UTAH SYSTEM OF HIGHER EDUCATION

MEMORANDUM

December 1, 2023

Adoption of Data Privacy Policies

Adopt proposed Board Policies R1010, Data Breaches, and R1011, Contractual Standards for Use of Personally Identifiable Student Data by Third-Party Contractors, as required by Utah Code Title 53B, Chapter 28, Part 5.

Background

The Utah Higher Education Student Data Protections Act, Utah Code Title 53B, Chapter 28, Part 5, passed in 2022 and amended in 2023, requires the Utah Board of Higher Education to enact several policies to protect the privacy of personally identifiable student data maintained by the Office of the Commissioner of Higher Education and USHE institutions. The first phase of policymaking under the act, focusing on time-sensitive policies specifically required by the act, proposes Board Policy R1010 to address data breach procedures and Board Policy R1011, establishing data protection standards for third-party contractors who use student data.

The proposed policies have been endorsed unanimously by the institutional data privacy officers designated under Utah Code 53B-28-503(4)(a) and reviewed and approved by general counsels. Additional policy proposals addressing USHE data governance planning and standards for institutional data protection policy and planning are anticipated to be completed during the first half of 2024.

R1010, Data Breaches

Utah Code 53B-28-504(2) requires the Board to make rules under the Utah Administrative Rulemaking Act to define a "significant" data breach. "Data breach" is defined in Utah Code 53B-28-501(3). Under Utah Code 53B-28-504(1), institutions are required to notify students of a data breach if it meets the definition of significance established by the Board.

Proposed Board Policy R1010:

- Defines a significant data breach based on the probability of substantial harm to the student;
- Establishes a risk assessment process for determining the likelihood of harm resulting from a data breach modeled on the risk analysis process of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 CFR 164.404;
- Identifies common circumstances in which there is a low probability of harm that are excepted from the definition of a significant data breach without requiring a risk analysis, also modeled on the HIPAA Privacy Rule; and

- Reiterates and clarifies the notification requirements of Utah Code 53B-28-504.

If approved by the Board, the Office of the Commissioner will send this policy through the administrative rulemaking process as required by Utah Code 53B-28-504(2).

R1011, *Contractual Standards for Use of Personally Identifiable Student Data by Third-Party Contractors*

Utah Code 53B-28-502(5)(b)(iii) requires the Board to establish privacy protection standards for the use of student data by third-party contractors. Contracts entered into by either the Board or a USHE institution after January 1, 2024, are required to comply with these standards.

Proposed Board Policy R1011:

- Requires all agreements in which USHE or an institution shares personally identifiable student data with vendors to meet the specific requirements of Utah Code 53B-28-505. Any applicable requirements for written agreements under the Family Educational Rights and Privacy Act (FERPA), 34 CFR Part 99, and any other applicable requirements;
- Provides institutions with flexibility in adopting specific provisions to meet widely varying legal requirements across data-sharing applications in a multi-jurisdictional space without compromising the ability of institutions and USHE to enter into mission-critical contracts; and
- Accepts standardized agreements endorsed by appropriate government authorities as providing equivalent protection to the requirements of Utah Code 53B-28-505 and the proposed Board Policy.

Implementation Guidelines

The higher education privacy officer designated by the Board under Utah Code 53B-28-503(2), in consultation with the institutional privacy contacts designated under Utah Code 53B-28-503(4)(a), will develop guidelines to support institutions in implementing these policies. These guidelines will parallel the extensive guidance on FERPA compliance set by the U.S. Department of Education's Privacy Technical Assistance Center. Guidelines will include model documents required under Utah Code 53B-28-502(4), such as summaries of applicable federal requirements, a catalog of commonly-used information that constitutes personally identifiable student data, best practices for breach response, a model data breach notice, and a model data privacy addendum for use with contractors.

Commissioner's Recommendation

The Commissioner recommends the Board adopt proposed Board Policy R1010, *Data Breaches*, as required by Utah Code 53B-28-504(2), and Policy R1011, *Contractual Standards for Use of Personally Identifiable Student Data by Third-Party Contractors*, as required by Utah Code 53B-28-502(5)(b)(iii).

Attachment

a

R1010, Data Breaches[1]

R1010-1 The following policy has been codified as Utah Administrative Code R765-1010.[2]

R1010-2 References

2.1 Utah Code Title 53B, Chapter 28, Part 5, Higher Education Student Data Protection

R765. Higher Education (Utah Board of), Administration.

R765-1010. Data Breaches.

R765-1010.1. Purpose.

This rule defines "significant data breach" under Section 53B-28-504(2) and establishes standards for an education entity to protect student data by notifying students of significant data breaches under Sections 53B-28-502(5)(b)(1) and 504(1).

R765-1010.2. Authority.

This rule is authorized by Section 53B-28-504.

R765.1010.3. Definitions.

(1) Terms used in this rule that are defined in Section 53B-28-501 and not otherwise defined in this rule have the same definitions as stated therein.

(2) "Personally identifiable student data," as used in this rule:

(a) Is defined by Section 53B-28-501(9); and

[1] *Adopted XXX.*
[2] This administrative rule must also be approved by the Utah Office of Administrative Rules and minor, non-substantive edits to conform with the Utah Administrative Code style guide may be made.

(b) Excludes information designated as directory information in accordance with the education entity's directory information policy, as described in 34 C.F.R. Section 99.37.

R765.1010.4. Significant Data Breaches.

(1) Except as provided in paragraph (2) of this section, a data breach is significant if the education entity that maintains the personally identifiable student data released, accessed, or disclosed in the breach determines that there is a moderate or high probability of substantial harm to the student based on a risk assessment considering the following factors based on the totality of the circumstances:

(a) The nature and extent of the personally identifiable student data involved, including the types of identifiers and the likelihood of re-identification;

(b) The degree to which the release, access, or disclosure of the personally identifiable student data breached could be used for unlawful purposes including subjecting an affected student to an invasion of privacy, heightened risk of unlawful discrimination, or identity theft or fraud;

(c) The unauthorized person who used the personally identifiable student data or to whom the disclosure was made;

(d) The likelihood that the personally identifiable student data was actually acquired or viewed;

(e) The extent to which the potential harm and risk to the student have been mitigated;

(f) The extent to which prompt notification would allow affected students to further mitigate the harm and risk to them in addition to the actions that the education entity can take itself; and

(g) Other factors that affect the likelihood that the incident is likely to result in substantial harm to the student.

(2) A data breach is not significant to the extent that the breach involves:

(a) Any inadvertent or unintentional acquisition, access, or use of personally identifiable student data by an employee or other person acting under the authority of an education entity or third-party contractor to another employee or other person acting under the authority of an education entity or third-party contractor, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under Utah Code Title 53B, Chapter 28, Part 5 or 34 C.F.R. Part 99;

(b) A disclosure of personally identifiable student data where an education entity or third-party contractor has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain, use, or disclose such student data;

(c) A disclosure of personally identifiable student data where the education entity has implemented safeguards, such as encryption, which the education entity has a good faith belief that render the personally identifiable student data unreadable or unusable;

(d) A disclosure of personally identifiable student data that was lawfully published or was otherwise lawfully in the public domain prior to the disclosure; or

(e) A disclosure of the personally identifiable student data of fewer than twenty-five individuals.

R765.1010.5. Notification of Significant Data Breaches.

(1) If a significant data breach occurs either at an educational entity or a third-party contractor using data disclosed by an educational entity, the educational entity shall notify each student in writing whose personally identifiable student data was disclosed.

(a) The notification shall include all components of the model data breach notification prepared under Section 53B-28-502(4)(b)(iii). An education entity may add additional content to the notification.

(b) The notification may be communicated by any written means that the education entity routinely uses for official communications with individual students.

(2) An education entity that provides notice of a data breach to affected individuals as required under any other law is deemed to have met the requirements of this rule with regard to the individuals so notified.

(3) Notifications regarding release, access, or disclosure of a record containing protected health information as defined in 45 C.F.R., Part 164, Standards for Privacy of Individually Identifiable Health Information, shall be governed by that part.

(4) The Office of the Commissioner of Higher Education may develop and communicate to institutions guidelines for compliance with this policy.

R1011, Contractual Standards for Use of Personally Identifiable Student Data by Third-Party Contractors[1]

R1011-1 Purpose: This policy establishes standards for a third-party contractor's use of student data as required by Utah Code section 53B-28-502(5)(b)(iii).

R1011-2 References

2.1 Utah Code Title 53B, Chapter 28, Part 5, Higher Education Student Data Protection

2.2 20 United States Code § 1232g, Family Educational Rights and Privacy Act

2.3 34 Code of Federal Regulations Part 99, Family Educational Rights and Privacy

2.4 United States Department of Education Privacy Technical Assistance Center, "The Family Educational Rights and Privacy Act: Guidance for Reasonable Methods and Written Agreements" (June 2015)

2.5 United States Department of Education Privacy Technical Assistance Center, "Frequently Asked Questions—Disclosure Avoidance" (May 2013)

2.6 Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ 2016 L 119/1, Art. 4(1), Art. 9(1), General Data Protection Regulation ("GDPR")

R1011-3 Definitions

3.1 Terms used in this policy that are defined in Utah Code section 53B-28-501 and not otherwise defined in this policy have the same definitions as stated therein.

3.2 "Data Processing Contract"

3.2.1 Means any written agreement, regardless of form, title, or description, that shares personally identifiable student data and is binding on a third-party contractor and an education entity; and

3.2.2 Excludes:

3.2.2.1 Agreements directly between users and providers of a service that do not fall under subsection 3.2.1; and

[1] *Adopted XXX.*

3.2.2.2 Software licensing agreements that do not involve transfer of personally identifiable student data.

3.3 "Personally Identifiable Student Data"

3.3.1 Is defined by Utah Code section 53B-28-501(9); and

3.3.2 Excludes information designated as directory information in accordance with the education entity's directory information policy, as described in 34 C.F.R. section 99.37.

R1011-4 Standards for Data Processing Contracts

4.1 Use of Standard Agreements: A data processing agreement or agreement to abide by standardized model data protection clauses that have been pre-approved by the European Commission, or by another legal authority to which a third-party contractor is subject that is stricter than the requirements of this policy, under which an education entity discloses personally identifiable student data to a third-party contractor shall be considered as in compliance with this policy.

4.2 Requirements for Non-Standard Agreements: Except as provided in Utah Code section 53B-28-505(7), when an education entity or a government agency contracting on behalf of an education entity enters a data processing contract with a third-party contractor to disclose personally identifiable student data to the contractor without using a standard agreement as described in subsection 4.1, the education entity or agency should ensure that the data processing contract terms include provisions that:

4.2.1 Require the third-party contractor to limit use of personally identifiable student data received under a data processing contract with an education entity strictly to the purpose of providing the contracted product or service within the negotiated data processing contract terms;

4.2.2 Establish requirements and restrictions related to the collection, use, storage, or sharing of the student data by the third-party contractor that are necessary for the education entity to ensure compliance with the applicable requirements for written agreements under the Family Educational Rights and Privacy Act (*see* subsections 2.2 and 2.3), restrictions on contractors under Utah Code section 53B-28-505, other applicable law, and Board policy;

4.2.3 Identify the persons, or type of persons, including affiliates of the third-party contractor such as subprocessors, affiliates, officers, agents, employees, or directors, with whom the third-party contractor may share student data;

4.2.4 Describe the data disposition processes by which the contractor will return, delete, or destroy personally identifiable student data after it is no longer to be retained or upon request of the education entity; and

4.2.5 Permit the education entity or the education entity's designee, at its request, to audit the third-party contractor to verify compliance with the data processing contract and applicable legal provisions and require the contractor to cooperate with such an audit.

R1011-5 Guidelines for Agreements: The Office of the Commissioner of Higher Education shall develop and communicate to institutions guidelines for compliance with this policy.