EXECUTIVE SUMMARY

Understanding Information Security and Privacy in Postsecondary Education Data Systems

JOANNA LYN GRAMA
EDUCAUSE

MAY 2016

EDUCAUSE

POSTSEC DATA

This publication is based on research funded in part by the Bill & Melinda Gates Foundation. The findings and conclusions contained within are those of the authors and do not necessarily reflect positions or policies of the Bill & Melinda Gates Foundation.

Executive Summary

The current national postsecondary education data infrastructure is insufficient to provide decision makers with the data they need most about students and their outcomes. Better data, acquired through both existing initiatives and through other options currently under consideration by education stakeholders, are required to provide meaningful information about student outcomes and to improve higher education. Although stakeholders have expressed concerns about student privacy and information security in light of the growing need for better data, it is possible to protect students and sensitive information while also developing effective data collection strategies and systems.

With thoughtful planning, comprehensive information security and privacy practices can be implemented within the national postsecondary education data ecosystem. For this planning to be successful, all stakeholders in the ecosystem must have a foundational understanding of basic information security and privacy concepts. They also must recognize the most important "big data" information security and privacy concerns such as volume, sensitivity, and access. Finally, while there is no exact formula to guarantee information security and privacy with any data or information technology (IT) solution, stakeholders in the ecosystem should adopt a risk-based approach to thoroughly protecting data in the education ecosystem.

Prior research has indicated that data collection activities designed to solve issues of equity and meaningfully contribute to positive student outcomes are necessary.[1] These data must be protected after they are properly collected. This paper outlines the information security and privacy challenges that exist within the national postsecondary education data infrastructure. It also introduces key language related to information security and privacy in order to provide a common lexicon to frame data protection discussions, describes the general technology architectures considered in the national postsecondary education data infrastructure, summarizes big data information security and privacy concerns, and outlines information security and privacy best practices that could be used to protect data within the national postsecondary education data ecosystem.

Discussions about information security and privacy often fail to meet desired outcomes because technologists and policymakers are not using the same language to describe data protection outcomes. Often concepts are "lost in translation" when both parties do not understand one another. This is quite common when policy and regulatory concepts must be reduced to technological controls that then must be applied to IT systems. To make sure that this does not happen in conversations around and in the further development of the national postsecondary education data ecosystem, it is incumbent upon all stakeholders in the system to understand information security and privacy concepts as they relate to big data.

The current national postsecondary education infrastructure is complex and has many stakeholders and many underlying IT systems. State and/or federal government action likely will be required to successfully steward student data, which includes robust information security and privacy practices. Information security and privacy must be a foundational element of any national postsecondary data system. With intentional, collaborative planning, stakeholders within the national postsecondary education data infrastructure can implement the necessary information security and privacy practices that reduce risk, safeguard data, and ensure transparency, accountability, and trust throughout the entire ecosystem. The following four recommendations form a holistic framework for ensuring effective information security and privacy protections within the national postsecondary education data ecosystem:

1. Adopt a risk-based approach to understanding information security and privacy threats and vulnerabilities.

2. Establish and adhere to a baseline set of information security protections.

3. Establish and adhere to a baseline set of privacy standards.

4. Implement a collaborative governance structure that includes addressing information security and privacy throughout the national postsecondary education data infrastructure.

1 Voight, M., Long, A., Huelsman, M., and Engle, J. (2014). *Mapping the postsecondary data domain: Problems and possibilities*. Washington, DC: Institute for Higher Education Policy. Retrieved from http://www.ihep.org/research/publications/mapping-postsecondary-data-domain-problems-and-possibilities; Engle, J.. (2016) *Answering the call: Institutions and states lead the way toward better measures of postsecondary performance*. Seattle: Bill and Melinda Gates Foundation. Retrieved from http://postsecondary.gatesfoundation.org/wp-content/uploads/2016/02/AnsweringtheCall.pdf

Envisioning the National Postsecondary Data Infrastructure in the 21st Century is a project of the Institute for Higher Education Policy and is supported by the Bill & Melinda Gates Foundation.