Public Records Training

October 6, 2017

Public Records and Private Police

Presented By
Warren I. Grody
Joshua D. Nolan

Bricker & Eckler LLP
Barnesville · Columbus · Cincinnati-Dayton · Cleveland · Marietta
www.bricker.com

I. Where We Are

A. Overview

1. University and college police departments must respond to public records requests

2. Police Department v. Campus Security Department

3. Interaction between FERPA and public records law.

    a. FOIA vs Ohio public records?

4. What is a public record?

    a. "Public record" means records kept by any public office, including, but not limited to, state, county, city, village, township, and school district units, and records pertaining to the delivery of educational services by an alternative school in this state kept by the nonprofit or for-profit entity operating the alternative school pursuant to section 3313.533 of the Revised Code.

    b. There are many exceptions to this definition. See O.R.C. 149.43.

5. Emails

    a. Emails that meet the definition of a public record are public records

    b. It is the message or content of the document that makes it a public record and not the medium on which the document is created, transmitted or kept. *State ex rel. Margolius v. Cleveland* (1992), 62 Ohio St.3d 456.

    c. Exceptions to the PRA apply to emails just like they do to other public records kept in any other format.

    d. If an email (or any other public record) contains information that is a public record and information that is not, the non-public information can be redacted and the rest of the email must be released.

6. Security and Infrastructure Records

    a. Revised Code Section 149.433 (B) states that, "A record kept by a public office that is a security record or an infrastructure record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section."

    b. "Infrastructure record" means any record that discloses the configuration of a public office's or chartered nonpublic school's critical systems including, but not limited to, communication, computer, electrical, mechanical, ventilation, water, and plumbing systems, security codes, or the infrastructure or structural configuration of the building in which a public office or chartered nonpublic

school is located. "Infrastructure record" does not mean a simple floor plan that discloses only the spatial relationship of components of a public office or chartered nonpublic school or the building in which a public office or chartered nonpublic school is located.

c. "Security record" means any of the following:

(a) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage;

(b) Any record assembled, prepared, or maintained by a public office or public body to prevent, mitigate, or respond to acts of terrorism, including any of the following:

(i) Those portions of records containing specific and unique vulnerability assessments or specific and unique response plans either of which is intended to prevent or mitigate acts of terrorism, and communication codes or deployment plans of law enforcement or emergency response personnel;

(ii) Specific intelligence information and specific investigative records shared by federal and international law enforcement agencies with state and local law enforcement and public safety agencies;

(iii) National security records classified under federal executive order and not subject to public disclosure under federal law that are shared by federal agencies, and other records related to national security briefings to assist state and local government with domestic preparedness for acts of terrorism. (ORC 149.333(A)(2)-(3).)

7. Financial Records

8. Personnel Files

a. "[N]ot all items in a personnel file may be considered public records * * *. To the extent that any item contained in a personnel file is not a 'record,' i.e., does not serve to document the organization, etc., of the public office, it is not a public record and need not be disclosed." *State ex rel. Fant v. Enright* (1993), 66 Ohio St.3d 186, 188.

B. Confidential Law Enforcement Investigatory Records (CLEIRs) Are Not Public Records.

1. Under the public records law, Confidential Law Enforcement Investigatory Records may be withheld from disclosure. R.C. §149.43(A)(1)(h) and (A)(2).

    a. Records may be withheld if they both:

        i. Pertain to a law enforcement matter of a criminal, quasi-criminal, civil, or administrative nature, and

        ii. If released would create a high probability of disclosing any of the following information:

            (a) Identity of a suspect who has not been charged with the offense to which the record pertains;

            (b) Identity of an information source or witness to whom confidentiality has been reasonably promised;

            (c) Information provided by an information source or witness to whom confidentiality has been reasonably promised, which information would reasonably tend to disclose the source's or witness's identity;

            (d) Specific confidential investigatory techniques or procedures or specific investigatory work product;

            (e) Information that would endanger the life or physical safety of law enforcement personnel, a crime victim, a witness, or a confidential information source.

2. Remember also that LEADS and OHLEG information are not public records. See OAC 4501:2-10-06(C); R.C. § 109.57(D)(1)(b).

C. If FERPA or Clery Protects It, It's Not a Public Record.

1. If FERPA prohibits disclosure, a record cannot be released pursuant to Ohio's Public Records law. See R.C. § 149.43(A)(1)(v) (defining "public record" to exclude "records the release of which is prohibited by state or federal law).

2. The Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232g, 34 C.F.R. Part 99, prohibits educational institutions from disclosing educational records, or the personally identifiable information contained therein, without the written consent of the student, unless an exception is met.

    a. "Education records" include records that are directly related to a student and are maintained by the institution. It does not matter whether the institution created

the records or another person/entity created them, so long as the institution has the records in its possession.

i. Directly related to a student

(a) Some courts hold that records are not directly related to a student if they do not document information related to the student's education.

(b) The Ohio Supreme Court rejected this approach in *State ex rel. ESPN, Inc. v. Ohio State University*, 2012 Ohio 2690.

(i) Upon consideration of our opinion in *Miami Student* and the Sixth Circuit Court of Appeals' opinion in *Miami Univ.*, we agree with the Sixth Circuit and hold that the records here generally constitute "education records" subject to FERPA because the plain language of the statute does not restrict the term "education records" to "academic performance, financial aid, or scholastic performance." Education records need only "contain information directly related to a student" and be "maintained by an educational agency or institution" or a person acting for the institution. 20 U.S.C. 1232g(a)(4)(A)(i) and (ii). The records here—insofar as they contain information identifying student-athletes—are directly related to the students.

ii. However, "education records" do not include law enforcement records created by campus law enforcement for purposes of law enforcement.

(a) If a record was not created by campus law enforcement but is maintained in their files, the record is still an education record subject to protection under FERPA.

(b) If a record was created by campus law enforcement exclusively for a non-law enforcement purpose, such as a disciplinary action or proceeding conducted by the institution, the record is an education record subject to protection under FERPA.

iii. FERPA neither requires nor prohibits the disclosure of law enforcement records by the institution.

b. "Personally identifiable information" includes, among other things:

i. Student's name, address, date of birth, and place of birth

ii. Names of student's family members

iii. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

iv. Information requested by a person who the institution reasonably believes knows the identity of the student to whom the education relates.

3. Students who believe their FERPA rights have been violated may file a complaint with the U.S. Department of Education Family Policy Compliance Office. Failure to comply with FERPA could result in a loss of federal funding for the institution.

4. FERPA specifically allows records to be disclosed without student's consent in certain situations. For purposes of law enforcement, the most common exceptions are as follows:

   a. Internal Disclosure – Records may be released to institution officials that have a legitimate educational interest in the records.

   b. Directory Information – Personally identifiable information that has been designated in the institution's policy as "directory information" can be released without consent unless the student has indicated to the college or university that he or she does not wish for such information to be released. Examples of commonly designated directory information include a student's name, class year, major, date of graduation, email address, and dates of attendance.

   c. Underage Drinking/Drugs – Parents may be notified without a student's consent if there is a disciplinary action by the institution for use or possession of alcohol or a controlled substance if the student is 21 years old at the time of the disclosure to the parent.

   d. Imminent Emergencies – The institution can disclose personally identifiable information from education records to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or others.

      i. The institution must look at the "totality of the circumstances" to determine whether there is an "articulable and significant threat" to health or safety of a student or others before it discloses personally identifiable information.

      ii. The U.S. Department of Education has indicated that there must be an "actual, impending, or imminent emergency" or a situation where warning signs lead school officials to believe that the student "may harm himself or others at any moment." However, an emergency does not mean threat of a possible emergency for which the likelihood of occurrence is unknown.

   e. Certain Disciplinary Proceeding Results – The institution may disclose the final results of a disciplinary hearing where the student is an alleged perpetrator of a crime of violence or non-forcible sex offense and the institution has determined that the student has committed a violation of the institution's rules or policies. The institution may not disclose the names of victim(s)/witnesses without the prior written consent of those students whose names would be disclosed.

5. FERPA does not prohibit the institution from disclosing, to an alleged victim of any crime of violence or a nonforcible sex offense, the final results of any institutional disciplinary proceeding conducted against the alleged perpetrator of such crime or offense with respect to that crime or offense. 20 U.S.C. § 1232g(b)(6)(A). (See Clery/VAWA Implications, below.)

    a. "Final result" includes only the name of the student, the violation committed, and the sanction imposed. It may include the name of other students, such as victims or witnesses, only with the written consent of the other students.

6. FERPA does not prohibit an institution from disclosing the final results of any disciplinary proceeding conducted by the institution against a student who is an alleged perpetrator of any crime of violence or a nonforcible sex offense, if the institution determines as a result of that disciplinary proceeding that the student committed a violation of the institution's rules or policies with respect to such crime or offense. 20 U.S.C. §1232g(b)(6)(B).

    a. "Final result" includes only the name of the student, the violation committed, and the sanction imposed. It may include the name of other students, such as victims or witnesses, only with the written consent of the other students.

7. If FERPA protects a record from release without consent and no exception is met that would otherwise allow for disclosure, the record cannot be released without a subpoena or court order, or without redacting all personally identifiable student information.

    a. If redacting, no student's identity may be personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. Remember to "black redact" so that it is clear that information has been redacted, and a cover letter must be included with the public records release to explain the reasons for the redactions.

8. Clery Act/VAWA Implications – Keep Calm and Carry On

    a. Notwithstanding FERPA or the Public Records laws, if you are required to release it under Clery/VAWA, you must continue to release it. Examples:

        i. Daily Crime Log:

            (a) You may continue to withhold information about the nature, date, time, and general location of each crime and/or the disposition of the complaint only if there is clear and convincing evidence that the release of the information would:

                (i) Jeopardize an ongoing criminal investigation or the safety of an individual;

                (ii) Cause a suspect to flee or evade detection; or

(iii) Result in the destruction of evidence. 34 C.F.R. § 668.46(f)(1) and (2).

(b) Updates to the daily crime log, unless the disclosure is prohibited by law or would jeopardize the confidentiality of the victim. 34 C.F.R. § 668.46(f)(2) and (4).

(c) Note that the Daily Crime log must open for public inspection for 60 days, and after that it must be available within two business days of a request for public inspection. This is typically a faster turnaround than R.C. §149.43 would otherwise require, and it would control.

ii. Missing Person notification

(a) If a student provides the institution with contact information in case they go missing, notification of that person should occur within 24 hours of the determination that the student is missing. 34 C.F.R. § 668.46(h)(1)(iii). This contact information is otherwise to be kept confidential unless used in a missing person investigation. 34 C.F.R. §668.446(h)(1)(iv). (The institution must also notify the custodial parent if the student is a minor.)

iii. The complainant and respondent in a sexual misconduct proceeding (i.e. dating violence, domestic violence, sexual assault, or stalking) must be simultaneously notified in writing of:

(a) the result of any institutional disciplinary proceeding,

(b) the institution's procedures for the accused and the victim to appeal the results, if such procedures are available;

(c) any change to the result; and

(d) when the results become final. 34 C.F.R. § 668.46(k)(v). Note that these provisions are explicitly exempt from FERPA. 34 C.F.R. § 668.46(l).

b. If you are required to keep something confidential under Clery/VAWA, you must continue to withhold it. This controls over the Public Records laws. Examples:

i. Withholding victim identification in timely warnings and emergency notification. 34 C.F.R. §668.46(e)(1).

ii. Institutions must complete public recordkeeping, including Clery Act reporting disclosures, without the inclusion of personally identifying information about the victim. 34 C.F.R. § 668.46(b)(11)(iii)(A).

iii. Institutions must keep confidential any accommodations or protective measures provided to the victim, to the extent that maintaining such

confidentiality would not impair the ability of the institution to provide the accommodations or protective measures. 34 C.F.R. § 668.46(b)(11)(iii)(B).

D. Home Addresses and Family Information of Peace Officers Are Usually Not Subject To Release.

1. Under the public records law, the "residential and familial information" of a peace officer is not considered a public record and therefore is not subject to disclosure. R.C. § 149.43(A)(1)(p). This includes records that disclose:

   a. The address of the actual personal residence of a peace office, except for the state or political subdivision in which the peace office resides;

   b. Information compiled from referral to or participation in an employee assistance program;

   c. The social security number, residential telephone number, any bank account, debit card, charge card, or credit card number, or the emergency telephone number of, or any medical information pertaining to, a peace officer;

   d. The name of any beneficiary of employment benefits, including, but not limited to, life insurance benefits, provided to a peace officer by the peace officer's employer;

   e. The identity and amount of any charitable or employment benefit deduction made by the peace officer's employer from the peace officer's compensation unless the amount of the deduction is required by state or federal law;

   f. The name, residential address, name of employer, address of employer, social security number, residential telephone number, any bank account, debit card, charge card, or credit card number, or the emergency telephone number of the spouse, a former spouse, or any child of a peace officer;

   g. A photograph of a peace officer who holds a position or has an assignment that may include undercover or plain clothes positions or assignments as determined by the peace officer's appointing authority.

2. Certain exceptions exist where the records are requested by a journalist. See R.C. §149.43(B)(9).

II. Records Retention

A. Adopting Your Records Retention Schedule

1. Local Records Commission

   a. For many public offices, the makeup of the records commission is set forth in statute.

i. No such statute for a private university or college police department.

ii. Suggestion: University President (or her designee), its Chief Financial Officer and the Chief of Police.

b. Approves your Schedule.

c. Forwards Schedule to the Ohio History Connection.

d. The records commission is required to hold at least one public meeting a year from that point forward. The purpose of this meeting is to approve any future proposed changes to the schedule and applications for one-time disposal of obsolete records.

2. Ohio History Connection

a. The OHC has up to 60 days to conduct its review.

b. Forwards the Schedule to the Auditor.

3. Ohio Auditor

a. The Auditor also has 60 days to approve the schedule.

b. Returns the approved Schedule to the college or university.

4. Once you receive your approved Schedule, you may start disposing of records in accordance with the Schedule.

B. Warning – Email is not a records series or category – retention is based on content

C. Penalties for illegal destruction of Records – R.C. 149.351.

1. An aggrieved person is entitled to injunctive relief, a $1,000 civil forfeiture for each illegally destroyed public record and attorney fees.

2. Civil forfeiture capped at $10,000 and attorney fees capped at the amount of civil forfeiture.

3. Five year statute of limitations.