PRIVACY AND SECURITY IN STATE POSTSECONDARY DATA SYSTEMS:
STRONG FOUNDATIONS 2020

ERNEST EZEUGO, CARRIE KLEIN, CHRISTINA WHITFIELD

JULY 2021

TABLE OF CONTENTS

INTRODUCTION

State postsecondary data systems contain a wealth of information—including detailed records about individuals—that allow states to analyze and improve their postsecondary education systems. The entities that maintain these systems operate in a context of concern about the privacy and security of educational records. They have both an interest in making valuable information available to researchers and policy analysts and a duty to protect sensitive data. This paper outlines the use of benchmark privacy and security processes, standards, and practices in state postsecondary data systems, using results from the 2020 administration of the State Higher Education Executive Officers Association's Strong Foundations survey.[1]

It is important to consider these results through the lens of an ever-changing data privacy and security landscape. When the first Strong Foundations survey was administered in 2010, state data systems' approaches to protecting privacy were framed predominantly by compliance with the 1974 Federal Education Rights and Privacy Act (FERPA); concerns about digital hygiene and cybersecurity were nascent in higher education and in the United States more broadly. In 2010, Facebook was six years old, Twitter was four, and neither had suffered a major, public data breach yet; we were just beginning our journey toward global interconnectedness and shared some collective naïveté about the implications for our data and privacy.

That began to change in 2013 when Facebook, via Cambridge Analytica, disclosed details of a bug that exposed the personal data of six million accounts, followed by high profile data breaches at businesses like Target and Sony—and at institutions like Penn State.[2] Public concern about the safety of their data in the hands of companies and institutions grew quickly, leading to a realignment of values concerning how data was protected and managed.[3] This had a significant effect on education policy and legislation: A report from the Data Quality Campaign revealed that in 2014 alone, 36 states introduced over 110 bills concerning education data privacy, including many that sought to set new standards for how state education agencies managed their data systems.[4]

Today, states' reckoning with evolving data systems, standards, legislation, and governance—and the precipitating events that inform evolving approaches to keeping data private and secure—continues apace. Incidents like the Facebook/Cambridge Analytica scandal and the recent hack of Colonial Pipeline[5] have made clear that how organizations and their members use, store, and manage data is as essential to privacy and security efforts as technological infrastructure.[6]

---

1. Since 2010, the State Higher Education Executive Officers Association (SHEEO) has periodically administered the Strong Foundations survey, which documents the content, structure, and effective use of state postsecondary student unit record systems. This paper highlights selected responses to the fifth administration of the survey. Information on previous iterations of the survey and previously published reports are available at https://postsecondarydata.sheeo.org

2. Straumsheim, C. (2015, July 6). A playground for hackers. *Inside Higher Ed*. https://www.insidehighered.com/news/2015/07/06/pennsylvania-state-u-cyberattacks-possibly-part-larger-trend-experts-say

3. Fazzini, K. (2019, December 23). In a decade of cybersecurity alarms, these are the breaches that actually mattered. *CNBC*. https://www.cnbc.com/2019/12/23/stuxnet-target-equifax-worst-breaches-of-2010s.html

4. Anderson, R. (2019). *The emergence of data privacy conversations and state responses*. Data Quality Campaign. https://vtechworks.lib.vt.edu/bitstream/handle/10919/92664/DataPrivacyLouisiana.pdf?sequence=1&isAllowed=y

5. Sanger, D.E., & Perlroth, N. (2021, May 14). Pipeline attack yields urgent lessons about U.S. cybersecurity. *New York Times*. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

6. See Lapowsky, I. (2019, March 17). How Cambridge Analytica sparked the great privacy awakening. *Wired*. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening

State legislatures have introduced laws governing how personally identifiable information[7] and other sensitive data are managed and shared. Perhaps as a result of these shifts, respondents' answers to the *Strong Foundations 2020* survey reflect a desire to stay ahead of the curve regarding privacy and security. Survey responses indicate more state agencies are incorporating more external guidelines, more personnel, and stricter protocols for handling data into their data governance strategies.

METHODOLOGY

Strong Foundations 2018 included, for the first time, detailed questions regarding states' approaches to ensuring privacy and security for their postsecondary data systems. These questions were repeated in *Strong Foundations 2020*. To reduce the burden on survey participants, responses for all 2018 survey items were pre-populated in the 2020 survey instrument, and returning respondents were asked to indicate whether any changes had occurred to affect their previous responses. New respondents received the full 2018 battery of privacy and security questions.[8] As was the case in 2018, and given states' interest in protecting the details of their privacy and security efforts, this report will not identify specific practices of individual states, except in cases where publicly available resources are referenced.

7. U.S. General Services Administration. *Rules and Policies - Protecting PII - Privacy Act*. GSA. (2018, October 8). https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act

8. For the full set of survey questions, see *Appendix A*.

PRIVACY AND SECURITY PROCESSES

We asked respondents to "briefly describe the process used to ensure privacy of unit record data in your state." In *Strong Foundations 2018*, we found that this question set the tone for the privacy and security battery. Agencies shared responses to this question that helped us understand the scale of structures and processes they manage to protect their data and the gravity with which they treat their data security responsibilities. *Strong Foundations 2020* responses were no different. Responses described robust efforts to protect data using levers from infrastructure, internal governance, and personnel. As an example, one respondent shared the following: "As an agency we take multiple steps to ensure the privacy of the information in our system. Some of these include implementing a full data governance program, implementing internal data access and management procedures, and having employees sign data confidentiality/non-disclosure agreements. Additionally, the system is tightly managed with multiple layers of access and data sharing agreements and memoranda of understanding are developed and maintained when data sharing of any kind occurs with external parties."

Three overarching themes stood out in the responses to this question: States rely on controlling who has access to the data, use legally binding agreements for data sharing, and employ robust cybersecurity infrastructures to ensure their data is private and secure.

STRONG FOUNDATIONS 2020 ASKED:

"Briefly describe the process used to ensure privacy of unit record data in your state."

ACCESS

Respondents cited the ability to control access to data 18 times, cementing it as one of their main methods of maintaining data privacy. Responses revealed that agencies put a great deal of thought into protocols for granting and removing data access rights.

- Role-Based Access: Five respondents specifically referenced role-based access in their responses, reflecting a desire to increase data privacy and decrease identifiability by limiting which groups and individuals access data according to specific roles and circumstances. One respondent said: "We set up role-level security when sharing data with institutions within the system—each institution can only access data of their own students." Another mentioned having specific "protocols for granting and removing data access rights and role level security for data in [their state postsecondary data system]."

- Limited/Restricted General Access: Thirteen respondents referenced broad efforts to limit access to their state postsecondary data systems for external use. Notably, each of these respondents referenced agreements as essential to external data sharing.

AGREEMENTS

Respondents cited binding and non-binding data sharing agreements as another common method of maintaining and promoting data privacy and security. Referenced 16 times, respondents shared that these agreements with agencies, researchers, institutions, and other stakeholders were crucial to protecting data privacy.

- Non-Disclosure Agreements: Respondents referenced non-disclosure agreements, designed to bar one or more parties from sharing confidential information, six times. One respondent shared that "[they] don't disclose deidentified data without a contract and notarized non-disclosure agreements."

- Memoranda of Understanding: Six agencies mentioned using MOUs to control access to their data systems, with one respondent remarking that the agreements promoted "data sharing with external parties while limiting access to sensitive variables (e.g., FAFSA data)."

DIGITAL SECURITY INFRASTRUCTURE AND PERSONNEL

Respondents referenced cybersecurity infrastructure and personnel support for data security 16 times. Responses indicated that privacy and security officers, training, and robust infrastructure for creating firewalls, encrypting data, and storing or transferring files play a big role in their data systems.

- Digital Infrastructure, Cybersecurity Practices: Seven respondents mentioned physical infrastructure and technology put in place to protect data as it is stored and transferred. One respondent said that "to ensure privacy of unit record data, files are encrypted inflight via a data portal and securely stored on an encrypted server at rest."

- Dedicated Personnel: Respondents referenced security and privacy officers three times. References positioned these officers as key in decision-making and approval. "The agency security coordinator reviews and audits permissions to data/directories quarterly," wrote one respondent, "[t]he security officer has policies in place/documented should a breach occur."

Of 60 returning respondents, 50 informed us that the processes used to ensure the privacy of unit record data in their state have not changed since they took *Strong Foundations 2018*. Among the 10 respondents whose answers had changed, three cited the addition of privacy and/or security personnel as a catalyst for more robust privacy and security practices. One agency told us that since the last time they completed the survey, they have hired a privacy officer who "revamped [their] information security program" and instituted an annual review of their data privacy policies. The remaining seven cited improvements to digital and physical infrastructure and changes to data governance policies around data sharing and de-identifying data. Critically, four of those seven respondents acknowledged that their changes were a response to changes in regulation. One respondent shared that "[the General Data Protection Regulation], along with other U.S. state legislation, is pushing us to elevate our requirements and guidance on privacy."

PRIVACY AND SECURITY STANDARDS

In *Strong Foundations 2018*, we sought to assess what standards states adhered to as the landscape of postsecondary data privacy and security grew more complex. For *Strong Foundations 2020*, we repeated this question to understand what changes, if any, states were making to keep their data protected.

STRONG FOUNDATIONS 2020 ASKED:

"Which standards or protocols does your agency use to determine privacy and security procedures?"

Each of the 60 respondents who answered this question in *Strong Foundations 2020* cited or alluded to the Family Educational Rights and Privacy Act (FERPA) as one of their guiding standards for protecting and securing their data systems. But while FERPA continues to be the most visible federal law governing data privacy in education, respondents referenced several other laws, regulations, and guidelines they are using to advise privacy and security efforts. *Strong Foundations 2020* saw an increase in the number of respondents who mentioned adhering to the National Institute of Standards and Technology (NIST) cybersecurity framework (22 references versus 14 in 2018) and Health Insurance Portability and Accountability Act (HIPAA) guidance materials (16 references versus 12 in 2018). More respondents also cited adding state or system guidance to their data management strategy.

TABLE 1

PROTOCOLS AGENCIES USE TO DETERMINE PRIVACY AND SECURITY PROCEDURES

STANDARD	NUMBER OF RESPONSES	PERCENT OF RESPONSES
FERPA	60	92%
NIST	22	34%
State or System	18	28%
HIPAA	16	17%
Other	10	15%
None Specified	5	8%

COMMONLY REFERENCED PRIVACY AND SECURITY STANDARDS AND THEIR RELEVANCE FOR STATE AGENCIES EXPLAINED

In *Strong Foundations 2018* and *2020*, respondents reported adhering to several privacy and security standards to comply with federal and state laws, regulations, and guidelines and to protect their data. The range and scope of these standards emphasize just how interconnected state postsecondary data systems are with other government agencies, institutions, and industries and how complicated managing these standards can be for state higher education agencies.[9]

- Sixty respondents noted compliance with the **Family Educational Rights and Privacy Act**—the foundational educational privacy law in the U.S., established to "protect the privacy of student education records."[10] **FERPA** establishes rights for eligible students (over the age of 18) to inspect, review, and correct their educational records and governs the notification, consent, and disclosure of student records by federally-funded higher education institutions and their educational partners (to include state agencies).

- Sixteen respondents mentioned the **Health Insurance Portability and Accountability Act**, commonly referred to as **HIPAA**, which is a federal law that created standards to "protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[11] HIPAA compliance is of particular concern to states and postsecondary data systems that store the medical records of institutions that provide health care and insurance to students as well as training to future health care practitioners.[12]

- Higher education data systems often collect information about students' financial circumstances. The **Gramm-Leach-Bliley Act**, cited by three *Strong Foundations 2020* respondents, requires that financial institutions "regulate the collection and disclosure of private financial information" and protect financial information by "implementing security programs."[13]

- One respondent cited the **Payment Card Industry Data Security Standard (PCI DSS)**, which requires businesses and organizations that interact with credit card data to adopt robust "security management, policies, procedures, network architecture, software design and other critical protective measures."[14] Institutions of higher education process and store credit card information for various business-related functions and have an obligation to follow PCI-DSS as a result.

---

9. For an overview of data privacy laws and regulations affecting higher education, see the University of Michigan's Information and Technology Services Safe Computing's History of Privacy Timeline at https://safecomputing.umich.edu/privacy/history-of-privacy-timeline

10. U.S. Department of Education (ED). (2020, December 15). *Family Educational Rights and Privacy Act (FERPA)*. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

11. Centers for Disease Control and Prevention. (2018, September 14). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. https://www.cdc.gov/phlp/publications/topic/hipaa.html

12. The COVID-19 pandemic raised the stakes for HIPAA compliance in higher education as institutions collected student health data to track on-campus transmissions and determine distance learning policies. With a growing number of institutions requiring COVID-19 vaccinations from students seeking to return to campus, HIPAA compliance may play an increasingly prominent role in data governance considerations.

13. Gramm-Leach-Bliley Act. Federal Trade Commission. (n.d.). https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

14. PCI DSS. (n.d.). *EDUCAUSE*. https://library.educause.edu/topics/policy-and-law/pci-dss. Also see: https://www.pcisecuritystandards.org/faqs

- The **National Institute of Standards and Technology (NIST)** provides standards and security protocols for data shared by the federal government with nonfederal entities. These guidelines, which 22 respondents cited in their answers to our question about protocols, apply to "Controlled Unclassified Information," which can include data shared for research purposes, financial aid information, and other data necessary for institutional operations, and more at the federal government's discretion.[15]

- When *Strong Foundations 2018* was released, there was little guidance regarding the impact of the **General Data Protection Regulation (GDPR)**— the landmark framework of standards regulating "collection and processing of personal information from individuals who live in the European Union"[16]—on higher education in the U.S. By 2020, the Future of Privacy Forum concluded that there is "significant guidance that can be analyzed and applied," and that the GDPR "applies to most U.S.-based higher education and EdTech companies, as these have some type of interaction with EU residents."[17]

We asked respondents: "Has this changed since your agency last completed the survey? If so, please describe the reason the change occurred." Of 60 returning respondents, 20 confirmed that the protocols and standards they used to secure their data did not change, and 33 left the field blank. Seven respondents answered affirmatively, with four referencing internal efforts to strengthen data governance, two referencing the involvement of privacy officers, and one referencing anticipation of global privacy regulations like the General Data Protection Regulation (GDPR).

15. Higher Education Information Security Council. *An introduction to NIST Special Publication 800-171 for higher education institutions.* (2016, April 18). *EDUCAUSE.* https://library.educause.edu/resources/2016/4/an-introduction-to-nist-special-publication-800-171-for-higher-education-institutions. Also see: https://www.nist.gov

16. GDPR.eu. *General Data Protection Regulation (GDPR) compliance guidelines.* (n.d.). https://gdpr.eu

17. Future of Privacy Forum (2020, December 17). *FPF releases new report on GDPR guidance for US higher education institutions.* https://fpf.org/blog/gdprhighered

PRIVACY AND SECURITY PRACTICES

For all entities that handle sensitive data, robust data management practices play a critical role in keeping information private and secure. *Strong Foundations 2018* asked state agencies about whether they had documented data protocols in place for managing data breaches and destroying data, and if they trained employees in proper data management. We also asked the frequency with which they audit their data systems. We asked respondents to address these same questions in *Strong Foundations 2020* to determine whether agencies adopted more data management practices over time. Additionally, we asked respondents who they partnered with to perform audits of their data systems.

DATA PROTOCOLS AND TRAINING

- **Data Breaches:** Of 65 total respondents, 58 said that they have documented protocols in place in the event of a data breach. Four respondents signaled that they do not have a protocol in place, and three left the field blank.

  Five respondents said they had either added data breach protocols or changed them since the last time they took the *Strong Foundations* survey (55 responded "no" or left the field blank). Of those responses, two cited state laws as the reason for the change. One agency cited the attempted data breach of a sister agency as the reason for updating their protocols. The remaining two cited changes to internal data governance structures.

- **Data Destruction:** Of 65 total respondents, 49 said that they have protocols in place for destroying data. Thirteen respondents signaled they do not have protocols in place, and three respondents left the field blank.

  Fifty-nine of 60 returning respondents said their answers to the previous question had not changed since they last filled out the survey. One affirmative response cited the implementation of data destruction best practices from another governmental agency within the state as the reason for the change in their answer.

- **Data Management Training:** Of 65 respondents, 54 said "yes." Nine respondents answered "no," and two left the field blank. This is a significant increase from 2018, when 39 of 58 respondents indicated they had training protocols in place.

TABLE 2
PRIVACY AND SECURITY PRACTICES

PRIVACY AND SECURITY PRACTICE	NUMBER OF RESPONSES		
	Yes	No	N/A
Data Breach	58	4	3
Destroying Data	49	13	3
Employee Training	54	9	2

STRONG FOUNDATIONS 2020 ASKED:

"How frequently is your data system audited?"

AUDITING

In *Strong Foundations 2018*, we asked agencies to share how frequently their data systems were audited. We repeated this question in *Strong Foundations 2020*, also asking agencies to share who is responsible for auditing their state postsecondary data systems. Responses revealed that 26 agencies (40% of respondents) had their data systems audited yearly, a significant increase from the 16 agencies (27% of respondents) who reported annual audits in 2018.

TABLE 3
FREQUENCY OF DATA SYSTEM AUDITS

FREQUENCY	NUMBER OF RESPONSES	PERCENT OF RESPONSES
Never	13	20%
Yearly	26	40%
Once Every 2 Years	4	6%
Once Every 3-5 Years	13	20%
No Answer Specified	9	14%

STRONG FOUNDATIONS 2020 ASKED:

"Who audits your student-unit record system?"

Notably, 24 agencies shared that external auditors play a significant or exclusive role in ensuring their data systems are compliant and accurate. Of those respondents indicating auditing agents, four cited state information technology teams, five cited state budget management and auditing agencies, and two mentioned state chief information officers. Another agency shared that they enlisted consulting firms such as Price Waterhouse Cooper or Deloitte to perform their audits. Eight responses shared that they exclusively perform internal audits of their state postsecondary data systems.

STATE PRIVACY AND SECURITY LEGISLATION

2018 was a bellwether year for legislative action on data privacy and security, prompting us to ask states whether recent legislation affected how they used and kept student unit record data. The trend continued in 2020; six new consumer privacy laws were passed in three states in 2020 alone, with tens more pending discussion in state legislatures across the country.[18]

STRONG FOUNDATIONS 2020 ASKED:

"Has any legislation on student or consumer privacy (proposed or enacted in the last five years) affected how you store and analyze student unit record data?"

Fifteen of 65 respondents answered "yes," while 48 respondents answered "no," and two did not provide an answer. We also asked respondents who answered affirmatively to "describe [the] legislation and how it has impacted your agency/entity." We identified a few themes in their responses:

- Legislation concerning the handling and use of personally identifiable information was referenced on five occasions—the most references in this category—with respondents citing examples of how these laws forced them to step up their de-identification efforts or otherwise limit what data they could collect. One respondent said such legislation "limited what data we could collect into the P-20W [statewide longitudinal data systems] and required all added fields to be reviewed annually by the legislature." At least two respondents shared concerns about how these new legislative rules might discourage data sharing, with one repeating a refrain we quoted in the *Strong Foundations 2018* report: "Legislation highly tilts towards data privacy versus availability" to the detriment of cross-agency collaboration.

- Two respondents alluded to the introduction of cybersecurity laws meant to encourage states to bolster their digital security infrastructure. Both respondents cited hiring trained information security officers and the laws giving their state information technology divisions more power in regulating cybersecurity efforts.

- One respondent shared that their state recently passed a law holding state agencies and employers accountable for reporting significant data breaches. The new law requires that entities must report breaches to the attorney general's office within 60 days if "250 or more [state] residents are found to have been compromised/breached."

---

18. Greenberg, P. (n.d.). *2020 consumer data privacy legislation.* National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx

RECOMMENDATIONS

The *Strong Foundations 2018* report included a recommendation that state postsecondary data systems fully adopt benchmark privacy and security practices, review their practices for compliance with emerging privacy and security standards, and consider adopting legislation that codifies privacy and security practices. While it would be inappropriate to assume causality, it is worth noting that progress has been made on these fronts. In 2020, increased numbers of respondents indicated they had protocols in place for responding to data breaches, destroying data no longer used for research, training employees handling sensitive information, and performing annual audits. In several instances, respondents noted that protocols adopted since 2018 were responses to new legislation.

Following *Strong Foundations 2020*, we encourage continued attention to privacy and security efforts by state higher education agencies. Based on the responses to this survey and on evolving standards and legislation, we recommend that agencies employ the following practices to advance a robust state postsecondary data system:

- **Create dynamic and inclusive data governance:** State postsecondary data systems do not exist in a vacuum. They are integral parts of agency operations, and the data within them are often shared within and across SHEEO agency boundaries. As such, these systems need a governance structure that is inclusive of various perspectives, organizations, and roles. Further, data governance efforts should be collaborative in order to establish robust and relevant data security and privacy provisions for the SHEEO agency and its stakeholders, including institutions, other state agencies, federal entities, educational researchers, and educational technology vendors.

  If not already established, SHEEO agencies should create data governance boards to set policy, processes, and protocols for how data are used and protected. Dynamic and inclusive boards work collaboratively with representatives from various units within the agency to create a vision for agency privacy and security efforts. Data governance boards should solicit input from stakeholders and expand participation beyond traditional data and information technology representatives to include faculty, student affairs administrators, diversity, inclusion, and equity officers, and—arguably—student representatives, since student data is central to postsecondary data systems. Incorporating diverse perspectives will create more innovative, equitable, and relevant data privacy and security standards and protocols.

  To support dynamic and inclusive data governance, SHEEO agencies should consider investing in a chief privacy officer (CPO) or data privacy officer (DPO) position. CPOs and DPOs are becoming increasingly important members of data teams within higher education institutions,[19] where they work to uphold institutional data privacy and security standards while communicating data

---

19. See Vogel, V. (2015, May 11). The chief privacy officer in higher education. *EDUCAUSE*. https://er.educause.edu/articles/2015/5/the-chief-privacy-officer-in-higher-education
Bermann, S., Blair, S., Chambers, S., et al. (2021, Feb. 1). The higher education CPO primer: Part I. *EDUCAUSE*. https://library.educause.edu/resources/2016/8/the-higher-education-cpo-primer-part-1-a-welcome-kit-for-chief-privacy-officers-in-higher-education

privacy efforts to the public. Their work promotes transparent and trustworthy use and sharing of data in postsecondary systems, via governance, policy development, and training programs. At the University of Michigan, for example, the Information and Technology Services Safe Computing's privacy team, led by a CPO, helps shape data privacy policies, create compliance standards, communicate privacy efforts to the community, educate campus members on how to protect data, convene community members for privacy-related events, and cultivate a culture of data privacy and security.[20] SHEEO agency CPOs or DPOs can also be important conveners and promoters for data privacy and security by sharing data privacy and security best practices, ensuring compliance across systems, and coordinating with CPOs and DPOs from other state agencies and institutions.

- **Establish or update agency data security and privacy policies and practices:** Transparency related to data privacy and security policies and practices is essential to bolstering strong postsecondary data systems and encouraging trust in using the data within those systems. The creation and publication of data privacy and security policies informs good practice, fosters transparency, and communicates SHEEO agency standards to stakeholders. Data privacy and security policies should provide information for how SHEEO agencies define and protect data during its lifecycle in a system—especially data containing personally identifiable information (PII)—and how data are stored, shared, retained, and destroyed.

  Strong SHEEO agency privacy and security policies should also reference and comply with relevant standards (including laws, regulations, and guidelines) and articulate the associated rights (including review, correction, or redress) of individuals whose data resides in state postsecondary systems. Benchmark policies will encourage the adoption of similar standards by institutions within the state and by third-party partners, like researchers or vendors. Further, policies should acknowledge the importance of using data ethically and equitably to advance SHEEO agency, institutional, and student outcomes.

  The University of Hawai'i System[21] provides a good example of a data security policy that defines various data types and how those data should be protected across its system by constituent institutions. A strong data privacy policy can be found at the University System of Georgia,[22] which explains to visitors why and how data is collected and used (both on their website and in their postsecondary data system) and the various rights individuals have within the agency's data collection program. SHEEO agencies can work to stay abreast of advances in data security and privacy policies and practices through organizations like NIST[23]

---

20. University of Michigan Information and Technology Services. (n.d.). *Privacy at U-M.* https://safecomputing.umich.edu/privacy/privacy-u-m

21. University of Hawai'i. (n.d.). *UH systemwide policies and procedures information system (PPIS): Executive policy 2.214, Institutional data classification categories and information security guidelines.* http://www.hawaii.edu/policy/?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=214

22. University System of Georgia. (n.d.). *Data privacy policy and legal notice.* https://www.usg.edu/siteinfo/web_privacy_policy

23. National Institute for Standards and Technology (NIST). (n.d.) *Cybersecurity framework.* https://www.nist.gov/cyberframework/framework

and the International Association of Privacy Professionals (IAPP).[24]

- **Require data security and privacy training:** Given the evolving nature of data use and the associated risk of that use, SHEEO agencies should require data privacy and security training for all SHEEO agency data and research staff and should encourage training for all other staff. Training is another mechanism for supporting appropriate data protections within postsecondary data systems by building users' knowledge of and appreciation for data privacy and security. With training comes increased literacy in the ways data can be leveraged, misused, or compromised within a postsecondary data system and the associated skills to minimize risk and improve outcomes. By training staff at all levels, SHEEO agencies build a corps of data privacy and security champions.

  There is no one standard for data privacy and security training; trainings should be tailored to individual SHEEO agencies and the roles within those agencies. However, the federal Department of Education does provide guidance and best practices related to data security and privacy.[25] SHEEO agencies should also encourage institutions within their state to provide data privacy and security training for any administrator, faculty, or staff member who works with institutional or student data.

24. International Association of Privacy Professionals (IAPP). (n.d.). *Homepage.* https://iapp.org
25. U.S. Department of Education. (n.d.). *Protecting student privacy.* https://studentprivacy.ed.gov

CONCLUSION

State postsecondary data systems are vital information resources for policymakers and researchers and contain large amounts of potentially sensitive information about students, faculty, and staff. The agencies that operate these systems take privacy and security considerations seriously, and our research indicates that the prevalence of benchmark privacy and security practices is increasing. By continuing to adapt to emerging privacy and security standards, states can use state postsecondary data systems to develop policy solutions and promote student success, while protecting personal information housed within them.

APPENDIX A: LIST OF QUESTIONS

RETURNING RESPONDENTS

Q0
Please enter your contact information.

- Name
- Email
- Agency
- Phone number

CHARACTERISTICS OF STUDENT UNIT RECORD SYSTEMS (SURS)

Q1
How many student unit record systems (SURS) does your agency manage?

- ☐ One
- ☐ Two
- ☐ Three
- ☐ More than three

Q2
Please indicate the name of your postsecondary student unit record system (SURS) for which you will be responding to the rest of this survey. If there are multiple, please select the SURS which you use to conduct the majority of your reporting and analysis of student-level data.

Note: The historical response could have had several SURS listed. Please ensure only **one** is listed here for this year's survey.

Q2A
Please briefly describe the function of the other SURS that your agency manages.

Q3

Please verify the types of postsecondary institutions from which your agency/entity currently collects student unit record data. *(Select all that apply.)*

- ☐ N/A
- ☐ 2-year public
- ☐ 4-year public
- ☐ Tribal
- ☐ Independent (private, nonprofit)
- ☐ Proprietary (private, for-profit)
- ☐ Other institution type, please specify

Q4

Please confirm or update which elements your agency collects or can access by institutional sector. **If your agency / entity does not have access to an element, please check "No access to this element."**

	2-year public	4-year public	Private nonprofit	Private for-profit	No access to this element
Student name	☐	☐	☐	☐	☐
Date of birth	☐	☐	☐	☐	☐
Gender	☐	☐	☐	☐	☐
Race / Ethnicity	☐	☐	☐	☐	☐
Age	☐	☐	☐	☐	☐
Military status	☐	☐	☐	☐	☐
Social Security number	☐	☐	☐	☐	☐
K-12 unique identifier	☐	☐	☐	☐	☐
Institution of higher education identifier	☐	☐	☐	☐	☐
Postsecondary student unique identifier	☐	☐	☐	☐	☐
Citizenship status	☐	☐	☐	☐	☐
State residency status	☐	☐	☐	☐	☐
Admissions scores	☐	☐	☐	☐	☐
Placement scores	☐	☐	☐	☐	☐
Prior college(s) attended	☐	☐	☐	☐	☐
Transfer credit(s)	☐	☐	☐	☐	☐
Retention by term or year	☐	☐	☐	☐	☐

	2-year public	4-year public	Private nonprofit	Private for-profit	No access to this element
Enrollment status (first-time, transfer, continuing)	☐	☐	☐	☐	☐
Degree-seeking status	☐	☐	☐	☐	☐
Full-time / Part-time status	☐	☐	☐	☐	☐
Term student first enrolled (fall, spring, summer)	☐	☐	☐	☐	☐
Program / Major	☐	☐	☐	☐	☐
Dependency status	☐	☐	☐	☐	☐
Family income	☐	☐	☐	☐	☐
Federal financial aid	☐	☐	☐	☐	☐
State financial aid	☐	☐	☐	☐	☐
Institutional financial aid	☐	☐	☐	☐	☐
Merit-based financial aid	☐	☐	☐	☐	☐
Need-based financial aid	☐	☐	☐	☐	☐
Other financial aid	☐	☐	☐	☐	☐
FAFSA fields	☐	☐	☐	☐	☐
Pell status	☐	☐	☐	☐	☐
Cost of postsecondary education (what student actually pays)	☐	☐	☐	☐	☐
Course mode of instruction	☐	☐	☐	☐	☐
Course grade	☐	☐	☐	☐	☐
Student credit hours attempted	☐	☐	☐	☐	☐
Student credit hours earned	☐	☐	☐	☐	☐
Academic term	☐	☐	☐	☐	☐
Degree awarded	☐	☐	☐	☐	☐
Degree date	☐	☐	☐	☐	☐
Cumulative credit hours earned	☐	☐	☐	☐	☐
Cumulative GPA	☐	☐	☐	☐	☐
Student tuition and fees	☐	☐	☐	☐	☐

Q5

Please confirm or update which metrics you are able to calculate based on data elements your agency collects or has access to.

- [ ] Credit accumulation
- [ ] Credit completion ratio (credits completed vs. attempted)
- [ ] Remedial course completion
- [ ] Gateway course completion
- [ ] Retention / persistence rate
- [ ] Transfer rate
- [ ] Graduation rate
- [ ] Completion ratio (completions per FTE)
- [ ] Net price
- [ ] Cumulative debt
- [ ] Loan repayment status
- [ ] Employment status
- [ ] Median wage of completers
- [ ] Median wage of non-completers
- [ ] Time to credential
- [ ] Credits to credential
- [ ] Other, please specify

LINKAGES AND ENHANCEMENTS TO SURS

Q6

Does your agency / entity currently link or plan to link with the following agencies, either through a warehouse or a federated model? *(Select all that apply.)*

	Currently link?	Plan to link?
Pre-K / Early childhood	[ ]	[ ]
State education agency (K-12)	[ ]	[ ]
State financial aid agency / entity	[ ]	[ ]
Labor / Workforce	[ ]	[ ]
Child protective services	[ ]	[ ]
Foster care	[ ]	[ ]
Health	[ ]	[ ]
Human services	[ ]	[ ]
Motor vehicle division / dept	[ ]	[ ]

	Currently link?	Plan to link?
Juvenile detention	☐	☐
Corrections	☐	☐
Court system	☐	☐
Other agency, please specify	☐	☐
Other agency, please specify	☐	☐

Q7

Which K-12 data elements does your agency / entity have access to and/or utilize through linking arrangements? *(Select all that apply.)*

	Have access?	Utilize?
Student name	☐	☐
Student date of birth	☐	☐
Student gender	☐	☐
Student race / ethnicity	☐	☐
Student resident county / district code	☐	☐
Dates of K-12 enrollment	☐	☐
Language spoken at home	☐	☐
Student free and reduced lunch eligibility	☐	☐
District / school code	☐	☐
Disability status	☐	☐
Course title	☐	☐
Course grade	☐	☐
Course type (regular, honors, AP, IB, dual credit)	☐	☐
High school grade point average	☐	☐
Assessment scores	☐	☐
Date student graduated (K-12)	☐	☐
Family income	☐	☐
Other K-12 data elements, please specify	☐	☐
Other K-12 data elements, please specify	☐	☐
Other K-12 data elements, please specify	☐	☐

Q8

Which labor/workforce data elements does your agency / entity have access to by virtue of linking arrangements? *(Select all that apply.)*

	Have access?	Utilize?
Employer name	☐	☐
Employer address	☐	☐
Employer ID number	☐	☐
Employer size; number of monthly employees	☐	☐
Employer county	☐	☐
North American Industry Classification System (NAICS) code	☐	☐
NAICS title	☐	☐
Wages earned	☐	☐
Hours worked	☐	☐
Employment quarter code	☐	☐
Employment year	☐	☐
Date student / employee applied for unemployment insurance	☐	☐
Date student / employee received first unemployment insurance check	☐	☐
Total weeks of unemployment insurance claims	☐	☐
Other agencies / entities providing services during period individual is in receipt of unemployment insurance	☐	☐
Standard Occupational Classification (SOC) code	☐	☐
SOC title	☐	☐
Other labor / workforce data element, please specify	☐	☐
Other labor / workforce data element, please specify	☐	☐
Other labor / workforce data element, please specify	☐	☐

Q9

If applicable, please describe how your agency / entity modified its SURS to allow linking to other data systems (e.g., adding new data fields, creating new file structures, etc.)

Q10

Which of the following barriers prevent or inhibit your agency / entity from linking to any unit record systems? *(Select all that apply.)*

- ☐ N/A
- ☐ Legislation
- ☐ Lack of fiscal resources
- ☐ Lack of time for agency staff to link/analyze data
- ☐ Lack of common identifiers/crosswalks
- ☐ Coordination with other state authorities/administrators
- ☐ Incompatible systems
- ☐ Information technology infrastructure
- ☐ Data quality concerns
- ☐ FERPA concerns
- ☐ Lack of interest from other agencies
- ☐ Other barrier, please specify

Q10A

What potential uses of your SURS could not occur due to lack of fiscal resources?

Q10B

Please describe any strategies your agency has adopted in an attempt to increase your ability to analyze SURS data.

Q10C

Does your agency employ a matching algorithm or formula to combine data sets with different unique identifiers?

- ☐ Yes
- ☐ No

Q10C1

Please describe in brief how the matching algorithm or formula operates.

Q10C2

If you are able to determine the successful match rate, please share it.

Q10D

Please describe any strategies your agency has adopted to increase coordination with other state authorities / administrators.

Q10E

What kinds of analysis are difficult or impossible to achieve for your SURS due to incompatible systems? *(Please explain.)*

Q10F

Please describe what concerns you have about the quality of data in your system.

Q11

Does your agency / entity link or share data with other states?

- ☐ Yes
- ☐ No

Q11A

What data is shared or linked with other states? How is it used?

USES OF STUDENT UNIT RECORD DATA

Q12

How has your SURS provided the greatest value to your state?

Q12A

Has this changed since your agency last completed this survey? If so, please describe.

Q13

In what ways does your SURS reduce burden for your constituent institutions?
(Select all that apply.)

- ☐ Producing data analysis or reports
- ☐ Fulfilling IPEDS reporting requirements
- ☐ Fulfilling state reporting requirements
- ☐ Determining student financial aid awards
- ☐ Producing feedback reports for institutions
- ☐ Producing accountability reports for institutions

- [ ] Analyzing transfer pathways for students between institutions
- [ ] Linking institutional student data to other data sets on their behalf
- [ ] Other, please specify

Q14

In what ways does your SURS reduce burden for your agency? *(Select all that apply.)*

- [ ] Complying with intermediary data requests (e.g., ATD, CCA, Strong Start to Finish, etc.)
- [ ] Fulfilling legislative reporting requirements
- [ ] Responding to federal, gubernatorial, or legislative ad-hoc data requests
- [ ] Improving data quality
- [ ] Producing public-facing dashboards
- [ ] Producing other consumer tools
- [ ] Other, please specify

Q15

Please provide examples of how data from your SURS has been used to inform policy decisions.

Q15A

Are there any new examples since your agency last completed this survey? If so, please describe.

Q16

Please provide examples of how connections between your SURS and other agencies have been used to inform policy decisions, if applicable.

Q17

What is the largest barrier to effective use of SURS data for your agency / entity?

Q17A

Has this changed since your agency last completed this survey? If so, please describe.

Q18

Do you have partnerships / data sharing agreements in place to share SURS data with external researchers?

- [ ] Yes
- [ ] Planning to
- [ ] No

Q18A

What does your agency see as the greatest value of research partnerships?

Q18B

What is the largest barrier to fulfilling student-level data research requests?

Q19

Approximately how many research proposals requesting student-level data does your agency **receive** per year?

Q20

What kinds of research questions are being asked of your SURS, if applicable?

Q21

Approximately how many research proposals requesting student-level data does your agency **approve** per year?

ENSURING DATA PRIVACY AND SECURITY

Please note: Responses in this section will not be reported or made available at the state level. Data will be analyzed in the aggregate and individual responses will be anonymized.

Q22

Please briefly describe the process used to ensure privacy of unit record data in your state.

Q22A

Has this changed since your agency last completed this survey? If so, please describe the change and the reason the change occurred.

Q23

Which standards or protocols does your agency use to determine privacy and security procedures (FERPA, HIPAA, NIST, etc.)?

Q23A

Has this changed since your agency last completed the survey? If so, please describe the change and the reason the change occurred?

Q24

Does your agency have a documented protocol for what to do in the event of a data breach?

- ☐ Yes
- ☐ No

Q25

Has this changed since your agency last completed this survey? If so, please describe the change and the reason the change occurred.

Q26

Does your agency have a documented protocol for destroying data?

- ☐ Yes
- ☐ No

Q27

Has this changed since your agency last completed this survey? If so, please describe.

Q28

How frequently is your data system audited?

- ☐ Yearly
- ☐ Once every 2 years
- ☐ Once every 3-5 years
- ☐ Once every 6+ years
- ☐ Never

Q28A

Who audits your SURS?

Q29

Do employees in your agency receive formal training for ensuring privacy, security, and confidentiality of student-level data?

- ☐ Yes
- ☐ No

Q30

Has any legislation on student or consumer privacy (proposed or enacted in the last five years) affected how you store and analyze student unit record data?

- ☐ Yes
- ☐ No

Q30A

Please describe this legislation and how it impacted your agency / entity.

FUTURE PLANS FOR THE SURS

Q31

Are there new uses of your student unit record system that are planned in the next two years? If so, please describe.

Q32

What policy issues exist for your agency that you anticipate your SURS will inform?

Q33

What, if any, are your procedures and plans for ensuring the sustainability (e.g., financial sustainability, operation sustainability, legislative sustainability) of your SURS?

Q33A

Has this changed since your agency last completed this survey? If so, please describe.

Q34

Is there a planned upgrade or migration to a new or improved SURS?

- ☐ Yes
- ☐ No

Q34A

When do you anticipate this system upgrade to be completed?

NEW RESPONDENTS

Q0

Please enter your contact information.

- Name
- Email
- Agency
- Phone number

CHARACTERISTICS OF STUDENT UNIT RECORD SYSTEMS (SURS)

Q1

How many student unit record systems (SURS) does your agency manage?

- ☐ One
- ☐ Two
- ☐ Three
- ☐ More than three

Q2

Please indicate the name of your postsecondary student unit record system (SURS) for which you will be responding to the rest of this survey. If there are multiple, please select the SURS which you use to conduct the majority of your reporting and analysis of student-level data.

Note: The historical response could have had several SURS listed. Please ensure only **one** is listed here for this year's survey.

Q2A

Please briefly describe the function of the other SURS that your agency manages.

Q3

What was the year this SURS was established?

Q4

Why was this SURS originally established? *(Select all that apply.)*

- ☐ Legislative mandate
- ☐ Audit compliance
- ☐ Institutional resource allocation / funding formula

- ☐ Awarding financial aid
- ☐ IPEDS reporting
- ☐ Increasing student achievement
- ☐ Tracking student retention/graduation
- ☐ Tracking students across institutions
- ☐ Federal civil rights mandates
- ☐ Other federal mandates
- ☐ Other reason, please specify

Q5

What legal authority assigns data collection and reporting responsibilities to your agency?
(Select all that apply.)

- ☐ N/A - Data collection occurs on a voluntary basis
- ☐ State law creating coordinating or governing board
- ☐ State law creating data system
- ☐ State law requiring the collection of student unit record data
- ☐ Administrative regulations/rules issued to interpret state law(s)
- ☐ Coordinating or governing board policy interpreting state law(s)
- ☐ Coordinating or governing board policy interpreting executive branch mandate
- ☐ Memorandum of understanding
- ☐ Attorney general opinion / statement
- ☐ Other legal authority, please specify

Q6

Please verify the types of postsecondary institutions from which your agency / entity currently collects student unit record data. *(Select all that apply.)*

- ☐ N/A
- ☐ 2-year public
- ☐ 4-year public
- ☐ Tribal
- ☐ Independent (private, nonprofit)
- ☐ Proprietary (private, for-profit)
- ☐ Other institution type, please specify

Q7

Please indicate which elements your agency collects or can access by institutional sector.
If your agency / entity does not have access to an element, please check "No access to this element."

	2-year public	4-year public	Private nonprofit	Private for-profit	No access to this element
Student name	☐	☐	☐	☐	☐
Date of birth	☐	☐	☐	☐	☐
Gender	☐	☐	☐	☐	☐
Race / Ethnicity	☐	☐	☐	☐	☐
Age	☐	☐	☐	☐	☐
Military status	☐	☐	☐	☐	☐
Social Security number	☐	☐	☐	☐	☐
K-12 unique identifier	☐	☐	☐	☐	☐
Institution of higher education identifier	☐	☐	☐	☐	☐
Postsecondary student unique identifier	☐	☐	☐	☐	☐
Citizenship status	☐	☐	☐	☐	☐
State residency status	☐	☐	☐	☐	☐
Admissions scores	☐	☐	☐	☐	☐
Placement scores	☐	☐	☐	☐	☐
Prior college(s) attended	☐	☐	☐	☐	☐
Transfer credit(s)	☐	☐	☐	☐	☐
Retention by term or year	☐	☐	☐	☐	☐
Enrollment status (first-time, transfer, continuing)	☐	☐	☐	☐	☐
Degree-seeking status	☐	☐	☐	☐	☐
Full-time / Part-time status	☐	☐	☐	☐	☐
Term student first enrolled (fall, spring, summer)	☐	☐	☐	☐	☐
Program / Major	☐	☐	☐	☐	☐

	2-year public	4-year public	Private nonprofit	Private for-profit	No access to this element
Dependency status	☐	☐	☐	☐	☐
Family income	☐	☐	☐	☐	☐
Federal financial aid	☐	☐	☐	☐	☐
State financial aid	☐	☐	☐	☐	☐
Institutional financial aid	☐	☐	☐	☐	☐
Merit-based financial aid	☐	☐	☐	☐	☐
Need-based financial aid	☐	☐	☐	☐	☐
Other financial aid	☐	☐	☐	☐	☐
FAFSA fields	☐	☐	☐	☐	☐
Pell status	☐	☐	☐	☐	☐
Cost of postsecondary education (what student actually pays)	☐	☐	☐	☐	☐
Course mode of instruction	☐	☐	☐	☐	☐
Course grade	☐	☐	☐	☐	☐
Student credit hours attempted	☐	☐	☐	☐	☐
Student credit hours earned	☐	☐	☐	☐	☐
Academic term	☐	☐	☐	☐	☐
Degree awarded	☐	☐	☐	☐	☐
Degree date	☐	☐	☐	☐	☐
Cumulative credit hours earned	☐	☐	☐	☐	☐
Cumulative GPA	☐	☐	☐	☐	☐
Student tuition and fees	☐	☐	☐	☐	☐

Q8

Does your agency have the authority to add or delete data elements and change definitions for any of the data elements above?

- ☐ Yes, full authority
- ☐ Yes, but only in conjunction with other stakeholders
- ☐ No

Q9

Which of the following sources does your agency use to define data elements?
(Select all that apply.)

- ☐ IPEDS
- ☐ U.S. Census
- ☐ Agency staff / workgroup
- ☐ Common Education Data Standards (CEDS)
- ☐ Other, please specify

Q10

Please indicate which metrics you are able to calculate based on data elements your agency collects or has access to.

- ☐ Credit accumulation
- ☐ Credit completion ratio (credits completed vs. attempted)
- ☐ Remedial course completion
- ☐ Gateway course completion
- ☐ Retention / persistence rate
- ☐ Transfer rate
- ☐ Graduation rate
- ☐ Completion ratio (completions per FTE)
- ☐ Net price
- ☐ Cumulative debt
- ☐ Loan repayment status
- ☐ Employment status
- ☐ Median wage of completers
- ☐ Median wage of non-completers
- ☐ Time to credential
- ☐ Credits to credential
- ☐ Other, please specify

LINKAGES AND ENHANCEMENTS TO SURS

Q11

Does your agency / entity currently link or plan to link with the following agencies, either through a warehouse or a federated model? *(Select all that apply.)*

	Currently link?	Plan to link?
Pre-K / Early childhood	☐	☐
State education agency (K-12)	☐	☐
State financial aid agency / entity	☐	☐
Labor / Workforce	☐	☐
Child protective services	☐	☐
Foster care	☐	☐
Health	☐	☐
Human services	☐	☐
Motor vehicle division / dept	☐	☐
Juvenile detention	☐	☐
Corrections	☐	☐
Court system	☐	☐
Other agency, please specify	☐	☐
Other agency, please specify	☐	☐

Q12

Which primary ID number(s) are used to match your agency's SURS data to unit record data from other agencies within your state? *Select all that apply. Be sure to fill out all 5 columns, if applicable.*

	Social Security Number	K-12 ID	Postsecondary ID	Longitudinal data system ID	Other ID
Pre-K / Early childhood	☐	☐	☐	☐	☐
State education agency (K-12)	☐	☐	☐	☐	☐
State financial aid agency	☐	☐	☐	☐	☐
Labor / Workforce	☐	☐	☐	☐	☐
Child protective services	☐	☐	☐	☐	☐
Foster care	☐	☐	☐	☐	☐
Health	☐	☐	☐	☐	☐
Human services	☐	☐	☐	☐	☐

	Social Security Number	K-12 ID	Postsecondary ID	Longitudinal data system ID	Other ID
Motor vehicle division / dept	☐	☐	☐	☐	☐
Juvenile detention	☐	☐	☐	☐	☐
Corrections	☐	☐	☐	☐	☐
Court system	☐	☐	☐	☐	☐
Other agency, please specify	☐	☐	☐	☐	☐
Other agency, please specify	☐	☐	☐	☐	☐

Q13

Which K-12 data elements does your agency / entity have access to and / or utilize through linking arrangements? *(Select all that apply.)*

	Have access?	Utilize?
Student name	☐	☐
Student date of birth	☐	☐
Student gender	☐	☐
Student race / ethnicity	☐	☐
Student resident county / district code	☐	☐
Dates of K-12 enrollment	☐	☐
Language spoken at home	☐	☐
Student free and reduced lunch eligibility	☐	☐
District / school code	☐	☐
Disability status	☐	☐
Course title	☐	☐
Course grade	☐	☐
Course type (regular, honors, AP, IB, dual credit)	☐	☐
High school grade point average	☐	☐
Assessment scores	☐	☐
Date student graduated (K-12)	☐	☐
Family income	☐	☐
Other K-12 data elements, please specify	☐	☐
Other K-12 data elements, please specify	☐	☐

	Have access?	Utilize?
Other K-12 data elements, please specify	☐	☐

Q14

Which labor / workforce data elements does your agency / entity have access to by virtue of linking arrangements? *(Select all that apply.)*

	Have access?	Utilize?
Employer name	☐	☐
Employer address	☐	☐
Employer ID number	☐	☐
Employer size; number of monthly employees	☐	☐
Employer county	☐	☐
North American Industry Classification System (NAICS) code	☐	☐
NAICS title	☐	☐
Wages earned	☐	☐
Hours worked	☐	☐
Employment quarter code	☐	☐
Employment year	☐	☐
Date student / employee applied for unemployment insurance	☐	☐
Date student / employee received first unemployment insurance check	☐	☐
Total weeks of unemployment insurance claims	☐	☐
Other agencies / entities providing services during period individual is in receipt of unemployment insurance	☐	☐
Standard Occupational Classification (SOC) code	☐	☐
SOC title	☐	☐
Other labor / workforce data element, please specify	☐	☐
Other labor / workforce data element, please specify	☐	☐
Other labor / workforce data element, please specify	☐	☐

Q15

If applicable, please describe how your agency / entity modified its SURS to allow linking to other data systems (e.g., adding new data fields, creating new file structures, etc.)

Q16

Which of the following currently allow your agency to link or share with other unit record systems? *(Select all that apply.)*

- ☐ Legislative mandate
- ☐ Executive mandate
- ☐ Memorandum of understanding / agreement
- ☐ Administrative rule / regulation
- ☐ Other, please specify

Q17

Which of the following barriers prevent or inhibit your agency / entity from linking to any unit record systems? *(Select all that apply.)*

- ☐ N/A
- ☐ Legislation
- ☐ Lack of fiscal resources
- ☐ Lack of time for agency staff to link / analyze data
- ☐ Lack of common identifiers / crosswalks
- ☐ Coordination with other state authorities / administrators
- ☐ Incompatible systems
- ☐ Information technology infrastructure
- ☐ Data quality concerns
- ☐ FERPA concerns
- ☐ Lack of interest from other agencies
- ☐ Other barrier, please specify

Q17A

What potential uses of your SURS could not occur due to lack of fiscal resources?

Q17B

Please describe any strategies your agency has adopted in an attempt to increase your ability to analyze SURS data.

Q17C

Does your agency employ a matching algorithm or formula to combine data sets with different unique identifiers?

- ☐ Yes
- ☐ No

Q17C1

Please describe in brief how the matching algorithm or formula operates.

Q17C2

If you are able to determine the successful match rate, please share it.

Q17D

Please describe any strategies your agency has adopted to increase coordination with other state authorities / administrators.

Q17E

What kinds of analysis are difficult or impossible to achieve for your SURS due to incompatible systems? *(Please explain.)*

Q17F

Please describe what concerns you have about the quality of data in your system.

Q18

Does your agency / entity link or share data with other states?

- ☐ Yes
- ☐ No

Q18A

What data is shared or linked with other states? How is it used?

USES OF STUDENT UNIT RECORD DATA

Q19

How has your SURS provided the greatest value to your state?

Q20

For what purposes does your agency currently use SURS data? *(Select all that apply.)*

- ☐ Decision making
- ☐ Policy making
- ☐ Generating reports and statistics (internal and external)
- ☐ Consumer information for prospective students
- ☐ Research
- ☐ Cross-sector collaboration (e.g., K-12 & labor)
- ☐ External reporting (e.g., IPEDS, Complete College America, Achieving the Dream, SREB, etc.)
- ☐ Other purpose, please specify

Q21

Does your agency use SURS data for analysis by the following categories? *(Select all that apply.)*

- ☐ Articulation
- ☐ Community college feedback
- ☐ Completions
- ☐ Course cost analysis
- ☐ Course-taking patterns
- ☐ Demographics (e.g., age, gender, race / ethnicity)
- ☐ Distance education
- ☐ Dual credit / Dual enrollment
- ☐ Economic impact / Jobs
- ☐ Facilities utilization
- ☐ Financial aid
- ☐ High school feedback
- ☐ Institutional finance
- ☐ Institutional profile, public
- ☐ Institutional profile, private
- ☐ Mobility / migration
- ☐ Non-credit instructional activity

- ☐ Performance measures
- ☐ Remediation
- ☐ Retention
- ☐ Student learning
- ☐ Teacher effectiveness evaluations
- ☐ Transfer
- ☐ Tuition / Fees / College costs
- ☐ Other, please specify

Q22

In what ways does your SURS reduce burden for your constituent institutions?
(Select all that apply.)

- ☐ Producing data analysis or reports
- ☐ Fulfilling IPEDS reporting requirements
- ☐ Fulfilling state reporting requirements
- ☐ Determining student financial aid awards
- ☐ Producing feedback reports for institutions
- ☐ Producing accountability reports for institutions
- ☐ Analyzing transfer pathways for students between institutions
- ☐ Linking institutional student data to other data sets on their behalf
- ☐ Other, please specify

Q23

In what ways does your SURS reduce burden for your agency? *(Select all that apply.)*

- ☐ Complying with intermediary data requests (e.g., ATD, CCA, Strong Start to Finish, etc.)
- ☐ Fulfilling legislative reporting requirements
- ☐ Responding to federal, gubernatorial, or legislative ad-hoc data requests
- ☐ Improving data quality
- ☐ Producing public-facing dashboards
- ☐ Producing other consumer tools
- ☐ Other, please specify

Q24

Are there mandates in your state for measuring workforce outcomes? If so, please describe the mandate.

Q25
Are data from your SURS used to fulfill the workforce outcomes mandate? If so, please describe.

Q26
Please provide examples of how data from your SURS has been used to inform policy decisions.

Q27
Please provide examples of how connections between your SURS and other agencies have been used to inform policy decisions, if applicable.

Q28
What is the largest barrier to effective use of SURS data for your agency / entity?

Q29
Do you have partnerships / data sharing agreements in place to share SURS data with external researchers?

- ☐ Yes
- ☐ Planning to
- ☐ No

Q29A
What does your agency see as the greatest value of research partnerships?

Q29B
What is the largest barrier to fulfilling student-level data research requests?

Q30
Approximately how many research proposals requesting student-level data does your agency **receive** per year?

Q31
What kinds of research questions are being asked of your SURS, if applicable?

Q31
Approximately how many research proposals requesting student-level data does your agency **approve** per year?

ENSURING DATA PRIVACY AND SECURITY

Please note: Responses in this section will not be reported or made available at the state level. Data will be analyzed in the aggregate and individual responses will be anonymized.

Q33

Please briefly describe the process used to ensure privacy of unit record data in your state.

Q34

Which standards or protocols does your agency use to determine privacy and security procedures (FERPA, HIPAA, NIST, etc.)?

Q35

Does your agency have a documented protocol for what to do in the event of a data breach?

- ☐ Yes
- ☐ No

Q36

Does your agency have a documented protocol for destroying data?

- ☐ Yes
- ☐ No

Q37

How frequently is your data system audited?

- ☐ Yearly
- ☐ Once every 2 years
- ☐ Once every 3-5 years
- ☐ Once every 6+ years
- ☐ Never

Q37A

Who audits your SURS?

Q38

Do employees in your agency receive formal training for ensuring privacy, security, and confidentiality of student-level data?

- ☐ Yes
- ☐ No

Q39

Has any legislation on student or consumer privacy (proposed or enacted in the last five years) affected how you store and analyze student unit record data?

☐ Yes

☐ No

Q39A

Please describe this legislation and how it impacted your agency / entity.

FUTURE PLANS FOR THE SURS

Q40

Are there new uses of your student unit record system that are planned in the next two years? If so, please describe.

Q41

What policy issues exist for your agency that you anticipate your SURS will inform?

Q42

What, if any, are your procedures and plans for ensuring the sustainability (e.g., financial sustainability, operation sustainability, legislative sustainability) of your SURS?

Q43

Is there a planned upgrade or migration to a new or improved SURS?

☐ Yes

☐ No

Q44

When do you anticipate this system upgrade to be completed?

APPENDIX B: LIST OF SURVEY RESPONDENTS

ALABAMA

Subrena Simpkins
Director of Research Services
Alabama Commission on Higher Education
subrena.simpkins@ache.edu

ALASKA

Gwen Gruenig
Associate Vice President
University of Alaska
gdgruenig@alaska.edu

ARKANSAS

Sonia Hazelwood
Associate Director
Arkansas Department of Higher Education
sonia.hazelwood@adhe.edu

CALIFORNIA

Edward Sullivan
Assistant Vice Chancellor for Academic
Research and Resources
The California State University
esullivan@calstate.edu

Chris Furgiuele
Director
University of California
chris.furgiuele@ucop.edu

Ryan Fuller
Research Specialist
California Community Colleges
Chancellor's Office
rfuller@cccco.edu

COLORADO

Michael Vente
Senior Director of Research
and Data Governance
Colorado Department of Higher Education
michael.vente@dhe.state.co.us

CONNECTICUT

Bill Gammell
Associate Vice President of Research
& System Effectiveness
Connecticut State Colleges and Universities
wgammell@commnet.edu

FLORIDA

Hayley Spencer
Director of Research and Analytics
Florida Department of Education
hayley.spencer@fldoe.org

Jason Jones
Chief Data Officer
Florida Board of Governors
jason.jones@flbog.edu

GEORGIA

Angela Bell
Vice Chancellor of Research
and Policy Analysis
University System of Georgia
angela.bell@usg.edu

Pascael Beaudette
Executive Director of Research
and Business Intelligence
Technical College System of Georgia
pbeaudette@tcsg.edu

HAWAI'I

Pearl Iboshi
Director, Institutional Research
& Analysis Office
University of Hawai'i
iboshi@hawaii.edu

IDAHO

Andy Mehl
SLDS Project Coordinator
Idaho State Board of Education
andy.mehl@osbe.idaho.gov

ILLINOIS

Eric Lichtenberger
Deputy Director for Information
Management and Research
Illinois Board of Higher Education
lichtenberger@ibhe.org

INDIANA

Sean Tierney
Associate Commissioner for Policy
and Research
Indiana Commission for Higher Education
stierney@che.in.gov

IOWA

Jason Pontius
Associate Chief Academic Officer
Board of Regents, State of Iowa
jason.pontius@iowaregents.edu

Vladimir Basis
Lead Education Program Consultant
Iowa Department of Education
vladimir.bassis@iowa.gov

KANSAS

Cynthia J. Farrier
Director, Data, Research & Planning
Kansas Board of Regents
cfarrier@ksbor.org

KENTUCKY

David Marshall Mahan
Associate Vice President, Data,
Research and Advanced Analytics
Kentucky Council on
Postsecondary Education
david.mahan@ky.gov

LOUISIANA

Kimberly Kirkpatrick
Associate Commissioner for
Institutional Research and Performance
Assessment Services
Louisiana Board of Regents
kim.kirkpatrick@regents.la.gov

MAINE

Rosa Redonnett
Chief Student Affairs Officer
University of Maine System
rosar@maine.edu

MARYLAND

Barbara Schmertz
Director
Maryland Higher Education Commission
barbara.schmertz@maryland.gov

MASSACHUSETTS

Mario Delci
Assistant Commissioner of Evaluation
and Policy Analysis
Massachusetts Department
of Higher Education
mdelci@dhe.mass.edu

MICHIGAN

Mike McGroarty
Director, Office of Analytics and Reporting
Michigan Center for Educational
Performance and Information
mcgroartym@michigan.gov

MINNESOTA

Meredith Fergus
Research and SLEDS Manager
Minnesota Office of Higher Education
meredith.fergus@state.mn.us

Nancy Floyd
Senior System Director for Research
Minnesota State Colleges and Universities
nancy.floyd@minnstate.edu

MISSISSIPPI

Jim Hood
Assistant Commissioner
for Strategic Research
Mississippi Institutions of Higher Learning
jhood@mississippi.edu

MISSOURI

Jeremy Kintzel
Director, Data and Research Services
Missouri Department of Higher Education
and Workforce Development
jeremy.kintzel@dhewd.mo.gov

MONTANA

John Thunstrom
MUS Information Technology Director
Montana University System
jthunstrom@mso.umt.edu

NEBRASKA

Mike Baumgartner
Executive Director
Nebraska's Coordinating Commission
for Postsecondary Education
mike.baumgartner@nebraska.gov

NEVADA

José Martinez
Director of Institutional Research
Nevada System of Higher Education
jmartinez@nshe.nevada.edu

NEW HAMPSHIRE

Jan Fiderio
Program Specialist for Research and Studies
New Hampshire Department of Education
janet.fiderio@doe.nh.gov

Charles Ansell
Chief Operating Officer
Community College System
of New Hampshire
cansell@ccsnh.edu

NEW JERSEY

Chad May
Director of Research and Analysis
New Jersey Office of the Secretary
of Higher Education
chad.may@oshe.nj.gov

NEW MEXICO

Dina Advani
Director of Planning and Research
New Mexico Higher Education Department
dina.advani@state.nm.us

NEW YORK

Teresa Foster
Associate Provost for Institutional
Research and Data Analytics
The State University of New York
teresa.foster@suny.edu

Leigh Mountain-Ross
Associate in Education Research
New York State Education Department
leigh.mountain@nysed.gov

Zun Tang
Director of Institutional Research
The City University of New York
zun.tang@cuny.edu

NORTH CAROLINA

Diane Marian
Vice President for Data & Analytics
The University of North Carolina
System Office
demarian@northcarolina.edu

NORTH DAKOTA

Jennifer Weber
Director of Institutional Research
North Dakota University System
jennifer.weber@ndus.edu

OHIO

Jill Dannemiller
Chief Data Officer
Ohio Department of Higher Education
jdannemiller@highered.ohio.gov

OKLAHOMA

Matt Eastwood
Assistant Vice Chancellor for Workforce
and Economic Development
Oklahoma State Regents for Higher
Education
meastwood@osrhe.edu

OREGON

Amy Cox
Director of Research and Data
Oregon Higher Education Coordinating
Commission
amy.cox@state.or.us

PENNSYLVANIA

Patricia Landis
Division Chief, Higher Education
Pennsylvania Department of Education
plandis@pa.gov

Kate Akers
Assistant Vice Chancellor for Advanced
Data Analytics
Pennsylvania State System of Higher
Education
kakers@passhe.edu

RHODE ISLAND

Andrea Spargo
Research Specialist
Rhode Island Office of the
Postsecondary Commissioner
andrea.spargo@riopc.edu

SOUTH CAROLINA

Monica Goodwin
Director
South Carolina Commission
on Higher Education
mgoodwin@che.sc.gov

Rosline Sumpter
Interim Vice President, Academics,
Student Affairs & Research
South Carolina Technical College System
sumpterr@sctechsystem.edu

SOUTH DAKOTA
Wendy Caveny
Director of Institutional Research
South Dakota Board of Regents
wendy.caveny@sdbor.edu

TENNESSEE
Chris Tingle
Assistant Vice Chancellor for Data Strategy
Tennessee Board of Regents
chris.tingle@tbr.edu

Amanda Klafehn
Assistant Director of Planning and Research
Tennessee Higher Education Commission
amanda.klafehn@tn.gov

TEXAS
Victor Reyna
Interim Director, Educational Data Center
Texas Higher Education Coordinating Board
victor.reyna@thecb.state.tx.us

UTAH
Carrie Mayne
Chief Economist
Utah System of Higher Education
cmayne@ushe.edu

VERMONT
Alexander Yin
Executive Director of Institutional Research
The University of Vermont
alexander.yin@uvm.edu

Juan Zhang
Institutional Research Analyst
Vermont State Colleges
juan.zhang@vsc.edu

VIRGINIA
Tod Massa
Director, Policy Research and
Data Warehousing
State Council of Higher Education
for Virginia
todmassa@schev.edu

Catherine Finnegan
Assistant Vice Chancellor for Research
and Reporting
Virginia Community College System
cfinnegan@vccs.edu

WASHINGTON
Darby Kaikkonen
Director of Policy Research
Washington State Board for
Community & Technical Colleges
dkaikkonen@sbctc.edu

Jim Schmidt
Manager of Education Research
& Data Center
Washington Office of Financial Management
jim.schmidt@ofm.wa.gov

Isaac Kwakye
Director of Research
Washington Student Advisory Council
isaack@wsac.wa.gov

WEST VIRGINIA

Christopher Treadway
Senior Director of Research and Policy
West Virginia Higher Education
Policy Commission
chris.treadway@wvhepc.edu

WISCONSIN

Dennis Rhodes
Senior Analyst
University of Wisconsin System
drhodes@uwsa.edu

WYOMING

Nicole Anderson
Social Service Analyst
Wyoming Community College Commission
nicole.anderson1@wyo.gov

Sue Koller
Associate Director, Institutional Analysis
University of Wyoming
ssavor@uwyo.edu