Volume 5, Issue 3

January 17, 2014

WSPA
WASHINGTON SCHOOL PERSONNEL ASSOCIATION

FOOD FOR THOUGHT

Student Data Breaches: Is Your District Prepared?

Unauthorized disclosure of confidential student data can occur, despite best efforts. Disclosure occurs when personally identifiable information (PII) from a student's education records is made available to a third party who does not have legal authority to access the information.

This can happen through a malicious attack by hackers gaining access to school computer systems or inadvertently when laptops, phones, or thumb drives are lost, stolen, or temporarily misplaced, employees negligently leave a password list in a publicly accessible location or misconfigure a security device, or through system failure such as the failure to backup security measures.

FERPA does not contain specific breach notification requirements, although it does require that school districts records each incident of data disclosure. 34 CFR §99.32.

Washington law requires any agency that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach to any individual whose unencrypted personal information may have been acquired by an unauthorized person. RCW 42.56.590.

Districts should consider putting policies and procedures in place to define "student data breach" and detail its efforts to prevent breaches as well as its response plan including notification of affected individuals and relevant agencies.

Additionally, direct student notification is advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

The Family Policy Compliance Office (FPCO), U.S. Department of Education has offered letters of guidance:

- *Letter to Parades* (2005)

Laptop containing student information was stolen and FPCA praised "quick and thorough" response to report incident to local police department and immediately notify students and assist in contacting credit bureaus.

- *Letter to Fagan* (2012)

School attorney reported to FPCA that flash drive containing students' education records went missing from a classroom. FPCO confirmed that it was an "inadvertent disclosure."

U.S. Department of Education Privacy Technical Assistance Center (PTAC) Data Breach Response Checklist

The items in this checklist (developed by PTAC) are the essential building blocks of an effective and efficient data breach response plan. The list below is not exhaustive and should be used only as a general guide, to be expanded and tailored to your district's unique operational and safety needs:

Before the Breach

✔ Establish and implement a written data breach response policy.

✔ Review your information system(s) and data and identify where PII and other sensitive information resides.

✔ Continuously monitor for PII and other sensitive data leakage and loss.

✔ Conduct frequent privacy and security awareness trainings as part of an on-going training and awareness program.

Responding to the Breach

✔ Validate the data breach

✔ Once a breach has been validated, immediately assign an incident manager to be responsible for the investigation

✔ Assemble incident response team

✔ Determine the scope and composition of the breach

✔ Determine the scope and composition of the breach

✔ Consider notifying FPCO and seeking technical assistance from PTAC

✔ Determine whether to notify the authorities/law enforcement (situation dependent)

✔ Decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved

✔ Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification

✔ Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification

For more information: www.ed.gov/ptac