FPF POSTSECONDARY STUDENT DATA PRIVACY ISSUE BRIEF

Student Affairs and Student Success Professionals' Knowledge, Beliefs, and Skills Related to College Student Data Privacy

APRIL 2022

KRISTEN A. RENN, PHD • MICHIGAN STATE UNIVERSITY

FUTURE OF PRIVACY FORUM

EXECUTIVE SUMMARY

Student affairs and student success (SASS) professionals in postsecondary education use online platforms and administrative data to support student engagement, learning, persistence, and achievement. They typically learn about student data privacy in the context of the Family Educational Rights and Privacy Act (FERPA) and sometimes the Health Insurance Portability and Accountability Act (HIPAA) policies on campus, but rarely beyond these foundations. This level of education, along with some campus cultures that misinterpret FERPA, may result in knowledge, beliefs, and practices that could lead to overly cautious or overly liberal use of student data.

To help privacy and education stakeholders understand and address these risks, a survey of 342 SASS professionals at nine large public research universities revealed the following results:

- Nearly all consider academic records, demographics, and health-related information to be student data, but fewer respondents understand that data from learning contexts (e.g., course management systems) and student life (e.g., ID card swipes for housing) is also student data.
- SASS professionals widely believe that FERPA, HIPAA, or both protect most student data, but less consensus exists regarding student life data.
- Little consensus exists about whether institutions collect and store data in homegrown platforms, vendor platforms, or both.
- SASS professionals trust the quality of academic and demographic data and algorithms used for student success interventions.
- Participants indicate that student behavioral health data (getting a COVID-19 test) and health records (the test results) can be treated differently from FERPA and HIPAA prescribe.
- SASS professionals and their supervisors largely agree on which skills they need regarding use of student data, but differ on where they learn these skills.

The following recommendations can help SASS professionals and institutional leaders improve student data privacy policy and practice:

- SASS professionals should learn which kinds of student data exist on campus, where data are collected and stored, and how campus professionals and vendors can use the data to improve student success. Professionals should understand privacy policies and guidelines governing data use in units and on campus. They can assess their data use skills and talk with supervisors about where they can develop these skills.
- Supervisors should assess supervisees' knowledge of the forms and locations of student data on campus, including on homegrown and vendor platforms. Supervisors should also know where supervisees learn about FERPA, HIPAA, and data usage skills. Supervisors should offer education and training, in addition to institution-wide offerings, on FERPA and HIPAA, and should consider training within units as needed to supplement institutional training and self-education.
- Senior institutional leaders should establish campus-wide conversations about student data and data privacy that go beyond FERPA and HIPAA training requirements, and communicate with SASS units about the different types of student data on campus. They should also ensure that training for employees who work with student data addresses the complexity of the current data environment and provides the skills to work with it. Finally, leaders should develop and share campus-wide guidelines for accessing and working with student data within and across units, regardless of the data's location.

Context and Background

The postsecondary education sector is home to many professionals who work directly with student data. Typically located in areas that fall under the umbrella of student affairs or student success (SASS), these professionals use student data long understood to be protected by the Family Educational Rights and Privacy Act (FERPA). They may also access and use data that did not exist when FERPA was enacted in 1974, for example the "grey data"[1] of digital records of student engagement in online course platforms or ID card swipes into campus housing or dining facilities. SASS professionals may also interact with digital platforms that use algorithms to predict students' academic success or psychosocial adjustment. Together with the prevalence of predictive analytics in academic advising and learning analytics in online academic spaces, the accumulation of non-academic card swipe records means that SASS professionals are immersed in student data. For this reason, understanding how SASS professionals think about student data has never been more important. To begin to meet this need, this brief reports the results of a multi-campus survey of SASS professionals' knowledge, beliefs, and skills related to student data privacy and makes recommendations for training, supervision, and policy regarding student data privacy.

Evolution of Data Use in Student Affairs and Student Success Services

The field of student affairs emerged in the twentieth century to meet the developmental, personal, and social needs of college students. Student affairs divisions vary across institutions but often include career services, student organization advising, campus housing and dining, recreational sports, conflict resolution and student conduct, and counseling. In the twenty-first century, student affairs divisions have joined the emerging field of student success services, which may include academic advising and coaching, peer mentoring, summer bridge or cohort programs, tutoring, and adjacent areas such as financial aid and enrollment management.[2] The purpose of all these units is to promote student learning, development, and success (measured most often as persistence and graduation rates).

Historically, student affairs divisions had access to student records generated through their own systems, such as analog and then digital housing assignment or student conduct data. Similarly, academic advisers used paper records until campuses developed homegrown record-keeping systems or purchased vended platforms; these digital platforms typically integrate with campus student information systems to provide access to real-time student academic records. Regardless of the format, the student records held in student affairs units and those held in advising and other student success areas have historically been siloed, just as higher education institutions contain silos of academic affairs, faculty, student affairs, and student success services.[3]

Two macro-level influences have come together to pressure the siloed nature of postsecondary institutions: the movement to improve student outcomes and the evolution of Big Data. In the early 2000s, when four-year institutions averaged a 57 percent six-year graduation rate,[4] state and federal governments and influential foundations (e.g., Lumina, Bill & Melinda Gates) joined the public to call for accountability from institutions in the form of improved completion rates. Dubbed the Completion Agenda, this movement resulted in state funding formulas that included graduation rates and an infusion of funding (federal and private) to study innovations that could lead to improvements. At the same time, computing power multiplied, enabling the collection, aggregation, and analysis of large amounts of data on an institutional or system level. These

forces combined and yielded a substantial for-profit industry of educational technologies purporting to solve the completion problem. Some institutions developed in-house (often called "homegrown") analytics systems to accomplish similar goals.[5]

SASS professionals at large institutions that have adopted multiple homegrown or vended platforms for data access, management, and/or analytics find themselves in workplaces radically different from when professionals kept student records in paper file folders and jotted meeting notes on sticky notes. SASS professionals at all types and sizes of institution need to access and use data through digital platforms, whether vended or homegrown,[6] and a single professional may have to interact with multiple platforms to accomplish their work.[7] Student data privacy, which previously was a matter handled within a work unit according to unit-level interpretations of FERPA, is now a matter that crosses SASS units and information technology departments. The interdependence of data owners and users who may not share an understanding of privacy standards and practices amplifies the risk of compromising student data privacy.

The aggregation and availability of large amounts of student data, including the kinds of historical trend data necessary for predictive analytics, invites questions about the duty to use available data in ways previously not considered or not possible. In 2014, EDUCAUSE documented the growing movement to integrate planning and advising services (IPAS) and noted that most institutions used systems to conduct degree audits/track academic progress and manage advising centers. But three-quarters of institutions surveyed also used or planned to use systems for other student success services, including credit transfer, academic early alerts, advising management, and education plan tracking.[8]

Common commercial products such as EAB's student success management system *Navigate*[9] and recently acquired student success platform *Starfish*[10] use large amounts of historical student data in algorithms that guide proactive academic advising. Learning management system (LMS) vendors include predictive analytics products to mine student course data.[11] Homegrown efforts such as Arizona State University's *eAdvisor*[12] employ similar approaches to analytics to give SASS professionals more information to guide their practice.

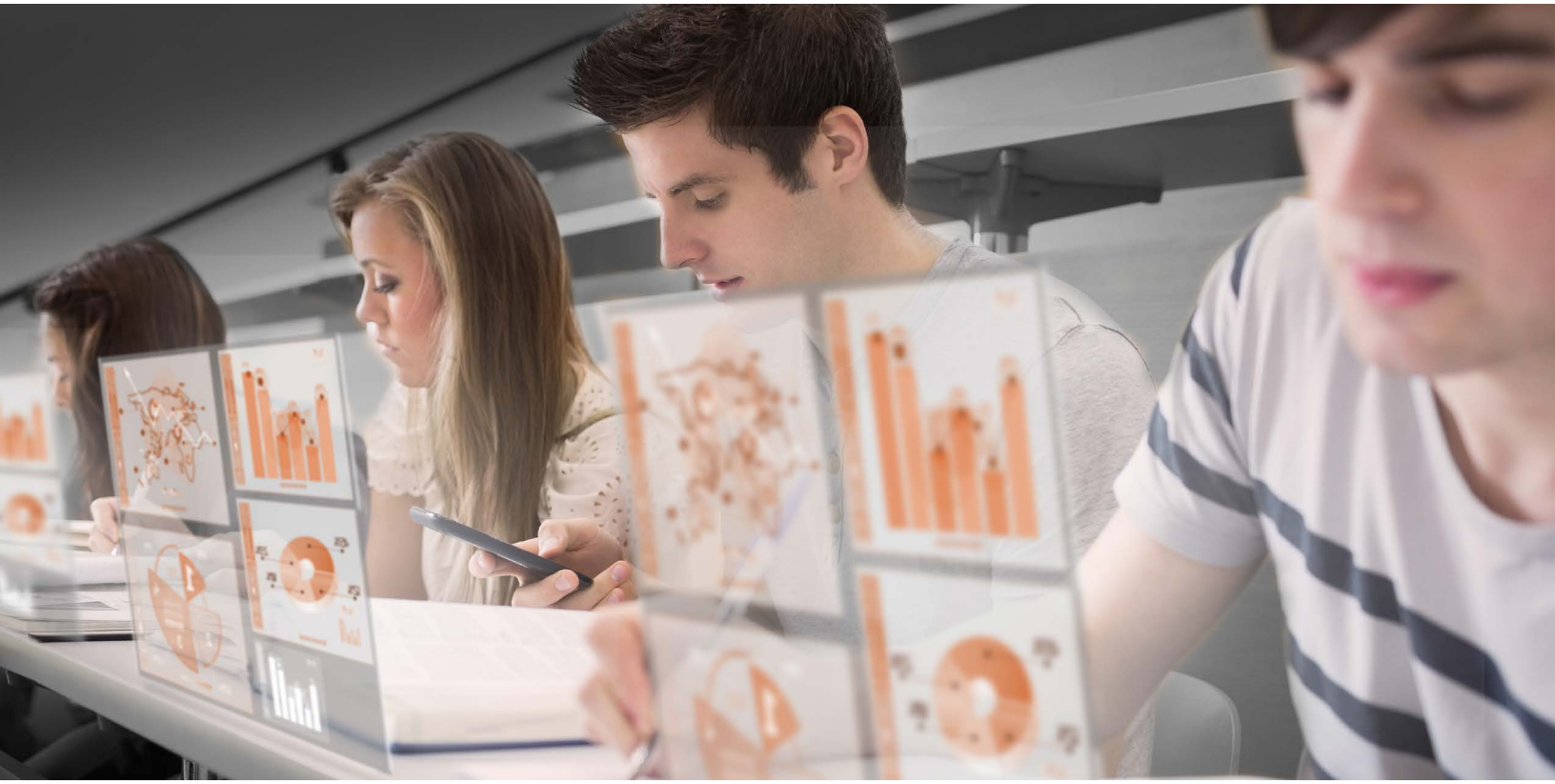
Academic advising is not the only area, as institutions' homegrown efforts also use student engagement data from instructors to create early alerts,[13] skim learning management systems for student data (e.g., University of Michigan's *Student Explorer*),[14] or look for campus dining patterns that might identify students who are isolated[15] or have patterns of residence hall entry[16] associated with persistence. Chatbots and other AI platforms aggregate information in ways that might help identify students in need of outreach about financial aid, mental health, or campus involvement.[17] Many of these approaches have mixed results in practice, but SASS professionals must nevertheless make decisions about how to use this data to improve student learning, development, well-being, and persistence.

How SASS Professionals Learn About and Enact Student Data Privacy

Given their access to and dependence on student data, SASS professionals are critical actors in the higher education student data privacy landscape. Despite research reporting college students' apparent lack of concern about how their institutions use their data,[18] SASS professionals and other campus actors have historically been careful to maintain the confidentiality and privacy of individually identifiable student data. Indeed, most SASS professionals believe that their campuses respect student privacy rights; Parnell and colleagues found that 94 percent of a sample of student affairs, institutional research, and information technology professionals agreed or strongly agreed that "In conducting student success studies, privacy rights are respected."[19]

FERPA plays a substantial role in how SASS professionals think about student data privacy. Campus culture shapes and is shaped by interpretations of FERPA, so there is variation across and within campuses about what constitutes a student record and who else on campus has, per FERPA, a "legitimate educational interest"[20] that rises to the level of sharing data.[21] Couture and colleagues found that some campus units operated under "FERPA fear," with strict interpretations and "fear of reprimands, sanctions, and lawsuits" for violations; other units operated under a "FERPA flex" stance in which "campus staff freely share information with those on campus who have a legitimate educational interest."[22]

Whether working in a hyper-regulated (FERPA fear) or open (FERPA flex) atmosphere, SASS professionals need to understand their local roles in accessing, using, and sometimes sharing student data. How they reach this understanding is not necessarily systematic. Parnell and colleagues found that 62 percent of institutions addressed training needs for staff on using student data,[23] and another study of student affairs professionals and predictive analytics recommended that institutions improve and maintain training for staff who use student data.[24] Without adequate training, some professionals invoke a "When in doubt, don't give it out" maxim,[25] which may limit their effectiveness and stifle campus innovation. Knowing how and when to use data appropriately is essential to contemporary SASS work.



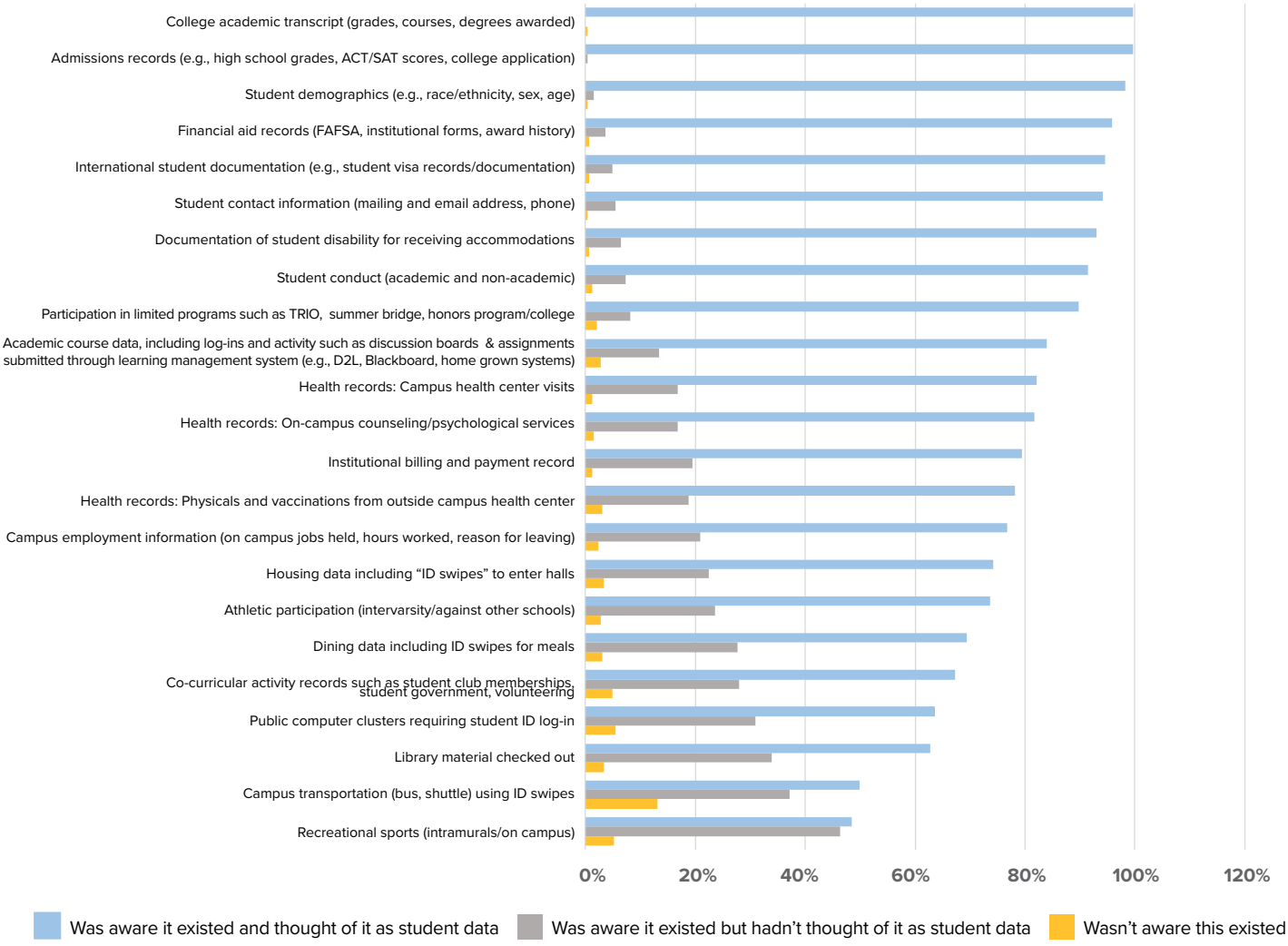
Survey of SASS Professionals

In May 2021, a survey of SASS professionals' knowledge, beliefs, and skills related to student data was distributed through the University Innovation Alliance, an organization of large public universities working to improve outcomes for low-income, first-generation, and racially minoritized students.[26] Nine campuses participated by distributing the survey to networks of SASS professionals. Three hundred and forty-two respondents completed the survey, and this brief reports their responses.

Knowledge of student data, its collection, and storage

Overall, most professionals were aware of the categories commonly considered "student data." Asked to choose from among "wasn't aware this existed," "was aware this existed but hadn't thought of it as student data," or "was aware it existed and thought of it as student data," respondents demonstrated high awareness of most data that would be part of student records, and more modest awareness of grey data such as dining or recreational sports swipes. Over 90 percent of respondents identified college transcript data (99.7 percent), admissions records (99.7 percent), demographic data (98.2 percent), financial aid records (95.8 percent), international student status (94.5 percent), contact information (94.2 percent), documentation of disability status (93.0 percent), and conduct records (91.5 percent) as student data. Over one-quarter of respondents either were not aware or were aware but had not thought of numerous categories as student data: housing data, including swipes into residence halls (25.8 percent not aware); intervarsity athletic participation (26.4 percent); dining data, including swipes to enter meals (30.6 percent); co-curricular activity records (32.7 percent); use of public computer clusters requiring student sign-ins (36.4 percent); library materials checked out (37.3 percent); campus transportation swipes (50.1 percent); and recreational sports participation (51.5 percent). Yet, all of these types of data may exist on campus. See Figure 1 for a full breakdown of responses.

Figure 1. Percentage of respondents indicating awareness of categories of student data



There was more variation in SASS professionals' understanding of where data was collected and stored on campus for each category of student data: homegrown platforms, vended solutions, or a combination of the two. The purpose of the survey was not to determine where campuses actually keep their data but to gauge SASS professionals' knowledge of these storage locations. Of the nine UIA campuses that included responses, five campuses had more than 25 respondents each, providing a reasonable basis for understanding the level of variation on a given campus. Do SASS professionals on a single campus share understanding of where student data resides? The five campuses with 25+ respondents reflect substantial variation in professionals' beliefs about data collection and storage locations.

For each category of student data named in the first question, respondents were asked whether they knew the location of data management on their campus: collected and stored in a homegrown platform, a vendor platform, or mixed (both homegrown and vendor). Fifty-five percent or higher indicated agreement within a campus regarding the location of data storage; for example, 6.2 percent of respondents on a single campus indicated that a homegrown platform kept academic course data, 60 percent indicated a vendor platform, and 33.8 percent indicated mixed homegrown and vendor platforms. The 60 percent consensus on vendor platform represents a reasonable level of shared knowledge. On this basis, the five campuses ranged from no agreement (no data categories that achieved 55 percent or higher on respondents' belief about where data is kept) to agreement ranging from 57.3 percent to 72.2 percent on 12 of the 23 data categories. These results indicate no substantial agreement on 93 of 115 categories across the five campuses. Regardless of where the institutions actually collect and store data, these findings indicate lack of shared knowledge. See Table 1 for a summary of responses for the five campuses.

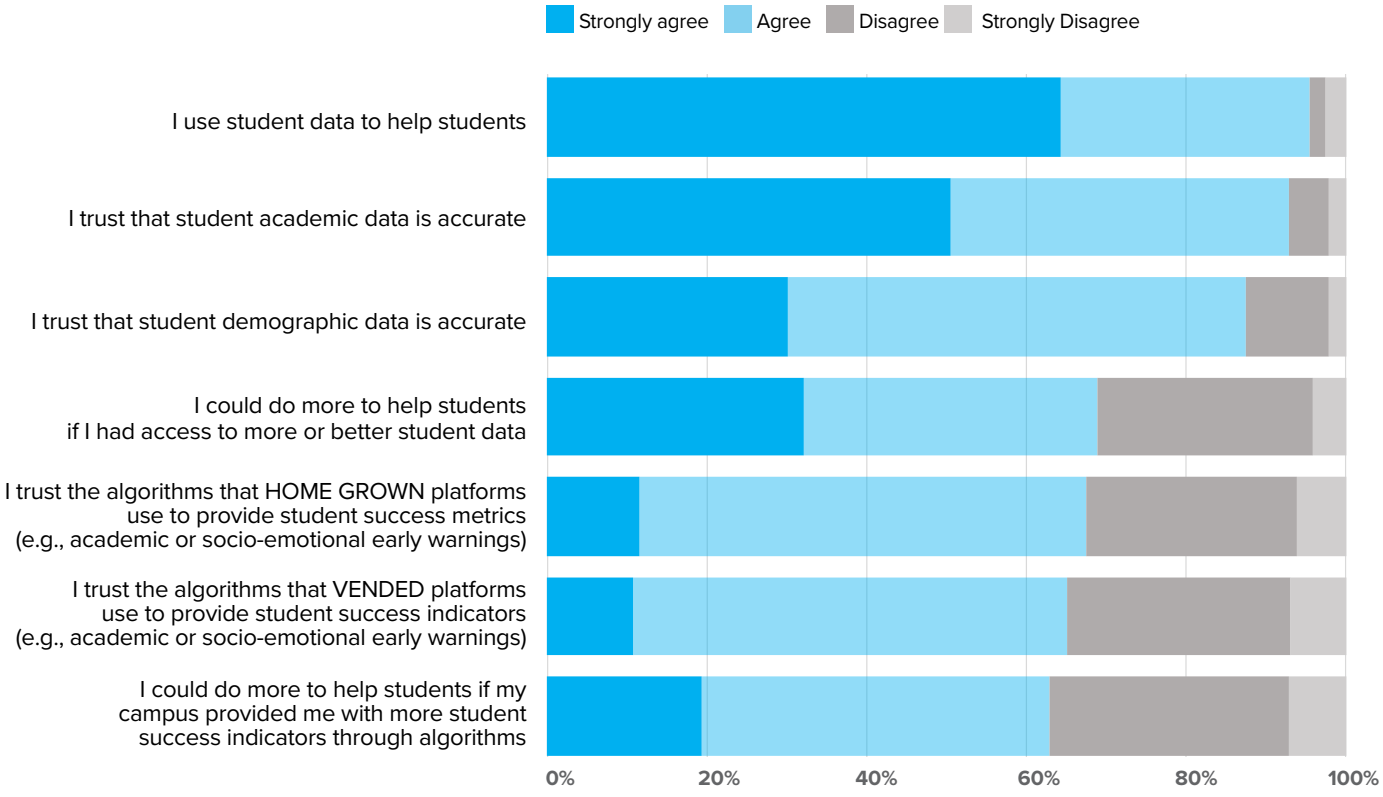
Table 1. Categories about which 55 percent or more of campus respondents agreed on where data is collected and stored (H = homegrown, V = vendor, M = mixed)

CAMPUS A	CAMPUS B	CAMPUS C	CAMPUS D	CAMPUS E
Transcript 55.3% H Course data 58.3% V Rec sports 55.6% H Health ctr visits 55.3% V Counseling 56.4% V Campus job 55.6% V	(none)	Athletics 56.3% M	Admissions 65.0% V Financial aid 58.3% V Counseling 55.6% H	Admissions 64.8% V Financial aid 61.8% V Transcript 60.6% V Demographics 60.3% V Contact into 57.3% V Billing/payment 72.2% V Course data 60.0% V Outside health 63.6% V Health ctr visits 64.9% V Counseling 58.3% V Conduct 52% V Intl status 60.4% V

Beliefs about data and working with data

Regardless of the data collection and storage locations, more than 95 percent of SASS professionals agreed or strongly agreed that they use data to help students. They also largely trust the accuracy of academic and demographic data (92.9 percent and 87.5 percent strongly agree or agree, respectively). Two-thirds reported that they could do more to help students if they had access to more or better data. On the question of algorithms to provide student success metrics (e.g., academic or socioemotional early warnings), whether on homegrown or vendor platforms, SASS professionals reported a fairly high degree of trust (67.4 percent and 65.1 percent, respectively). Nearly the same percentage (62.8 percent) believed they could do more to help students if they had more student success indicators provided through algorithms. Figure 2 summarizes responses to these items.

Figure 2. Percentage of respondents agreeing with statements on data use and reliability

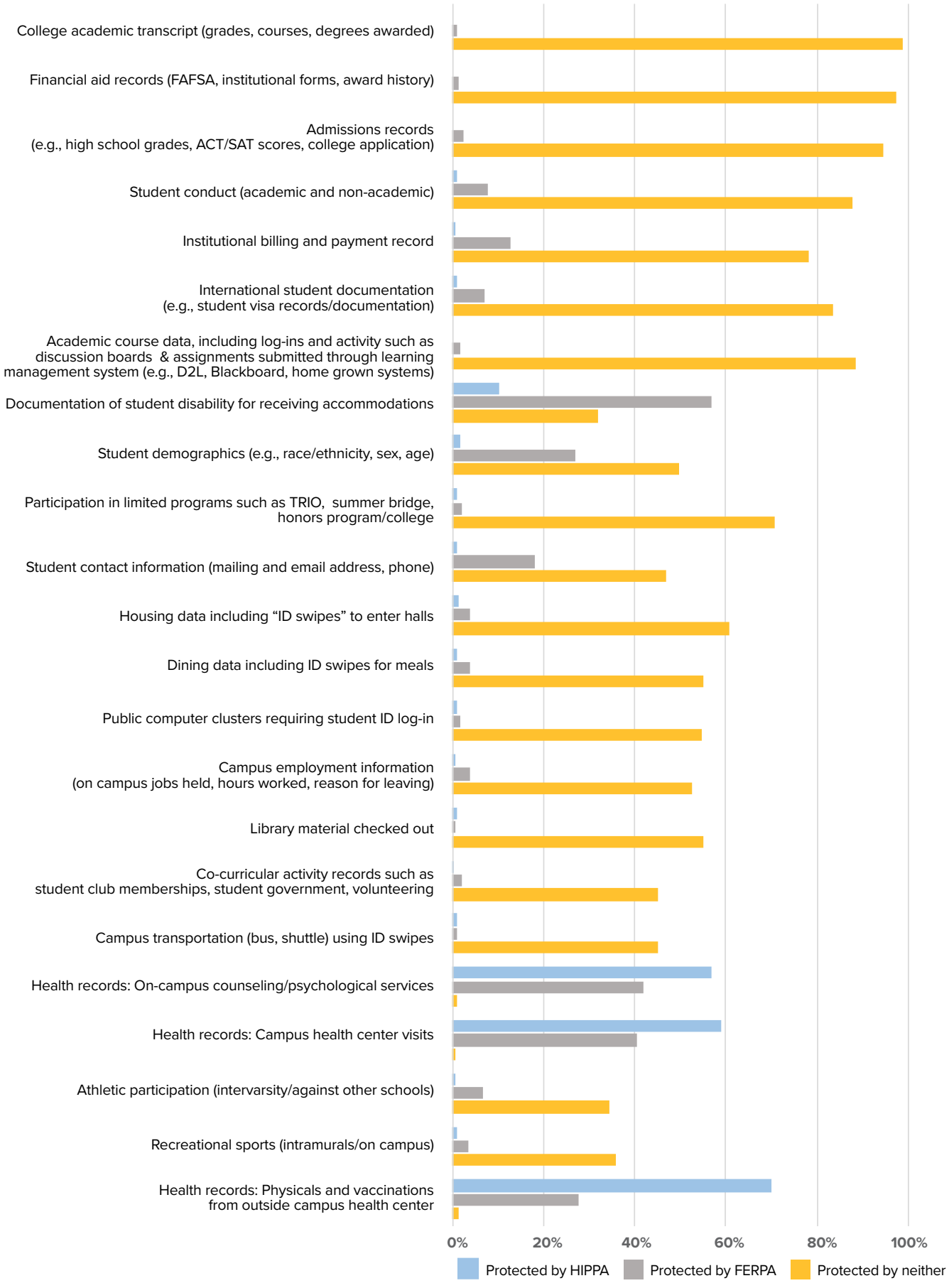


Beliefs about data privacy

Given the ubiquity of data and SASS professionals' heavy reliance on data in their work helping students, these professionals' beliefs about data privacy are of key interest. SASS professionals view several categories of student data with which they work as subject to FERPA or HIPAA policies. The professionals most often considered academic categories (e.g., transcripts, admissions), financial (financial aid, billing), and student conduct data to be under FERPA's purview, and 65 to 90.7 percent of respondents also considered the law to govern other student status data (e.g., international, disability, demographics, limited participation academic programs such as TRIO, honors college, etc.). One in ten respondents believed that FERPA did not cover academic course data submitted through an LMS. Categories related to student life (housing, dining, rec sports, campus transportation, campus employment, library and computer usage, and co-curricular activities) fell in the middle range of 45.9 to 65 percent. Approximately one-half of respondents believed that neither FERPA nor HIPAA applied to this data. About 40 percent of respondents included campus student health data under FERPA regulation, and nearly all identified off-campus and on-campus health and counseling records as under HIPAA protection. For each data category, at least some respondents indicated that one or both laws applied; only 50 percent of respondents indicated that neither HIPAA nor FERPA protected intervarsity athletics, recreational sports participation, campus transportation, and co-curricular activity participation data. See Figure 3 for a summary.

Given the widespread belief that either FERPA, HIPAA, or both laws cover most student data categories, it is important to understand where SASS professionals learn about these policies. We asked, in a "check all that apply" format, where respondents had learned about FERPA, and most indicated general training from their institutions (86.4 percent) as the source, followed by training in their specific work units (40.1 percent), courses or training during a degree program (26.5 percent), and on their own (21.2 percent). Of those who learned on their own, one in five had no other source of FERPA education/training. Asked the same question about HIPAA, respondents indicated less formal training: 44.8 percent responded that they received general training from their institution, 43.4 percent learned on their own (by reading professional publications and media, attending conferences, and other non-campus-based professional development), 15.3 percent learned in courses or a degree program, 14.7 percent were trained in their specific work units, and 8.8 percent had never learned about HIPAA. Although every SASS professional may not need to know HIPAA regulations, the lack of systematic training could be a concern given the percentage of respondents who indicated that HIPAA covered different non-health categories of student data.

Figure 3. Percentage of respondents indicating that FERPA, HIPAA, or neither law protects specific data categories



Beliefs about data usage

Using the same 55 percent standard for substantial consensus on a campus, the results show greater consistency in beliefs about uses of student data, and there was little variation by campus. Of 17 items designed to measure beliefs about data use and privacy, respondents on each campus substantially agreed about 15, 16, or all 17. There were small differences across campuses, which may result from locally held FERPA "fear/flex" attitudes and cultures of data sharing across units. Overall, respondents believed that homegrown and vendor-held data is, in most cases, accessible to individuals from other areas of campus, with permission of the unit that holds the data; otherwise, respondents believed that such data was somewhat to largely not eligible for sharing for analysis, research, or other purposes. Table 2 summarizes all responses.

Table 2: Percentage of all respondents who indicated the statement was true.

HOMEGROWN DATA PLATFORM	
Individuals on campus can access data from other areas of campus but only with permission of the unit who holds the data.	59.6%
A unit can analyze its own data without getting IRB approval.	48.1%
Only individuals who work in that area (e.g., admissions, dining) can access data in that system.	38.9%
Individuals on campus can access data from other areas of campus, but only with permission of the unit who holds the data and only if the data are de-identified (no student identifiers attached to the data).	26.0%
Faculty researchers within the institution can access any data once they receive institutional review board (IRB) approval.	24.5%
Outside RESEARCHERS can access and use data with permission of the unit who holds the data.	11.2%
Outside COMPANIES can access and use data with permission of the unit who holds the data.	6.8%
VENDOR DATA PLATFORM	
Individuals on campus can access vendor-held data from other areas of campus but only with permission of the unit who holds the data.	60.2%
A unit can analyze data generated within or about that unit without getting IRB approval.	41.3%
Only individuals who work in that unit (e.g., admissions, dining) can access vendor-held data generated within or about that unit.	38.9%
The vendor can develop and apply algorithms such as predictive analytics to the data without sharing the algorithm with my campus.	32.2%
The vendor can report on the data publicly but only by keeping my institution's name confidential and de-identifying student data.	31.0%
Individuals on campus can access vendor-held data from other areas of campus, but only with permission of the unit who holds the data and only if the data are de-identified (no student identifiers attached to the data).	28.9%
Faculty researchers within the institution can access any data from the vendor once they receive institutional review board (IRB) approval.	24.8%
Outside ACADEMIC RESEARCHERS can access and use data with permission of the vendor.	12.4%
Outside COMPANIES can access and use data with permission of the vendor.	10.0%
The vendor can use the data in any way it wants to.	9.4%

Respondents were evenly split on the question of the need for IRB approval to analyze one's own unit data held on homegrown platforms (48.1 percent said that IRB approval was not required) and substantially split on the same question regarding data held on vendor platforms (41.3 percent said that IRB approval was not required). IRB approval is not generally needed to analyze data for educational improvement purposes, but regardless of the professionals' interpretation of human subjects research policy, the wide discrepancy in beliefs is noteworthy. Also notable is that only one in three respondents believed that vendors could develop and apply algorithms such as predictive analytics to the data without sharing the algorithm with their campus; in fact, many vendors do not share proprietary algorithms with clients.[27] Combined with the responses about trusting vendor algorithms, this finding reveals a potential naivete regarding how vendors actually behave with institutional data and clients.

Beliefs about pandemic-related data usage

In a context in which student data related to COVID-19 testing is of paramount interest,[28] SASS professionals reported beliefs about data privacy that reveal some tensions. Although test results are health-related data, not educational data, four out of five (79.9 percent) respondents believed that if students test positive for COVID-19, appropriate campus offices (e.g., student housing, athletic departments for student athletes, instructors, and/or academic support services for students who must quarantine) should be notified. More than half (52.5 percent) believed that the institution should track the test results (positive or negative) but *only in* student medical records; 29.5 percent believed that the institution should track the test results but only *outside* medical records. This apparent contradiction (positive test results should be shared with campus offices, but test results should be tracked only in medical records) reveals the complexity in how SASS professionals believe they must understand and act regarding student health data in an unprecedented public health crisis.

In terms of student conduct, however, most respondents (67.8 percent) believed that if a student is required to get a COVID-19 test and fails to do so, then appropriate campus offices (e.g., student housing for on-campus students, athletic departments for student athletes, and/or student conduct offices if mandatory testing is part of campus COVID-19 policies) should be notified. One-quarter of respondents believed that institutions should track whether a student got a test *outside* medical records, and 36 percent believed institutions should track this *only in* medical records. FERPA has long covered student behavior data, and respondents demonstrated more consensus in how to approach privacy related to student testing than they showed about handling the results of that testing.

Skills and skill development related to data usage

SASS professionals regularly use multiple data skills to conduct their work. We asked professionals and individuals who supervise professionals to indicate the importance of common data usage skills in their work. Respondents rated each item on a scale from 1 to 4 (Not Important, Somewhat Unimportant, Somewhat Important, Very Important) with an option to indicate "N/A, do not use." There was substantial alignment between professionals and their supervisors regarding the importance of skills. Although professionals in different fields use different skills, the findings indicate a high level of importance overall, and the highest rating (3.8 out of 4.0) was for accessing individual student data. Table 3 presents the professionals' and supervisors' ratings.

Table 3. SASS professionals' and supervisors' ratings of the importance of data skills

Skill	SASS professionals' rating of importance	Supervisors' rating of importance	Number and percentage of professionals indicating N/A, do not use
Accessing individual student data	3.8	3.8	9 (2.7%)
Accessing aggregated student data (e.g., all students in a particular major or student club)	3.4	3.3	24 (7.3%)
Connecting individual student data across platforms (e.g., admissions data to current GPA or demographics to sports participation)	3.4	3.2	33 (10.1%)
Analyzing student data (e.g., to see trends across time in participation)	3.6	3.3	26 (7.9%)
Creating written or verbal reports of data	3.3	3.0	31 (9.5%)
Creating visual reports of data (e.g., charts, figures, graphs)	3.2	3.0	36 (11.0%)

The strong emphasis on accessing, analyzing, and connecting individual student data across platforms demonstrates the need for SASS professionals to be aware of student data privacy policies and procedures. The high value that supervisors place on professionals' need to access individual data reinforces this finding.

Asked where they learned data usage skills and where they expected their supervisees to learn these skills, SASS professionals revealed a wider divergence, reporting that they learned through general training from their institutions (65.8 percent), on their own (60.5 percent), in their work units (59.4 percent), during a course or degree program (29.8 percent), or some other way (6.1 percent). Supervisors reported that they expected their staff to learn through general training at the institution (22.5 percent), training in the work unit (22.5 percent), on their own (8.5 percent), courses or degree programs (5.8 percent), or other (2.0 percent). Supervisors may expect SASS professionals to come to their positions already trained. The discrepancy between where professionals say they learned skills and where supervisors expect them to do so suggests an opportunity to consider more formal education and training in the workplace. This discrepancy also provides clearer understanding of how and what professionals are learning on their own.

Summary of survey findings

SASS professionals are accustomed to using individual student data in their daily work. Their awareness of the range of student data collected, stored, and accessed through homegrown and vendor platforms varies, and is highest for the kinds of data (e.g., admissions files and academic, student conduct, and health-related records) that FERPA and HIPAA regulations have protected for decades. There was less awareness of some data categories that accumulate in campus systems through everyday activities of student life: housing, dining, computer cluster, library usage, transportation, co-curricular participation, and recreational sports. This range of awareness suggests opportunities for educating SASS professionals about which data are available on campus that might be used to promote students' well-being and success, such as understanding how student engagement relates to academic outcomes. The range of beliefs about which categories of data FERPA and HIPAA protect also represent opportunities for education.

Homegrown and vendor platform usage varies across the campuses represented in the sample, but even within-campus analyses show lack of consensus in knowledge of data collection locations. The study incorporated a generous interpretation of 55 percent agreement representing knowledge consensus on a campus, but only one of five campuses reflected consensus on data storage locations for most categories (12 of 23 categories). With regard to SASS professionals' general knowledge of campus data collection locations, the lack of consensus indicates that many professionals are incorrect and there is no shared knowledge across campus. Respondents also displayed various beliefs about who can use data from platforms for which purposes. The trust that SASS professionals place in vendor algorithms and their belief that vendors share those algorithms with clients deserves attention in order to educate professionals about how for-profit companies engage with student data.

SASS professionals rated all of the data skills as important, with accessing student records the most important (3.8 out of 4). Supervisors also rated this skill as most important. But professionals and supervisors have different ideas about where SASS professionals learn how to work with student data. A large percentage of professionals reported that they learned on their own, indicating an opportunity to explore how and what they are learning, and to verify that these skills and knowledge align with unit expectations.

Recommendations

The survey results indicate several recommendations for postsecondary practice, including those aimed at student-facing SASS professionals, their supervisors, and senior leaders (e.g., vice presidents of student affairs or student success services, chief information officers, purchasing agents for SASS software platforms, privacy officers, and IT executives). Recommendations include building and sharing knowledge, addressing disparate beliefs about student data and data privacy, and providing adequate opportunities for SASS professionals to develop and maintain skills related to working with data.

SASS PROFESSIONALS

1. Learn about which kinds of student data exist on campus. SASS professionals should talk to colleagues outside their own units to consider data that may be created in student interactions with campus programs and services such as applications, housing, dining, transportation, or co-curricular activities. Consider ways that these types of data might be able to help improve SASS professionals' work on behalf of students.

2. Learn where student data on campus is collected and stored, whether in homegrown or vendor platforms or both. Ask questions about how vendors use student data and who can access it in identifiable or deidentified forms.

3. Learn who on campus is allowed to access student data and under which circumstances (e.g., educational improvement, educational need to know, research) and when IRB engagement is necessary.

4. Understand the privacy policies and guidelines that govern data use in individual units and on campus.

5. Talk with colleagues about student data and how professionals collect, share, and use it on campus and how vendors use it. When differences in knowledge or beliefs arise, look for the correct answer in campus contexts to build shared, accurate knowledge among SASS professionals.

6. SASS professionals can assess their skills in data usage and talk with their supervisors about where they can learn or refresh skills.

SUPERVISORS OF SASS PROFESSIONALS

1. In addition to following the above recommendations, supervisors should assess supervisees' knowledge of data on campus in different forms and locations inside and outside their units, in homegrown and vendor platforms.

2. Understand where supervisees learn about FERPA, HIPAA, and data usage skills.

3. Offer data privacy education and training in addition to institution-wide offerings on FERPA and HIPAA.

4. Consider ways to increase skill training within units as needed to supplement institutional training and self-education among supervisees.

SENIOR INSTITUTIONAL LEADERS

1. Establish campus-wide, cross-unit conversations about student data and data privacy that go beyond FERPA and HIPAA training requirements, to create shared culture and knowledge of student data.

2. Communicate with SASS units about the student data in different parts of campus.

3. Review current training for employees who work with student data to ensure that it addresses the complexity of the current data environment and the skills necessary to work with it.

4. Develop and share campus-wide guidelines for accessing and working with student data within and across units, regardless of where the data is held. Clarify who needs IRB approval to analyze a unit's data and for what purposes.

References

Blue, A. *Researcher Looks at 'Digital Traces' to Help Students.* The University of Arizona News. (March 7, 2018). https://news.arizona.edu/story/researcher-looks-digital-traces-help-students.

Borgman, C. L. *Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier. Berkeley Technology Law Journal (2018) 33 (2): 365-412.* https://doi.org/10.15779/Z38B56D489.

Botnevik S., Khalil M., and Wasson B. *Student Awareness and Privacy Perception of Learning Analytics in Higher Education*. In C. Alario-Hoyos, M. J. Rodríguez-Triana, M. Scheffel, I., Arnedillo-Sánchez, and S. M. Dennerlein (Eds). Addressing Global Challenges and Quality Education (pp. 374-379). (2020). Springer, Cham. https://doi.org/10.1007/978-3-030-57717-9_30.

Brown, M., and Klein, C. *Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents*. The Journal of Higher Education (2020) 91(7): 1149-1178. https://doi.org/10.1080/00221546.2020.1770045.

Burke, M., Parnell, A., Wesaw, A., and Kruger, K. *Predictive Analysis of Student Data: A Focus on Engagement and Behavior. National Association of Student Personnel Administrators, Inc.* (2017). https://www.naspa.org{filedir_3}predictive_full_4-7-17_download.pdf/.

Couture, R., Schwehm, J., and Couture, V. *FERPA Fear or FERPA Flex: Student Affairs Practitioners' Understanding of Federal Privacy Laws on Campus*. Journal of Student Affairs (2018–2019) 28: 39–50. https://mountainscholar.org/bitstream/handle/10217/211435/JOUF_JOSA_v28_2018-19.pdf?sequence=1#page=39.

Ekowo, M, and Palmer, I. *Predictive Analytics in Higher Education: Five Guiding Principles for Ethical Use. New America.* (March 6, 2016). https://www.newamerica.org/education-policy/reports/predictive-analytics-in-higher-education/.

Gierdowski, D. C., Brooks, D. C., and Galanek, J. *Technology Report: Supporting the Whole Student. EDUCAUSE Research.* (October 19, 2020). https://library.educause.edu/resources/2020/10/2020-student-technology-report-supporting-the-whole-student.

Jarratt, L., Bowman, N. A., Polgreen, L. A., Kruckeberg, T., and Segre, A. M. *Common Data, Uncommon Use: Dining Hall Meal Swipes Predict Retention and Graduation.* Change: The Magazine of Higher Learning (2019) 51(6): 26–33. https://doi.org/10.1080/00091383.2019.1674098.

McKenzie, L. *Early-Alert Systems Seen as Mixed Bag.* InsideHigherEd. *(September 11, 2018).* https://www.insidehighered.com/news/2018/09/11/academics-question-system-measuring-academic-performance-flagging-potential-problems.

Oblinger, D. *Smart Machines and Human Expertise: Challenges for Higher Education.* EDUCAUSE Review. (August 27, 2018). https://er.educause.edu/articles/2018/8/smart-machines-and-human-expertise-challenges-for-higher-education.

Park, J., and Vance, A. *Data Privacy in Higher Education: Yes, Students Care. EDUCAUSE Review.* (February 11, 2021). https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care.

Parnell, A., Jones, D., Wesaw, A., and Brooks, D. C. *Institutions' Use of Data and Analytics for Student Success. National Association of Student Personnel Administrators, Inc., the Association for Institutional Research, and EDUCAUSE. (2018).* https://www.naspa.org/images/uploads/main/DATA2018_DOWNLOAD.pdf.

Reidenberg, J. R., and Schaub, F. *Achieving Big Data Privacy in Education*. Theory and Research in Education (2018) 16 (3): 263–279. https://doi.org/10.1177/1477878518805308.

Schaffhauser, D. *The Rocky Road of Using Data to Drive Student Success.* Campus Technology. (July 26, 2018). https://campustechnology.com/articles/2018/07/26/the-rocky-road-of-using-data-to-drive-student-success.aspx.

Steele, G. E. *Technology and Academic Advising. In T. J. Grites, M. A. Miller, & J. G. Voler (Eds.). Beyond Foundations: Developing as a Master Academic Advisor* (pp. 305–326). (2016). San Francisco: Wiley.

Torres, V., and Renn, K. A. *Does Metric-Centered Leadership Generate More Silos? An Organizational Model for Student Success Integration.* Change (2021), 53 *(2): 49–56.* https://doi.org/10.1080/00091383.2021.1883982.

US Department of Education. *Legislative History of Major FERPA Provisions.* (2004). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html.

US Department of Education. *Table 326.10, Graduation Rates from First Institution for First-Time, Full-Time Bachelor's Degree-Seeking Students*. Digest of Education Statistics (2020). https://nces.ed.gov/programs/digest/d20/tables/dt20_326.10.asp?current=yes.

Vu, P., Adkins, M., and Henderson, S. *Aware, But Don't Really Care: Student Perspectives on Privacy and Data Collection in Online Courses.* Journal of Open, Flexible and Distance Learning (2019), 23 (2): 42–51. http://www.jofdl.nz/index.php/JOFDL/article/view/350.

Yanosky, R. *Integrated Planning and Advising Services: A Benchmarking Study. EDUCAUSE Center for Analysis and Research. (2014).* http://www.educause.edu/ecar.

Endnotes

1 C. L. Borgman, *Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier*, Berkeley Technology Law Journal (2018) 33 (2): 365-412, https://doi.org/10.15779/Z38B56D489 p. 2.

2 V. Torres and K. A. Renn, *Does Metric-Centered Leadership Generate More Silos? An Organizational Model for Student Success Integration,* Change (2021) 53 *(2): 49–56*, https://doi.org/10.1080/00091383.2021.1883982.

3 Ibid.

4 US Department of Education, *Table 326.10, Graduation Rates from First Institution for First-Time, Full-Time Bachelor's Degree-Seeking Students*, Digest of Education Statistics, (2020), https://nces.ed.gov/programs/digest/d20/tables/dt20_326.10.asp?current=yes.

5 It is beyond the scope of this brief to discuss the wider landscape of student data privacy and data analytics. To start reading in this area, consult J. Park and A. Vance, *Data Privacy in Higher Education: Yes, Students Care*, EDUCAUSE Review, (February 11, 2021), https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care; J. R. Reidenberg and F. Schaub, *Achieving Big Data Privacy in Education*, Theory and Research in Education, (2018) 16 (3): 263–279, https://doi.org/10.1177/1477878518805308.

6 A. Parnell, D. Jones, A. Wesaw, and D. C. Brooks, *Institutions' Use of Data and Analytics for Student Success*, National Association of Student Personnel Administrators, Inc., the Association for Institutional Research, and EDUCAUSE, (2018), https://www.naspa.org/images/uploads/main/DATA2018_DOWNLOAD.pdf.

7 G. E. Steele, "Technology and Academic Advising," in T. J. Grites, M. A. Miller, & J. G. Voler (Eds.), *Beyond Foundations: Developing as a Master Academic Advisor* (pp. 305–326), (2016), Wiley.

8 R. Yanosky, *Integrated Planning and Advising Services: A Benchmarking Study*, EDUCAUSE Center for Analysis and Research, (2014), http://www.educause.edu/ecar.

9 EAB, *Navigate*, EAB, (n.d.), https://eab.com/products/navigate/.

10 EAB, *EAB Acquires Starfish*, EAB, (n.d.), https://eab.com/starfish/.

11 See D. Schaffhauser, *The Rocky Road of Using Data to Drive Student Success*, Campus Technology, (July 26, 2018), https://campustechnology.com/articles/2018/07/26/the-rocky-road-of-using-data-to-drive-student-success.aspx, for a description of the California State University system's use.

12 Arizona State University, *Meet eAdvisor™,* ASU (n.d.), https://eadvisor.asu.edu/.

13 L. McKenzie, *Early-Alert Systems Seen as Mixed Bag*, InsideHigherEd, (September 11, 2018), https://www.insidehighered.com/news/2018/09/11/academics-question-system-measuring-academic-performance-flagging-potential-problems.

14 See University of Michigan Information and Technology Services, *Teaching & Learning Data Sets*, University of Michigan, (2021), https://its.umich.edu/enterprise/administrative-systems/data-warehouse/data-areas/teaching-learning.

15 L. Jarratt, N. A. Bowman, L. A. Polgreen, T. Kruckeberg, and A. M. Segre, *Common Data, Uncommon Use: Dining Hall Meal Swipes Predict Retention and Graduation*, Change: The Magazine of Higher Learning (2019) 51(6): 26–33, https://doi.org/10.1080/00091383.2019.1674098.

16 A. Blue, *Researcher Looks at 'Digital Traces' to Help Students*, The University of Arizona News, (March 7, 2018), https://news.arizona.edu/story/researcher-looks-digital-traces-help-students.

17 D. Oblinger, *Smart Machines and Human Expertise: Challenges for Higher Education*, EDUCAUSE Review, (August 27, 2018), https://er.educause.edu/articles/2018/8/smart-machines-and-human-expertise-challenges-for-higher-education.

18 S. Botnevik, M. Khalil, and B. Wasson, "Student Awareness and Privacy Perception of Learning Analytics in Higher Education," in C. Alario-Hoyos, M. J. Rodríguez-Triana, M. Scheffel, I., Arnedillo-Sánchez, and S. M. Dennerlein (Eds), *Addressing Global Challenges and Quality Education* (pp. 374-379), (2020), Springer, Cham, https://doi.org/10.1007/978-3-030-57717-9_30; D. C. Gierdowski, D. C. Brooks, and J. Galanek, *Technology Report: Supporting the Whole Student,* EDUCAUSE Research, (October 19, 2020), https://library.educause.edu/resources/2020/10/2020-student-technology-report-supporting-the-whole-student; P. Vu, M. Adkins, and S. Henderson, *Aware, But Don't Really Care: Student Perspectives on Privacy and Data Collection in Online Courses*, Journal of Open, Flexible and Distance Learning (2019) 23 (2): 42–51, http://www.jofdl.nz/index.php/JOFDL/article/view/350.

19 A. Parnell, D. Jones, A. Wesaw, and D. C. Brooks, *Institutions' Use of Data and Analytics for Student Success*, National Association of Student Personnel Administrators, Inc., the Association for Institutional Research, and EDUCAUSE, (2018), https://www.naspa.org/images/uploads/main/DATA2018_DOWNLOAD.pdf, p. 12.

20 US Department of Education, *Legislative History of Major FERPA Provisions,* (2004), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html, ¶ 16.

21 M. Brown and C. Klein, *Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents*, The Journal of Higher Education (2020) 91(7): 1149–1178, https://doi.org/10.1080/00221546.2020.1770045; R. Couture, J. Schwehm, and V. Couture, *FERPA Fear or FERPA Flex: Student Affairs Practitioners' Understanding of Federal Privacy Laws on Campus*, Journal of Student Affairs (2018–2019) 28: 39–50, https://mountainscholar.org/bitstream/handle/10217/211435/JOUF_JOSA_v28_2018-19.pdf?sequence=1#page=39.

22 R. Couture, J. Schwehm, and V. Couture, *FERPA Fear or FERPA Flex: Student Affairs Practitioners' Understanding of Federal Privacy Laws on Campus*, p. 45.

23 A. Parnell, D. Jones, A. Wesaw, and D. C. Brooks, *Institutions' Use of Data and Analytics for Student Success.*

24 M. Burke, A. Parnell, A. Wesaw, and K. Kruger, *Predictive Analysis of Student Data: A Focus on Engagement and Behavior*, National Association of Student Personnel Administrators, Inc., (2017), https://www.naspa.org{filedir_3}predictive_full_4-7-17_download.pdf/.

25 R. Couture, J. Schwehm, and V. Couture, *FERPA Fear or FERPA Flex: Student Affairs Practitioners' Understanding of Federal Privacy Laws on Campus*, p. 46.

26 University Innovation Alliance, (2021), https://theuia.org/.

27 M. Ekowo, and I. Palmer, *Predictive Analytics in Higher Education: Five Guiding Principles for Ethical Use,* New America, (March 6, 2016), https://www.newamerica.org/education-policy/reports/predictive-analytics-in-higher-education/.

28 The survey did not ask about mask wearing or vaccinations.

FUTURE OF
PRIVACY
FORUM