299C.41 E-CHARGING.

Subdivision 1. **Definitions.** (a) The definitions in this subdivision apply to this section.

(b) "Auditing data" means data in e-charging that document:

(1) who took a particular action;

(2) when the action took place;

(3) the Internet Protocol address of the computer used to take the action;

(4) the identification number of the organization employing the individual taking action;

(5) what action was taken;

(6) the unique identification for the document against which the action was taken;

(7) the purpose for taking the action;

(8) the date and time the request was received by the e-charging system; and

(9) the identification number of the system from which the request originated.

(c) "Credentialed individual" means an individual who has provided credentialing data to a government entity or a court and has been authorized to use e-charging.

(d) "Credentialing data" means data in e-charging that document for an individual who is or was authorized to use e-charging:

(1) user identification;

(2) password; and

(3) jurisdiction identification.

For law enforcement officers, credentialing data also includes a biometric identifier. For notaries public, credentialing data also includes an e-notary digital certificate.

(e) "E-charging" means a service operated by the Bureau of Criminal Apprehension to provide communication and work flow tools for law enforcement agencies, prosecutors, and the courts to use in apprehending, prosecuting, or adjudicating a person for an alleged delinquent act or an alleged criminal or petty misdemeanor offense under a law of this state or its political subdivisions. The e-charging service also includes communication and work flow tools provided for the use of the Department of Public Safety in its administration of the license revocation provisions under sections 169A.50 to 169A.53 or 171.177.

(f) "Government entity" has the meaning given in section 13.02, subdivision 7a.

(g) "Individual" has the meaning given in section 13.02, subdivision 8.

(h) "Work flow and routing data" means data in e-charging that document:

(1) the assignment or reassignment of a document to a person or place;

(2) any deadline for the action on the assignment; and

(3) validation that the needed action has been completed.

Subd. 2. **Data classification.** (a) Credentialing data held by a government entity are classified as private data on individuals as defined in section 13.02, subdivision 12, or nonpublic data as defined in section 13.02, subdivision 9.

(b) Auditing data and work flow and routing data maintained by the Bureau of Criminal Apprehension are classified as confidential data on individuals as defined in section 13.02, subdivision 3, or protected nonpublic data as defined in section 13.02, subdivision 13, until the investigation is inactive as defined in section 13.82, subdivision 7. Once the investigation is inactive, and the recipient of the data authorizes release to the data subject, the auditing data and work flow and routing data maintained by the Bureau of Criminal Apprehension are classified as private data on individuals as defined in section 13.02, subdivision 12, or nonpublic data as defined in section 13.02, subdivision 9. The same data maintained by any other government entity are classified as provided by other law.

Subd. 3. **Data sharing authorized.** (a) Auditing data, work flow and routing data, or credentialing data must be disclosed to a credentialed individual to resolve issues about the integrity of data at issue in a pending criminal matter. No use outside the pending criminal matter is authorized and no recipient can redisclose the data that are received. To the extent that court rules make the data accessible to the public, they are accessible in the court records.

(b) Auditing, work flow and routing data, or credentialing data must be disclosed to a defendant in a pending criminal matter when the data are relevant to the individual's defense as defined in the Rules of Criminal Procedure. Relevance must be determined by the court using the standard set in Rules of Criminal Procedure, rule 9.01, subdivision 2(1). If the data are found to be relevant, the court must issue an order directing disclosure and send it to the Bureau of Criminal Apprehension. Disclosure cannot be made unless the court's order provides the full name and date of birth of the defendant, the law enforcement agency number, the law enforcement case number connected to the charge, the specific data to be disclosed, and that the recipient must not redisclose the data. The bureau shall provide the data to the defendant's attorney and the prosecutor. The data may not be used outside the pending criminal matter and a recipient may not redisclose the data that are received. To the extent that court rules make the data accessible to the public, they are accessible in the court records.

(c) Auditing data, work flow and routing data, or credentialing data may be disclosed to an employee of a government entity or court who has been accused of inappropriate access to, or use of data in, e-charging and to the employee's employer. The data may not be used outside the pending employee disciplining case and a recipient may not redisclose the data that are received. To the extent that section 13.43 or court rules require the disclosure of the data as part of the final disposition of discipline against an employee, the data are public.

(d) Auditing data, work flow and routing data, or credentialing data may be disclosed as part of a criminal or civil matter against a person for unauthorized access to, or use of data in, e-charging. The data may not be used outside the civil or criminal case and a recipient may not redisclose the data that are received. To the extent that the rules of public access to records of the judicial branch make the data accessible to the public, they are accessible in the court records.

Subd. 4. [Repealed, 2008 c 299 s 28]

History: *2008 c 242 s 3; 2008 c 299 s 15; 2011 c 91 s 1; 2017 c 83 art 3 s 18*