Ratwik, Roszak & Maloney, P.A.

730 Second Avenue South, Suite 300
Minneapolis, Minnesota 55402

(612) 339-0060
Fax (612) 339-0038
www.ratwiklaw.com

A Deep Dive into Data: Taking a Closer Look at the Intersection of Special Education & Data Privacy

Elizabeth M. Meske
emm@ratwiklaw.com

2017 MASE Fall Leadership Conference
October 27, 2017

I. LAWS GOVERNING DATA PRIVACY

Data about students are governed by both state and federal law. Specifically, the Minnesota Government Data Practices Act governs data relating to students and incorporates by reference much of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g, and its implementing regulations, 34 C.F.R. Part 99. In addition to FERPA and the MGDPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. Accordingly, school district employees must be prudent when disseminating any information about special education students to ensure compliance with the MGDPA and federal law.

Note: Data privacy laws are complex and fact-specific. While it is important for all school personnel to have an understanding of the laws, it is very important to seek advice from an attorney or school district administrator, who has been designated as the school district's "responsible authority," if there are any uncertainties regarding data privacy.

A. The Family Educational Rights and Privacy Act (FERPA).

FERPA is a federal law that protects the privacy of student education records. FERPA applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education. This includes virtually all public schools and school districts.

Note: School districts must comply with FERPA with respect to the education records of the student placed at a private school. Though, private and religious elementary and secondary schools generally do not receive funds from the Department of Education and are, therefore, not subject to FERPA, if a school district places a student with a disability in a private school that is acting on behalf of the school district with regard to providing services to that student, the records of that student are still subject to FERPA.

B. The Individuals with Disabilities Education Act (IDEA).

The IDEA is a federal law that ensures students with a disability are provided with a Free Appropriate Public Education (FAPE). Pursuant to the IDEA, the United States Secretary of Education is required "to ensure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by State educational agencies and local educational agencies…." 20 U.S.C. § 1417(c). The privacy protections under Part B of the IDEA are found at 34 CFR 300.560–300.577.

C. The Minnesota Government Data Practices Act (MGDPA).

The MGDPA is a state law that controls how government data are collected, created, stored/maintained, used, and released/disseminated. The MGDPA sets out certain requirements relating to the right of the public to access government data and the rights of individuals who are the subjects of government data. Educational data are classified and governed by this law.

1. **Government Data Defined.** The term "government data" is defined as all data collected, created, received, maintained or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media, or conditions of use. Minn. Stat. § 13.02, subds. 7 and 7(a). All government data is classified as public unless it is specifically classified otherwise by law. Minn. Stat. § 13.03.

   Note: The mere fact that government employees observe or hear information does not cause the information to become government data that are subject to the MGDPA. However, once data are recorded in any

form, the data become "government data" regardless of their physical form, storage media or the conditions of their use.

2. **Classifications of Data.** The three types of data that generally arise in the educational setting are public data, private data, and confidential data.

   a. Public data on individuals: data which the public may access because no state or federal law or regulation denies such access. Minn. Stat. § 13.02, subd. 15.

      Note: Data on individuals is all government data in which an individual is or can be identified as the subject of that data, unless the appearance of the data can be clearly shown to be incidental. *See KSTP-TV v. Ramsey County*, 787 N.W.2d 198 (Minn. App. 2010). Data is "data on individuals" if it identifies an individual in itself, or if it can be used in connection with other data elements to uniquely identify an individual. Minn. R. 1205.0200, subp. 4.

   b. Private data on individuals: data which the public may not access under the law, but which is accessible to the subject of the data. Minn. Stat. § 13.02, subd. 12.

   c. Confidential data on individuals: data which neither the public nor the subject of the data may access. Minn. Stat. § 13.02, subd. 3.

II. EDUCATIONAL DATA

A. Definitions.

1. **Educational Data.** Per the MGDPA, "educational data" means data on individuals maintained by an educational agency or institution or by a person acting for an educational agency or institution which relates to a student. Minn. Stat. § 13.32, subd. 1(a).

   a. "Student" means an individual currently or formerly enrolled or registered, or an applicant for enrollment or registration, at a public school, and individuals who receive shared time educational services from a public school. Minn. Stat. § 13.32, subd. 1(c).

2. **Education Records.** Under FERPA, the term "education records" is defined as those records that contain information directly related to a student and which are maintained by an educational agency or institution

or by a party acting for the agency or institution. 20 U.S.C. § 1232g(a)(4); Minn. R. 1205.0500, subp. 4(a).

B. **Private Data.** Generally, educational data is private data on individuals, which means the data may not be disclosed to the public and must be disclosed to the subject of the data (student) or students' parents upon request. However, there are some exceptions, as discussed in Section III. Minn. Stat. § 13.32, subd. 3.

C. **Student Health Data.** Per the MGDPA, health data concerning students, including but not limited to, data concerning immunizations, notations of special physical or mental problems and records of school nurses are educational data. Minn. Stat. § 13.32, subd. 2.

1. Student health records maintained by the school are education records or treatment records of eligible students under FERPA. These records are **not** subject to HIPPA.

D. **Student Census Data.** Student census data, including emergency information and family information are educational data. Minn. Stat. § 13.32, subd. 2.

E. **Desk Drawer Records.** Records of instructional personnel which are in the sole possession of the maker and are not accessible or revealed to any other individual except a substitute teacher, and are destroyed at the end of the school year, are not educational data. Minn. Stat. § 13.32, subd. 1(a).

F. **Law Enforcement Records.** Records of a law enforcement unit of a public educational agency or institution which are maintained apart from education data and are maintained solely for law enforcement purposes, and are not disclosed to individuals other than law enforcement officials are not educational data. Minn. Stat. § 13.32, subd. 1(a).

G. **Student Employee Records.** Records relating to a student who is employed by a public educational agency or institution which are made and maintained in the normal course of business, relate exclusively to the individual in that individual's capacity as an employee, and are not available for use for any other purpose are classified as personnel data under the MGDPA, not educational data. Minn. Stat. § 13.32, subd. 1(a).

H. **Personally Identifiable Information.** Generally, under FERPA, personally identifiable information cannot be disclosed without written consent from a parent or eligible student (18 or older). 34 C.F.R. § 99.30-31. Personally identifiable information includes a student's name, social security number,

student number, or other information linked to a specific student that would allow a person in the school community to identify the student. 34 C.F.R. § 99.3.

I. Records on Special Education Students. Records that schools maintain on special education students, including records on services provided to students under the Individuals with Disabilities Education Act (IDEA), are "education records" under FERPA. This is because these records are: (1) directly related to a student; (2) maintained by the school or a party acting for the school; and (3) not excluded from the definition of "education records."

III. DISCLOSURE OF PRIVATE EDUCATIONAL DATA

The following is a non-exhaustive list of the more common situations in which a school district may disclose educational data. The Minnesota Government Data Practices Act, FERPA, and the other data privacy related federal laws are extensive, thus one should always check the statutes before releasing or refusing to release government data.

A. Upon Request by a Parent of the Student or Student (if Over 18).

1. Under the MGDPA, a responsible authority is required to withhold data from parents or guardians, or individuals acting as parents or guardians in the absences of parents or guardians, upon request by the minor if the responsible authority determines that withholding the data would be in the best interest of the minor. However, parents may not be denied access to data that is considered an education record. Minn. R. 1205.0500, subp. 4. Therefore, the power of a responsible authority to grant the request of a minor to deny access by the parents of the minor to private data concerning the minor does *not* apply to education records. Minnesota Rules Part 1205.0500, subpart 4, specifically states that "the responsible authority shall not deny access by parents to data that is considered an 'education record,'. . . unless the minor to whom the data pertains is enrolled as a full-time student in a post-secondary educational institution or the student has attained the age of 18."

2. When a student reaches the age of 18, the parent no longer has the right to access a student's records without the student's consent, unless the student is still a dependent of the parent for tax purposes. 20 U.S.C. § 1232g(b)(1)(H).

B. Informed Consent of Parents or Student (if Over 18) is Provided.

1. The written consent form must specify the records that may be disclosed, state the purpose of the disclosure, and identify the party or class of parties to whom the disclosure may be made.

2. A parent or guardian of a student my designate an individual to participate in a school conference involving the child of the parent or guardian. Minn. Stat. § 13.32, subd. 10a(a). Prior written consent from the parent or guardian must be provided to the school and may be withdrawn by the parent or guardian, in writing, at any time. *Id.*

C. Pursuant to a Valid Court Order.

D. Pursuant to a Statute Specifically Authorizing Access to Private Data.

E. Data is Properly Designated as Directory Information.

1. Information which a school district properly designates as **"directory information" constitutes public data** on individuals. Such information will be identified by school district policy. Under FERPA, "directory information" includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student. 20 U.S.C. § 1232g(a)(5)(A).

2. School Districts must provide public notice of the categories of information which it has designated as directory information and allow a reasonable period of time after notice has been given for a parent to inform the school district that any or all of the information designated should not be released without the parent's prior consent. 20 U.S.C. § 1232g(a)(5)(B).

3. Data concerning parents of students are private data on individuals but may be treated as directory information if the same procedures are used by a school district to designate student data as directory information. Minn. Stat. § 13.32, subd. 2(c).

F. A Health or Safety Emergency Exists.

If a true emergency exists and disclosure is necessary to protect the health

and safety of the student or other individuals, a school district may disclose educational data. *See* Minn. Stat. § 13.32, subd. 3(d); 34 C.F.R. § 99.36. The Minnesota Department of Administration, which is charged with interpreting the MGDPA, has opined that the health or safety emergency exception applies very narrowly.

G. To Proper Health Authorities.

Educational data may be disclosed to appropriate health authorities to the extent necessary to administer immunization programs and for bona fide epidemiological investigations which the Health Department Commissioner determines are necessary to prevent disease or disability.

H. Pursuant to FERPA.

Federal regulations identify numerous scenarios where prior consent is not required to disclose information, including, but not limited to, instances where the following conditions are met:

1. **Legitimate Educational Interest. (34 C.F.R. § 99.31(a)(1)).** Disclosure to other school officials and teachers with a *legitimate educational interest* in the information. The MGDPA also clarifies that within a governmental agency or entity, private information may be accessed by persons whose job duties *require* such access. Minn. Rules, Part 1205.0400, subp. 2. This can cover volunteers, consultants, and agents of a school.

2. **Lawfully Issued Subpoena. (34 C.F.R. § 99.31(a)(9)).** School districts may disclose educational data in response to a lawfully issued subpoena, but the district must first give the parents and student notice that it has received a subpoena and intends to comply with it. This theoretically provides the parent an opportunity to ask a judge to "quash" the subpoena.

3. **Victim of Violent Crime. (34 C.F.R. § 99.31(a)(13)).** Disclosure to the victim of a crime of violence about the results of a disciplinary action taken against a student perpetrator.

4. **Transfer of Records to New School. (34 C.F.R. § 99.31(a)(2)).** Disclosure to school officials in another school in which the student seeks to enroll.

I. To the Juvenile Justice System in Limited Cases.

School districts may disclose educational data to appropriate authorities, as provided in United States Code, Title 20, Section 1232g(b)(1)(E)(ii), if the data concern the juvenile justice system and the ability of the system to effectively serve, prior to adjudication, the student whose records are released; and provided that the authorities to whom the data are released submit a written request for the data that certifies that the data will not be disclosed to any other person except as authorized by law without the written consent of the parent of the student and the request and a record of the release are maintained in the student's file. Minn. Stat. § 13.32, subd. 3(i).

1. **To protect the safety of a student or others.** A school district may also disclose educational data to the juvenile justice system if information about the behavior of a student who poses a risk of harm is reasonably necessary to protect the health or safety of the student or other individuals. Minn. Stat. § 13.32, subd. 3(l). Thus, educational institutions clearly have the legal authority to provide information to the juvenile justice system about juveniles who threaten the safety of themselves or others connected with the school.

2. **Reporting serious crimes of disabled students.** IDEA states that school districts may exercise their responsibilities under state and federal law to report a crime committed by a disabled student to law enforcement and judicial authorities. *See* 20 U.S.C. § 1415(k)(6). IDEA further states that a school district reporting such a crime *must* ensure that copies of the special education and disciplinary records of the disabled student are transmitted "for consideration by the appropriate authorities to whom it reports the crime." *Id.*

3. **Possession of a firearm.** In compliance with the Federal Gun-Free Schools Act (20 U.S.C. 7151), Minnesota law requires that school districts have in place a policy which refers to law enforcement any pupil who brings a firearm to school unlawfully. *See* Minn. Stat. § 121A.06. This explicit requirement in the law permits a school district to report a student to law enforcement notwithstanding any provision of the MGDPA.

J. To School Volunteers.

Volunteers who are determined to have a legitimate educational interest in the data and who are conducting activities and events sponsored by or endorsed by the educational agency or institution for students or former student. Minn. Stat. § 13.32, subd 3(j).

K. To the Minnesota Department of Education Commissioner.

Educational data may be disclosed to the MDE Commissioner for purposes of an assessment or an investigation of a maltreatment of minors report. Minn. Stat. § 13.32, subd. 3(n).

L. To Military Recruiters.

A secondary school must release limited student data to military recruiting officers including the names, addresses, and home telephone numbers of students in grades 11 and 12. Minn. Stat. § 13.32, subd. 5(a).

1. Parents and students must be provided with notice of the right to refuse release of this data to military recruiting officers. Minn. Stat. § 13.32, subd. 5(a).

2. Use of this data is limited by statute. *See* Minn. Stat. § 13.32, subd. 5(a).

V. COLLECTING PRIVATE DATA

A. Tennessen Warning.

Individuals who are asked to supply private or confidential data concerning themselves must be informed, prior to the collection of the data, of the following:

1. the purpose and intended use of the requested data within the collecting government entity;

2. whether the individual may refuse or is legally required to supply the requested data;

3. any known consequence arising from supplying or refusing to supply private or confidential data; and

4. the identity of other persons or entities authorized by state or federal law to receive the data.

Minn. Stat. § 13.04, subd. 2. This notice is commonly referred to as a "Tennessen warning," named after Senator Robert Tennessen, the author of the original data privacy law in Minnesota.

Therefore, whenever a school district collects private data on individuals, including any student, a Tennessen warning should be provided to the student *prior* to any collection of data.

V. RESPONDING TO DATA REQUESTS

A. Maintenance of Government Records.

Easily Accessible. Pursuant to the Minnesota Government Data Practices Act ("MGDPA"), data must be easily accessible. This includes government records. The MGDPA provides that "[t]he responsible authority in every government entity shall keep records containing government data in such an arrangement and condition as to make them easily accessible for convenient use." Minn. Stat. § 13.03, subd. 1.

B. The Data Subject.

1. **Rights of the data subject**. An individual—and, in the case of a minor or incapacitated person, the parent or guardian of an individual, or an individual acting as a parent or guardian in the absence of a parent or guardian—has the right to be informed whether he/she is the subject of stored data on individuals and whether the data are classified as public, private or confidential. The subject of the data also has the right to be shown the stored public or private data and to be informed of its meaning, upon request. *See* Minn. Stat. § 13.02, subd. 8; 13.04, subd. 3. Upon request, the individual subject has a right to receive copies of the data from the responsible authority.

    a. Compliance with such a request is to be **immediate if possible**, although it may be extended up to **ten days**, excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible. *See* Minn. Stat. § 13.04, subd. 3.

    b. Typically, after an individual has been shown the private data and informed of its meaning, the data need not be disclosed to that individual for six months thereafter unless a dispute or action pursuant to this section is pending or additional data on the individual has been collected or created. *See* Minn. Stat. § 13.04, subd. 3. However, the MGDPA does not limit the frequency in which a parent or guardian, or student who has reached the age of majority, can inspect the educational records pertaining to a child with a disability. Minn. Stat. § 13.32, subd. 10.

c. Data maintained in a computer storage medium must be provided in an electronic form if so requested. However, there is no requirement that data be provided in a format or program different from the format or program in which it is maintained by the government entity. Minn. Stat. § 13.03, subd. 3(e). *See* Department of Administration Op. 01-027.

d. Requests must be made to the responsible authority. *See Scheffler v. City of Anoka*, 890 N.W.2d 437 (Minn. Ct. App. 2017) (holding that a person seeking data from a government entity must make his request to the government entity's specified responsible authority or designee before claiming violations of the MGDPA for failure to provide data or failure to provide a reason for denial).

e. No fee may be charged to search for or retrieve educational records. Minn. Stat. § 13.32, subd. 10.

g. If a school district receives a request for copies of the educational records of a child with a disability, the school district may only charge a fee that reflects the costs of reproducing the records, except when to do so would impair the ability of the child's parent or guardian, or the child who has reached the age of majority, to exercise their right to inspect and review those records.

2. **Student's access to private data.** A **s**tudent does **not** have the right to access financial records and statements of the student's parents. Minn. Stat. § 13.32, subd. 4.

C. Accessing Public Data.

1. **Timeline.** When an individual requests access to public data, the entity must reply within a reasonable time. Minn. Stat. § 13.03, subd. 1 & 3(c); Minn. R. 1205.0300. The definition of "reasonable time" may vary on a case by case basis depending on the complexity of the data request. However, a public entity should try to fulfill the request as soon as reasonably possible.

a. The Department of Administration has repeatedly addressed the "reasonableness" requirement in its advisory opinions. When compliance has been delayed due to the complexity of finding voluminous data, the Department has most commonly relied upon the language regarding the entity failing to maintain the data in a

manner that is easily accessible for convenient use to facilitate timely access.

b. The main theme of the opinions finding that the entity did not appropriately comply can be stated as follows:

i. The entity should respond promptly with a time estimate as to when the data will be ready;

ii. The entity should give the individual requesting the data the opportunity to review data when some, but not all, is ready; and

iii. The time for responding must reasonably relate to the amount of data requested.

Practice tip: Communicate regularly with the person making the request. Give updates as to your progress regarding the request. Document the communications. Forward information as it becomes available, upon receipt of payment if copies are requested.

2. **Generally, requests for identification and justification are prohibited.** Except where specifically authorized by statute, a public entity may not require persons to identify themselves, state a reason for or justify a request for access to public data. *See* Minn. Stat. § 13.05, subd. 12.

a. Identifying data or clarifying information can only be requested in order to facilitate access to the requested data.

b. This provision does not limit a public entity's power to require identification as a precondition to examining private data.

3. **Inspection of data.** If the person requesting access only wants to inspect the data, no fee can be charged. This is true even if data has to be redacted to remove private data from the public data. Minn. Stat. § 13.03, subd. 3(a).

"Inspection" includes, but is not limited to, the visual inspection of paper and similar types of government data. Inspection does not include printing copies by the government entity, unless printing a copy is the only method to provide for inspection of the data. Minn. Stat. § 13.03, subd. 3(b).

In the case of data stored in electronic form and made available in electronic form on a remote access basis to the public by the government entity, inspection includes remote access to the data by the public and the ability to print copies of or download the data on the public's own

computer equipment. *Id.* A government entity may charge a fee for remote access to data where either the data or the access is enhanced at the request of the person seeking access. *Id.*

4. **Copies of data.** The responsible authority may charge a reasonable fee for the actual costs of providing copies of public data. These charges can include the following:

   a. The cost of materials, including paper, used to provide the copies;

   b. The cost of labor required to prepare the copies or electronically transmit records;

   c. Any schedule of standard copying charges as established by the agency in its normal course of operation;

   d. Any special costs necessary to produce such copies from machine based record keeping systems including, but not limited to, computers and microfilm systems; and

   e. Mailing costs.

   f. For 100 or fewer pages of black and white, letter or legal size paper copies the entity may not charge the actual cost, *but instead* may charge no more than 25 cents for each page copied. (*Not* labor costs plus photocopying).

   See Minn. Stat. § 13.03, subd. 3.

D. Accessing Private Data on Individuals.

1. **Consent.** If the individual subject of data gives prior informed consent, the responsible authority may make access to the private data available to members of the public. *See* Minn. Stat. § 13.05, subd. 4.

2. **Court order.** A party seeking access to government data may bring before a presiding judicial officer, arbitrator, or administrative law judge an action to compel discovery. *See* Minn. Stat. § 13.03, subd. 6.

3. **Other situations allowed by statute.** Specific state and federal statutes authorize the disclosure of private or confidential data in specific circumstances.

V. DATA SECURITY & ELECTRONICALLY STORED DATA

While *data privacy* relates to the collection and use of personal information of both students and staff, *data security* relates to the protections in place to prevent unauthorized access to or acquisition of data. Though a distinct concept, data security for schools is an essential component of keeping private data private.

A. Data Security Risks Faced by Schools.

1. **Theft.** Schools have and will continue to face deliberate attacks on systems and individuals with the intent of accessing sensitive data.

2. **Loss.** Data may also be compromised if it is inadvertently exposed due to loss of technology or media.

3. **Neglect.** Insufficiently protected data is also at risk,

4. **Insecure practices.** If a school's practices pertaining to collecting, storing sending, encrypting, finding and removing data are insufficient, the data is also vulnerable.

B. Safeguarding Data.

1. **Data governance plan.** To protect against a data breach, school districts should develop a governance plan. This includes having and maintaining a clear understanding of the following:

    a. What type of protected data is being collected?

    b. How is the data being used?

    c. Where is the data stored?

    d. Who has access to the data?

    e. Who can share the data?

    f. Where is the data being transmitted?

    e. How is the data protected as it moves through the system?

2. **Policies and procedures.** School districts should have in place specific policies and procedures that focus on data security including an Incident Response Plan to contain and remedy any breach of data and an Acceptable Use policy that governs all online activity. Additionally,

school districts should engage in comprehensive employee training on data privacy laws, known or suspected data security risks, common errors that lead to data breaches, school district policies and the consequence(s) of violating those policies.

3. **Document destruction.** Under document destruction regulations implemented pursuant to the IDEA, personally identifiable information belonging to a child must be destroyed at the request of the parent when such information is identified by the school district as no longer needed to provide educational services to the child. 34 C.F.R. §§ 300.624(b), 303.416(b). However, a permanent record of a student's name, address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed may be maintained without time limitation. 34 C.F.R. §§ 300.624(b). Of course, school districts should adhere to any applicable records retention policy.

4. **Protect electronically stored data with secure user IDs and passwords.** Access to sensitive data should be limited to only those individuals who require access to the data to do their jobs. Individuals who are provided with access should be required to use secure passwords when accessing the data.

5. **Encryption.** Private data stored on servers or on mobile devices like laptops or smart phones as well as data that are transmitted via unsecure email or over public networks should be encrypted to ensure protection.

C. Data Breaches.

The MGDPA requires that individuals whose data has been improperly accessed are informed in writing and that an investigation report is prepared. Minn. Stat. § 13.055.

Practice tip: Consult with legal counsel before sending notices to anyone admitting to the improper disclosure of data. A legal and factual analysis should take place first. The notice can be used as an admission against the government entity in litigation.

VI. LIABILITY FOR IMPROPER DISSEMINATION OF GOVERNMENT DATA

A. Damages. Under Section 13.08, subdivision 1, a public entity is liable to a person who suffers any damages due to a violation of the MGDPA; thus, an individual may bring an action against a school district to compel compliance with the MGDPA and recover the cost of doing so. Minn. Stat. § 13.08, subd. 4. That liability covers damages sustained, plus costs and reasonable attorneys' fees. *See Navarre*, 652 N.W.2d 9. If a court issues an order requiring a county to comply with its obligations under the MGDPA, it may also impose a civil penalty of up to $1,000. Minn. Stat. § 13.08, subd. 4(a).

A "willful violation" can result in punitive damages of from $1,000.00 to $15,000.00 for each violation. Minn. Stat. § 13.08, subd. 1. An individual may bring an action against the entity to compel compliance with the MGDPA and recover the cost of doing so.

B. Individual Consequences. Any person who willfully violates the MGDPA or whose conduct constitutes the knowing unauthorized acquisition of not public data is guilty of a criminal misdemeanor. A willful violation of the MGDPA by any public employee also constitutes just cause for suspension without pay or dismissal of the public employee. Minn. Stat. § 13.09.

1. As set forth in Section 13.055, subdivision 1, "unauthorized acquisition" means that a person has obtained, accessed, or viewed government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernment purposes.

C. Common Law Claims. Minnesota recognizes a common law action for invasion of privacy. *See Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998). Publication of private facts is an invasion of privacy when one gives publicity to a matter concerning the private life of another if the matter publicized is of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public. *Id.*

VII. CONSIDERATIONS FOR SPECIAL EDUCATION PERSONNEL

A. Discussing Student Information. Teachers and paraprofessionals can discuss student information and pass that information along to other school officials if the school has determined that each recipient of the information has a legitimate educational interest in knowing or accessing the student's private educational information or if the parent or eligible student has provided consent.

B. Preventing Unintentional Disclosure of Private Education Data. The Minnesota Department of Education has advised that, as a best practice, school professionals who have a legitimate educational interest in sharing private student educational data should not discuss student information in community areas such as hallways, lounges, and parking lots in order to prevent the unauthorized disclosure of private student data. Furthermore, privacy of information can often not be guaranteed when using emailing and faxing as communication methods. School staff should carefully weigh the risks of the communication methods they use. Overall, school staff should refrain from discussing personal student information in public areas and be aware of the security risks of the communication methods used when sharing private student data, such as in emails or faxes.

C. **Social Media.** School staff should not post anything on social media (or anywhere else) concerning special education students, including pictures and/or comments which identify the student as a special education student. *See* Dept. of Administration Advisory Op. 04-024 (school district did not comply with the MGDPA in publishing a photograph of a student in the school's yearbook on a page that identified the student as receiving special education services). School staff should also refrain from discussing any the terms of a student's IEP, the services a student receives, or any other particulars of a student's special education status.

D. **Use Discretion.** As a general rule, school staff and school administrators should not put anything in writing that they would not want read out loud in court. It is possible that every social media post, email, handwritten note, text and/or instant message may become part of the record in administrative proceedings and/or litigation.