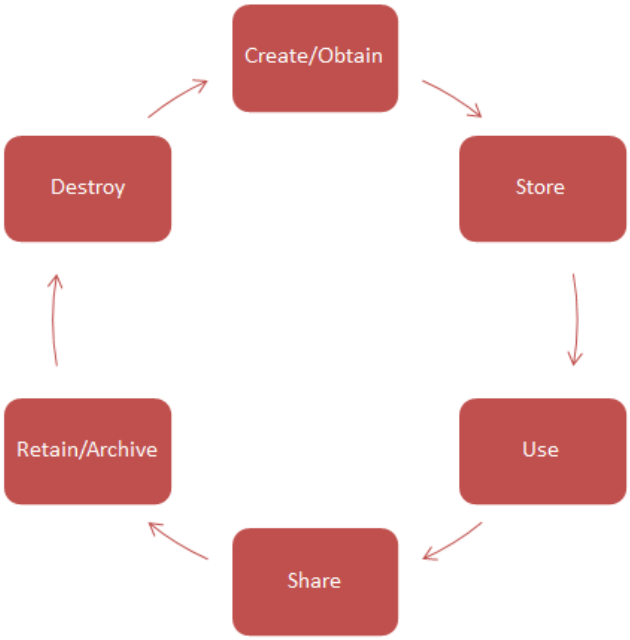

Figure 1. Data life cycle

Be aware that this could be an enormous task. At large, comprehensive research universities in particular, data are likely to be extremely widely dispersed, and even centralized data stores are likely to be complex, with data spread among many disparate systems (not only the usual ERPs but also a customer relationship management system, the LMS, and other systems). Questions to ask include:

- What are the institution's policies regarding data governance? Investigate whether there are formal (written) and informal policies and standards in place regarding the collection, storage, sharing, use, and destruction (information life cycle) of data. Ask whether these policies are enforced, and, if so, how? Also determine whether there is a data classification policy that establishes separate handling requirements for different classes of data. Be sure to ask about informal practices as well because you may need to identify practices that need to be revised in order to maintain information privacy. This is also a good time to gauge general awareness of the institution's data governance policies. Ask people if they ever receive training on those policies and data handling requirements. This will help you identify which units or departments may need some additional privacy attention.
- The Records Management Services/Office within an institution (especially a public institution) manages and oversees compliance with state and federal laws and regulations relating to the preservation and destruction of information created and received by the institution. Most will have a records-

retention schedule for determining how long electronic and paper records must be retained and their location. This is often a great place to unearth records, investigate the extent to which they may contain PII, and explore the gaps between what you have learned about records management and your institution's retention schedule. Do you have warehouses full of paper records? What are the relevant retention schedules, and is anyone managing the disposition of those records? Does your retention schedule apply across all media, or is there a gap for records held in certain formats? Does the retention schedule address archiving as well as destruction or disposal requirements?[7]

- Learn about the document scanning practices at your institution: Is PII redacted? Where and how are scanned documents stored? Who has access to these scanned records? Are records management retention policies tied to the document scanning workflow? Are there any mandated protocols when scanning official institutional records (e.g., state agency requirements for official state records)?
- What are the policies on ownership, handling, and disposition of data (research, student, administrative, or intellectual property) and devices that store this information when faculty, staff, or students separate from the institution (off-boarding)? Consider these issues and document them in guidance or policy to ensure a consistent approach.[8] What are the policies on the intermingling of personal and institutional data while associated with the institution? What happens to these data upon separation? Who is responsible for ensuring that the person leaving the institution understands and follows data-handling policies (HR, IT, privacy)?
- Are there existing data asset inventories? Ask specifically about data (student, faculty, staff, etc.) containing PII and research data. It also helps to ask specifically about imaging data and data collected in response to surveys (e.g., satisfaction or business process surveys) as well. Important questions to ask include:
  - Who are the data stewards and custodians, and what are their roles? Are these responsibilities formalized and clearly articulated to the holders of those roles and to others?
  - How were the data **acquired**? Ask specifically whether the data were created at the institution, received from another source (individuals, third parties, contractors, federal agencies, etc.), publicly available, or part of legacy systems.

  - How are the data **stored**? This question can surface many additional questions and conversations, such as these: Are the data stored on premises or in the cloud? Are the data stored in a central repository (data warehouse), and does the unit or department maintain any secondary (aka "shadow") data storage systems? If the unit maintains a secondary system, how is it maintained? Do all the storage mechanisms follow university policy, particularly data governance, records retention, compliance, and encryption policies?
  - What is the main method for data **transfer** on or off campus, and is that method secure? Ask specifically whether cloud-based sharing mechanisms are used or whether e-mail is the main transfer method.
  - Are the data shared with third parties (e.g., consultants, data processors, auditors)? How are third parties involved in data sharing and use, and are there agreements in place with third parties about data use?
  - How and by whom are the data **used** and accessed? Ask specifically who has access to what data and how that access is governed. Does the university have policies in place to grant access to data based on need-to-know standards, to engage in periodic access review, and to terminate access to data when such access is no longer needed?
- What is the institution's data-breach history, and what is the CPO's expected role in a data breach? Are you part of the assessment as to whether a data incident is considered a reportable breach or just a teachable moment? Are you part of the process or the responsible party to conduct breach notification? Forewarned is forearmed. Be sure to ask what the institution's experience is with data breaches—when, where, and how? Also ask how incident response is handled for paper and electronic data-breach events. Is there an incident response policy or process that is documented and followed, and are you part of it? Now is also a good time to make sure that you are familiar with your state's data-breach notification laws, as well as any federal standards that may apply to the data in use at your institution.[9]

Refine Your Elevator Speech

Within the first 100 days, continue refining your elevator speech (see Appendix A). As you learn more about the institution, your stakeholders and collaborators, and the privacy practices in place at the institution, you can finesse your elevator speech to reflect the pulse of the campus and show that you are keenly aware of your community's unique values, priorities, and obligations in regard to privacy.

The First Year

With the first few months under your belt, you are now ready to map out your goals for the first year and identify longer-term goals for your privacy program. The following checklist offers some high-profile quick wins that you can accomplish in the first year to help boost your visibility at your institution, as well as suggestions for foundational work to help establish roots to anchor your longer-term agenda.

During the first year, most CPOs will be actively establishing the privacy program's visibility (or their own visibility) on campus, identifying goals as part of the program's overall strategic plan, and addressing short-term goals while undertaking the foundational work for longer-term goals. As a CPO in your first year, think of yourself as starting a journey—you are building your privacy roadmap by identifying your route and selecting the vehicles that will help get you to your destination.

- Publish your mission statement, vision, charter, strategic plan, and annual goals for the privacy office.[10]
- Show up everywhere where privacy may be an issue. Be the ultimate champion. Give talks. Write articles. Have a presence on social media.
- Network and collaborate with your peers by finding groups that allow you to share and compare strategies, pitfalls, ideas, professional development opportunities, and more. For example, the EDUCAUSE Higher Education Chief Privacy Officers Working Group meets on a monthly basis to share and create resources. The International Association of Privacy Professionals (IAPP) also offers ways to connect with other privacy professionals around the world.
- Sign up as a champion for Data Privacy Day (January 28) every year. Consider partnering with other institutions in your region that celebrate Data Privacy Month (observed every year between January 28–February 28).
- Offer to work with the security function during National Cyber Security Awareness Month (October).
- Be an active participant in the software development and acquisition process, as well as the review of procurement and service contracts involving the collection of, the use of, access to, or the storage of protected data (e.g., PII, Payment Card Industry Data Security Standard [PCI DSS], protected health information [PHI], etc.). Work with campus counsel to establish a template addendum for standard data privacy and security requirements, and get involved as necessary in high-risk or unusual contract negotiations.[11]
- Offer training (online, class-based, or both) on privacy topics such as FERPA or university data policies.

- Develop an internal list of projects and initiatives for the second year, which may include:
  - Establishing a privacy office (if this did not exist before you were hired as the CPO)
  - Reviewing and updating policies that need to be revised
  - Establishing/reviewing privacy notices (website, annual FERPA notifications), standards, and/or processes
  - Starting down a "privacy by design" path to build privacy safeguards into campus administrative processes[12]
  - Establishing a privacy impact assessment program that will allow you to assess new projects and initiatives as well as monitor existing processes and procedures
- Continue engaging campus stakeholders and collaborators:
  - HR, registrar, information security officer, internal audit, government relations, records management, policy officer, risk management, compliance officers, librarians, research administration, safety/police, etc.
  - Individuals with elements of privacy compliance embedded in their roles
  - Relevant committees—add privacy issues to the agendas of existing committees on compliance, audit, policy, risk, governance, data stewardship, security, IT, transparency and accountability, physical security, and surveillance; and consider whether a new committee is needed to address any of these areas for students, faculty, and staff[13]
  - Faculty, researchers, and student groups whose interests involve privacy or data protection in some way
- Develop a communications/outreach strategy:
  - Define an outreach plan for your basic message: the university's philosophical approach to privacy. Look to your privacy elevator speech, mission statement, vision, charter, or strategic plan to develop this message.
  - Develop an approach for topical, timely, and call-to-action (tips) messages.
  - Develop a matrix or playbook for how to reach your target audiences. Consider different vehicles for reaching different stakeholders (e.g., blogs, tweets, web presence).

- See if it's possible to draw on the departmental or campus marketing and communications functions.
- Consider leveraging existing committees or more informal networks of campus stakeholders to spread the privacy message.
- Evaluate/establish the privacy function's web and social media presence:
  - How can you improve it or create a web presence if none exists?
  - Learn the mechanics of your content management system and how people are driven to pages you create and curate.
  - Talk with your institution's communications staff about how to partner with them on social media:
    - Will your function have its own Facebook page or Twitter account? Or will you leverage your institution's existing social media accounts?
    - How will you resource these social media accounts in terms of staff and content?
    - What does the institution monitor regarding social media?
      - Who is monitoring?
      - What are they monitoring?
      - What are the rules in existence or that are needed?

- Define the privacy guidelines and expectation for the privacy office itself: What is the level of confidentiality for individuals who contact you with complaints or concerns? Be sure to consider the implications of mandatory reporting requirements and, for public institutions, the overlay of public records and public information laws, as well as other possible reasons for disclosure.
- Begin working on the areas of highest risk identified in your environmental scan. Cultivate the buy-in of leaders in these high-risk areas to gain the organizational clout to implement needed changes.
- At the end of your first year conduct a program maturity assessment. There are several frameworks and privacy maturity models that can be adapted (see Appendix C).
- Publish a report speaking broadly about what's been accomplished and what's to come. Although an annual report may be ambitious for your first year, you may want to publish a blog or short summary about a measurable accomplishment. For example, see this Data Privacy Day summary from Indiana University.

What's Next?

> "[T]he power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do."
>
> —President Barack Obama, "Obama's Speech on N.S.A. Phone Surveillance," *New York Times*, January 17, 2014

The job of a higher education CPO is never done. While you are tackling identified gaps, mitigating high-risk issues, and addressing major strategic initiatives, changes in technology, in laws and regulations, and in societal attitudes mean that an institutional privacy program is constantly facing new challenges. Meet these challenges head-on by evolving in response to a changing world; scan for hot topics on a regular basis to stay current and keep your campus community informed and prepared. In a world of pervasive technology, big data, and heightened surveillance by government, the private sector, and even higher education, privacy must be "baked in" to ongoing practices. Privacy is not an end state. It's both a collaborative process and a commitment to community values.

Words of Wisdom from Higher Education CPOs

- Privacy is a process, not a solution. Work on embedding it in operations, program management, application development, etc.
- When evaluating and implementing new technologies or security safeguards, keep in mind privacy by design, simplified user choice, and transparency and respect for privacy rights.
- Privacy values change with cultures and generations—continually evolve your program.
- Position privacy as an enabler rather than a hurdle; be a collaborator rather than a naysayer.

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 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)
- Sara Chambers (Indiana University)
- Michael Corn (University of California, San Diego)
- Denise Dolezal (University of California, Santa Cruz)
- Patrick Feehan (Montgomery College)
- Jeff Gassaway (University of New Mexico)
- Lisa Ho (University of California, Berkeley)
- Alex Jalso (West Virginia University)
- Micki Jernigan (University of North Carolina–Chapel Hill)
- Gary Miller (The College of New Jersey)
- Ann Nagel (University of Washington)
- Geoff Nathan (Wayne State University)
- Leonard Nelson (Temple University)
- Jane Rosenthal (Colorado School of Mines)
- Rachel Krinsky Rudnick (University of Connecticut)
- Scott Schafer (University of Pennsylvania)
- Kent Wada (UCLA)
- Cheryl Washington (University of California, Davis)
- Ronise Zenon (University of California, San Diego)

Additional thanks goes to the following contributors:

- Holly Benton (Duke University)
- Susan Blair (University of Florida, emerita)
- Joanna Grama (EDUCAUSE)
- Carolyn Heald (Queen's University)
- Lisa Palazzo (Case Western Reserve University)
- David Sherry (Princeton University)
- Robert Turner (University of Wisconsin–Madison)
- Valerie Vogel (EDUCAUSE)

Notes

1. Family Educational Rights and Privacy Act of 1974 (FERPA), U.S. Code, vol. 20, sec. 1232g (2012); 34 CFR Part 99.
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA), U.S. Code, vol. 42, sec. 1320d (2012).
3. The Higher Education Compliance Alliance maintains a helpful Compliance Matrix.
4. Michael D. Watkins, "Why the First 100 Days Matters," *Harvard Business Review*, March 23, 2009.
5. See "Does FERPA or HIPAA Apply to Records on Students at Health Clinics Run by Postsecondary Institutions?" U.S. Department of Health & Human Services, HIPAA FAQs for Professionals.
6. See Basic HHS Policy for Protection of Human Research Subjects (45 CFR 46, Subpart A).
7. Learn more from the "Records Retention and Disposition Toolkit," *2014 Information Security Guide*.
8. For example, see the University of Pennsylvania's Guidance on Disposition of Documents and Data of Faculty and Staff Who Are Leaving Penn or Have Left Penn.
9. The National Conference of State Legislatures (NCSL) provides a comprehensive list of security breach notification laws. For additional information on recent breaches, the Privacy Rights Clearinghouse maintains a Chronology of Data Breaches.
10. For an example, see the University of Pennsylvania's Information Security and Privacy Program Charter.
11. For an example, see UC Berkeley's Data Privacy and Security Appendix.
12. Learn more about the privacy by design approach.
13. Two committees that have been chaired by the CPO at UC Berkeley include the Information Risk Governance Committee (IRGC) and the Campus Information Security and Privacy Committee (CISPC).

Appendix A: Some Notes on a Good Privacy Elevator Speech

As the champion for privacy at your institution, you must have a good elevator speech. You'll be using this over and over and over again to educate the campus community on why privacy issues are of institutional importance. In addition, if you are new to the privacy role but not new to your institution, you can also use your elevator speech to distinguish your new role from your former one. (This can be especially important if you are keeping some of your old job duties in addition to your new privacy responsibilities.)

What makes a good elevator speech? It must be:

- Clear and succinct—a compelling sound bite
- Short enough to deliver in an elevator ride (under one minute)
- Focused on a single topic or important strategy
- Positive and forward-thinking
- Interesting and able to move people to action*

To help develop your privacy elevator speech, focus on addressing the following topics:

- Describe your privacy initiative(s).
  - Briefly explain what you do and your privacy initiative (or planned initiative) in one or two sentences. Use nontechnical terms and avoid jargon.
  - Identify who benefits from the privacy initiative you described.
  - Share why the initiative is needed on campus.
- Provide compelling reasons for the listener (and campus community) to participate in the privacy initiative. You can tie the initiative to institutional mission and goals, or you could focus on how it supports core human values. Other questions that you may want to address include:

* Shirley Payne, assistant vice president for information security, policy, and records at the University of Virginia (retired), offered these tips for developing a good elevator speech, as well as an elevator speech outline (from a 2009 Security Professionals Conference seminar).

  - What distinguishes this particular strategy from its primary alternative?
  - What makes it a good choice?
  - How does it differ from the information security officer's role?
- End with a call to action for the listener to support the privacy program or initiative. Be prepared to let the listener know exactly what he or she can do to support you and your initiative. You may not always have the same call to action for each person that you talk to. Some ideas for action include:
  - Visit a web page to learn more.
  - Attend an event.
  - Volunteer to teach others about the initiative.
  - Continue the dialogue with the privacy program (e.g., follow-up meeting or discussion).
  - Provide professional or monetary support.

The following sample elevator speech is a slightly modified version of an elevator speech developed by the former CPO at the University of Florida:

> *"Hey, have we met? I'm Susan Blair, the chief privacy officer for the University of Florida.*
>
> *People often wonder why UF has a privacy office. It can be simply stated: We safeguard individual privacy rights that have been dictated by law. So whether we're talking about student privacy rights, patient privacy rights, or financial privacy, it's the privacy office that shoulders the accountability for protecting all types of restricted data.*
>
> *Most privacy rights focus on information, and more specifically, personal information. And our customers—students, faculty, staff, patients, alumni, and others—trust that we will keep their information confidential. To meet this expectation, we, the privacy office staff, provide consultation, advice, and training. We also respond to complaints and reported incidents with investigations, and if necessary, with sanctions.*
>
> *Why is this important to you? Because your information may be involved, and without protections, you might lose the freedom to make decisions about how your information will be used. Protecting everyone's privacy also helps maintain the university's reputation and integrity. When you do business with UF, whether as a student, patient, or creditor, you can expect this same protection for your personal information.*

For us to succeed, we need you to join our effort to safeguard all private information. We need you to complete your role-specific training, ask for appropriate identification when dealing with restricted data, and report any privacy-related complaints or incidents immediately.

You can call us with any privacy question. Just last week, a caller asked if an individual could use their arrest mugshot as a form of identification. No, I'm not making this up! By the way, do you know the answer?

Contact us if you need assistance with any privacy matters or if you have a privacy-related question. Remember, when it comes to information and privacy, it's personal. Be aware before you share, and when in doubt, give us a shout.

Oops, this is my stop. Make it a good day!"

It is important for all professionals to be prepared with a good elevator speech, even on your first day in a new role. Remember that you can evolve and refine your elevator speech as your program matures. Practice and be prepared to recite it with ease and confidence!

Appendix B: Data Inventory Template

A data inventory can be a useful tool to help you understand what data are used at your institution, where those data are located, how they are used, the sensitivity of the data, and the impact to your institution in the event of breach or loss. A data inventory can be stored in a tool created for that task or in a database or spreadsheet. It can be as simple or sophisticated as your resources allow. The table provided here is a simple list of data elements that could be included in a data inventory spreadsheet.

Table 1. Sample data inventory template

Data Element	Example Response
Data Set*	*Whistleblower complaints*
Data Element/ Type of Data	*Report description, whistleblower name/contact info (not required)*
Data Source	*EthicsPoint system (external vendor)*
Data Classification†	*High (reputational impact), potentially high retaliation risk to reporter*
Notice Triggering?‡	*Does not trigger state notification law*
Functional Owner/Data Steward	*Whistleblower investigations department; ethics, risk, and compliance*
Data Custodian/IT Service Provider	*External vendor, such as EthicsPoint*
When Collected or Received	*Submission of report by reporter*
Who Has Access	*Whistleblower investigators, locally designated official, resolution team*
Where Stored	*EthicsPoint system, whistleblower departmental file share*
How Used	*Investigate complaints*

* Start by identifying the big categories of data (data sets). If/when resources allow, move on to identify each data element within the data set.

† What is the level of risk to the institution if the data are compromised? What level of security protections are required? Consider confidentiality and data integrity as well as business continuity in case data are unavailable. See, for example, UC Berkeley Data Classification Standard.

‡ Impact in the event of breach: Is there a legal requirement to notify individuals in the case of unauthorized disclosure of this data element?

Appendix C: Additional Resources

Privacy Impact Assessment Templates

- International Association of Privacy Professionals (IAPP), Privacy Impact Assessment Resources (members only)
- University of California, Berkeley, Privacy and Online Monitoring Balancing Process (see Appendix B)
- U.S. General Services Administration (GSA), Privacy Impact Assessments
- U.S. Department of Homeland Security (DHS), Privacy Impact Assessments

Privacy Program Maturity Models

- Minnesota Privacy Consultants, Privacy Maturity Model (hosted by IAPP)
- American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (CICA), Privacy Maturity Model
- Nymity, Privacy Management Accountability Framework
- West Virginia University has shared a template in spreadsheet format that may be modified and used by your institution.

Appendix D: Growing as a CPO in Higher Education

Being a CPO in higher education can be a challenging and rewarding career. This section serves as a guide for finding privacy professional development resources, networks, and partnership opportunities. (Also see Appendix C: Professional Resources in part 1 of the CPO Primer.)

Conferences and Networking Opportunities

For professional growth opportunities beyond your campus, there are many conferences, workshops, and webinars that focus on privacy and other areas that may be within your scope of responsibility (policy, compliance, audit, incident management, etc.).

The following list offers some suggestions for annual events and conferences that may be of interest. For more ideas, the Future of Privacy Forum maintains a global Privacy Calendar. The Berkman Klein Center for Internet & Society at Harvard University also hosts online or in-person discussions, lectures, conferences, and other gatherings on privacy throughout the year (see their Events page).

January

- FTC PrivacyCon
- Data Privacy Day events (various hosts and locations)

February

- Bloomberg Law Outlook on Privacy & Data Security

March

- BCLT Privacy Law Forum hosted by the Berkeley Center for Law & Technology

April

- IAPP Global Privacy Summit
- BCLT/BTLJ Symposium co-hosted by the Berkeley Center for Law & Technology and Berkeley Technology Law Journal
- EDUCAUSE Security Professionals Conference

May

- IEEE Symposium on Security & Privacy

June

- Higher Education Compliance Conference hosted by the Society of Corporate Compliance and Ethics
- NACUA Annual Conference

September

- Privacy. Security. Risk. Conference hosted by the IAPP Privacy Academy and CSA Congress
- URMIA Annual Conference

October

- Privacy + Security Forum (George Washington University Law School and University of California Berkeley School of Law)
- EDUCAUSE Annual Conference
- National Cyber Security Awareness Month events (various hosts and locations)

CPOs in higher education also have access to numerous local activities for professional development, depending on the campus or surrounding area. One only needs to look around:

- Audit a law, business, policy, or IT class regarding privacy, organizational behavior, or project management.
- Monitor your institution's newspaper, newsletters, Twitter feeds, and blogs for special speakers and presentations offered to the community on privacy-related topics.
- Join your local IAPP KnowledgeNet chapter and participate in their events.

Paying It Forward

Many organizations offer opportunities to contribute to the privacy body of knowledge and mentor others. Be sure to check with professional associations to see if they offer volunteer opportunities. Privacy-focused student organizations, law schools, or other departments on your campus may welcome a partnership, as well.

About EDUCAUSE

EDUCAUSE is a nonprofit association and the foremost community of IT leaders and professionals committed to advancing higher education. EDUCAUSE programs and services are focused on analysis, advocacy, community building, professional development, and knowledge creation because IT plays a transformative role in higher education. EDUCAUSE supports those who lead, manage, and use information technology through a comprehensive range of resources and activities. For more information, visit educause.edu.

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.