To: School District’s Technology Supervisor

From: OhCR Assist Team

Date: March 11, 2023

Subject: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations

The NIST Core V1.1 Cybersecurity Assessment’s ID.GV-3 requirement: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood, and managed, begins with research at the school district.

In the OhCR Cybersecurity Assessment and Gap Analysis, the school district’s onsite and cloud networks are in possession of Personal Identifying Information (PII), Protected Health Information (PHI), and Payment Card Industry (PCI) information and K12 student grades.

In our research, the School Districts is subject to the following data security requirements:

* FERPA Data Security Requirements
  + Confidential Information includes “education records,” as that term is defined in the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. 1232g, 34 CFR Part 99, and Ohio Revised Code 3319.321.
* HIPAA Data Security Requirements
  + Centers for Medicare and Medicaid Services (CMS) as well as Ohio Department of Medicaid requires HIPAA and NIST data security compliance by contract agreement.
    - School Nurse maintains health records on students.
    - The Athletic department collects physicals for student athletes.
    - The school district may have shot records at the enrollment office.
* NIST Data Security Requirements
  + IRS 1075 Financial Audits by contract agreement.
  + Centers for Medicare and Medicaid Services (CMS) as well as Ohio Department of Medicaid requires HIPAA and NIST data security compliance by contract agreement.
  + Some Ohio schools receive CJIS funding. Criminal Justice Information Services (CJIS) Security Policy Version 5.6 (06/05/2017) requires NIST data security controls.
* PCI
  + By assessment, the school district engages with cloud-based network systems that collect money using credit card payment.

The school district will use data flows (ID.AM-3: Organizational communication and data flows are mapped) to identify the location of critical data.

The School District will need to achieve and sustain NIST Core V1.1 compliance.

* + The School District needs to apply the NIST data security controls to protect the data to their internal and external (cloud based) networks.
  + Once NIST compliant, the School District executives can evaluate their program to the Ohio ‘Safe Harbor’ law.
  + The School District executives need to maintain the NIST Risk Management program annually.
  + The School District executives need to maintain and train their local Incident Response team utilizing the Ohio Cyber Reserve and the Ohio Cyber Range Institute with Regional Programming Center (RPC) support.
  + The School District Technology Department needs to maintain the Cybersecurity Assessment and Gap Analysis with an internal auditor.
  + The School District needs to continue to train Staff, Teachers, and Students to protect data.

The School District will invite the Ohio Cyber Reserve to update the Cybersecurity Assessment and Gap Analysis annually.

End of report.