December 19, 2023

Vanessa Wrenn

Chief Information Officer

Technology Services and Digital Learning

North Carolina Department of Public Instruction

Dear Ms. Wrenn,

We appreciate the work the North Carolina Department of Public Instruction (NCDPI) has put into protecting the privacy and security of student data, as well as the recent updates to their required policies. After review and feedback from members, we are writing to express our continuing concerns about the requirements listed in the updated "Data Confidentiality and Security Agreement for Online Service Providers and Public School Units" (Agreement) as well as to request additional clarity from the DPI on certain issues of critical importance to our community:

- The requirement that the vendor request the public school unit's (PSU) advanced review and approval for both the use of subcontractors and the sharing of data with any subcontractor would be unnecessarily time-consuming for both the PSU and the vendor.
    - *We suggest requiring the vendor to obligate subcontractors to follow the privacy and security requirements outlined in the vendor's contract.*
- The definition of shared data goes beyond the scope of data defined by the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99) and in North Carolina statute (Chapter 115C Article 29).
    - *We suggest aligning the definition of shared data to align with state and federal law.*
- The 24-hour breach disclosure timeframe and requirements (such as the 48-hour status report and 48-hour postmortem report, as well as direct notification to students, parents, and employees) may be operationally difficult, if not impossible, to meet.
    - *We suggest at least seventy-two (72) hours after the vendor confirms that there is a breach, and if that breach poses a risk of harm to customer data.*
- The Agreement states the vendor must provide confidential information related to the breach as reasonably requested by NCDPI. However, there is no apparent nondisclosure agreement directly between NCDPI and Vendor to ensure that NCDPI has a duty of confidentiality regarding Vendor's confidential information.

- *We suggest that if the NCDPI requests confidential information from the vendor, then there must be an inherent and written duty of confidentiality between the vendor and NCDPI.*

- NCDPI still states that there are to be no changes to the Agreement, however, the new Authorization to Operate Letter indicates that, at the PSU's own risk, the PSU may accept a Vendor's modifications to the Agreement.
    - *We suggest that NCDPI allows for more flexibility on reasonable and necessary modifications to the Agreement, on a case-by-case basis.*

- The vendor compliance with NCDPI's recent updates to the third-party assessment standard will take significant time, in excess of the brief notification period allotted between November 2023 and January 1, 2024.
    - *We suggest that if a third-party assessment should be required, that NCDPI provide a more lenient timeframe to complete this assessment, preferably by the annual state education funding deadline for the upcoming school year.*

- The requirement to submit to a third-party penetration test with required remediation dictated by that third-party, prior to use authorization, would not be feasible for our members. The Agreement states that this request is at the sole discretion of the PSU, meaning that the expectations will vary depending on the PSU and the product.
    - *We suggest a better solution would be allowing the vendor to share a table of contents from a non-confidential report, that is from a nationally-recognized, cybersecurity framework, such as the Service Organization Control Type 2 (SOC 2) or other industry-standard frameworks.*

- Contrary to NC's student data privacy statute[1], the Agreement still seems to imply that the customer owns de-identified, aggregated data and metadata. After looking at NC's student data privacy statute, there is nothing written that implies a customer could own this type of data, and on the contrary, there are provisions in NC law that permit operators to use this data to improve educational services.
    - *We suggest that NCDPI revise the Agreement to require the vendor to comply with the applicable aforementioned NC law.*

- The timeline for which the vendor shall permanently delete or destroy the customer's data and provide the customer with written notice of destruction, after the termination of the subscription, lacks clarity. More specifically, it requires the vendor to: extract data within 90 days; and complete destruction and written consent to PSU "promptly" but not less than 30 days.
    - *We suggest that the vendor destroys the data at the earliest of customer request; or pursuant to the vendor's data retention policy.*

[1] N.C.G.S § 115C-402.5 (https://www.ncleg.gov/enactedlegislation/statutes/pdf/bysection/chapter_115c/gs_115c-402.5.pdf)

Additional Questions from the Education Industry

1. How do you know what qualifies as an approved third-party conducted assessment? What if it is not currently listed in the provided list, but it is more rigorous than some of the other types of assessments listed?
2. Can you clarify whether the security information provided as required by Sections 6 and 7 of the Agreement would have the same protections as set out in Section 8(i) of the Agreement with regard to the Public Records Act?
3. In the "Process Overview Flow Chart," why is "Vendor Self-Assessment: 1EdTech" grayed out?
4. For purposes of the third-party conduct assessment report requirement, is the International Organization for Standardization (ISO) 27001 certificate[2] issued by a third-party auditor sufficient to satisfy this portion of the NCDPI process?

We look forward to the continuous collaboration with NCDPI. Thank you for your time and attention to responding to these and other questions from the vendor and school community.

Regards,

Christopher A. Mohr

President

Software & Information Industry Association (SIIA)

[2] https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en