

COPY

DATA EXCHANGE AGREEMENT

BETWEEN THE

SOCIAL SECURITY ADMINISTRATION

AND THE

WISCONSIN DEPARTMENT OF WORKFORCE DEVELOPMENT

PROVIDING FOR THE

RELEASE OF SPECIFIED DATA

RELATING TO THE

**TEMPORARY ASSISTANCE TO NEEDY FAMILIES
(AKA W-2 IN WISCONSIN),**

CHILD SUPPORT,

FOOD STAMP, and

**MEDICAID
(AKA MEDICAL ASSISTANCE IN WISCONSIN)**

PROGRAMS

February, 1999

I. PARTIES TO THIS AGREEMENT

The parties to this agreement are the Social Security Administration (hereinafter SSA) and the Wisconsin Department of Workforce Development (hereinafter DWD) and one of its divisions, the Division of Economic Support (hereinafter DES).

II. TERM

This agreement shall remain in effect until the parties agree to amend or terminate it, unless sooner suspended or amended under the terms and conditions set forth in Articles XIII and XVII. This agreement will be effective immediately with the signing by all parties to this agreement and will be effective for a period of five years.

III. DEFINITIONS

- A. SSA is the federal agency charged with the responsibility of enforcing obligations under section 1106 of the Social Security Act (42 USC 1306).
- B. DWD is the state agency of the State of Wisconsin charged with the responsibility for enforcing the provisions of:
 - 1. The TANF (W-2) program under a state plan approved under Title IV-A of the Social Security Act;
 - 2. The Medicaid (aka Medical Assistance or MA) program under a state plan approved under Title XIX of the Social Security Act;¹
 - 3. The Food Stamp (FS) program and the Food Stamp Employment and Training (FSET) Program under the Food Stamp Act of 1977, as amended; and,
 - 4. The Child Support (CS) program under a state plan approved under Title IV-D of the Social Security Act.
- C. DWD data stewards are the individuals designated by the administrator, Division of Economic Support to:
 - 1. Coordinate and administer DWD/SSA agreement amendments;
 - 2. Coordinate with SSA to oversee the procedures for designating SSA staff to access CARES and KIDS data; and,
 - 3. Coordinate data sharing requests between DWD and SSA in accordance with this agreement. These persons will be the sole contact in any communications between DWD and SSA regarding data exchange. Any exceptions must be agreed upon by the DWD data stewards and SSA data exchange coordinators.

¹ Note: Medicaid or Medical Assistance (MA) is administered in Wisconsin by the Department of Health and Family Services (DHFS). When DWD was created in 1996 by state statute, TANF (W-2), FS and CS were placed in DWD. MA was placed in DHFS under the same state statute. By agreement with DHFS, the CARES system retains Medicaid functionality. DHFS will receive a courtesy copy of this agreement for reference.

- D. SSA data exchange coordinator is the person designated by the SSA administrator to coordinate data sharing requests between SSA and DHSS in accordance with this agreement.
- E. The names of the SSA data exchange coordinator and the DWD data stewards are specified in Addendum A. Addendum A shall be updated as required during the period this agreement is in force.
- F. CARES is the Client Assistance for Re-employment and Economic Assistance data system. This system is used by DWD and DHFS to administer the TANF (W-2), Medical Assistance, and Food Stamp programs.
- G. KIDS is the Kids Information Data System. This system is used by DWD to administer the Child Support Enforcement program.

IV. PURPOSE

The purpose of this agreement is to establish procedures for the release of TANF (W-2) payment data, child support payment information and Food Stamp benefit data by DWD to SSA. The information shall be used for the following purposes:

- A. To make accurate determinations of entitlement to Social Security Act Titles II and XVI benefits by SSA, and to accurately determine payments.
- B. To establish age, citizenship, and identity for the assignment of Social Security numbers.
- C. To achieve cost savings to DWD and SSA from the data sharing described in this agreement will be realized through:
 - 1. More timely cessation of W-2, FS, MA and/or General Relief grants or adjustments to grant levels.
 - 2. Reduced overpayments of benefits and associated recovery of overpaid monies.
- D. Addenda B and C to this agreement identify the specific CARES and KIDS screens, respectively, which SSA shall have access under the terms of this agreement. Addenda B and C may be updated as necessary while this agreement is in force.

V. INFORMATION TO BE PROVIDED AND PURPOSES

The specific information which will be requested by SSA pursuant to this agreement, and the purposes for which such requests will be made; pursuant to section 1106 of the Social Security Act (42 USC 1306), the Privacy Act (5 USC 552a), and the Freedom of Information Act (5 USC 552); are as follows:

- A. TANF (W-2) payment data;
- B. Food Stamp benefit data; and,
- C. Child Support payment data.

W-2, FS, and MA are provided via the CARES queries as enumerated in Addendum B.

VI. AUTHORITY TO QUERY DATA AND TO REQUEST SPECIFIC DATA FILES

- A.** SSA will provide an up-to-date listing of line staff with responsibilities for monitoring payment systems. The same list will be used for KIDS and CARES access. DWD/DES will supply DES-10 forms for CARES/KIDS access. Properly completed DES-10 forms are required for each SSA staff person requiring access.
- B.** Under terms of this agreement between SSA and DWD, DWD agrees to safeguard all information submitted by the employees of SSA as part of the state's computer access registration requirements. The information submitted to DWD will be used only for the purposes of facilitating assignment of a state provided personal identification number for SSA employees who will be accessing the state system. It is further agreed that all information collected in fulfillment of the registration requirement will be protected in accordance with applicable federal, state and or local privacy regulations. Misuse of the collected information may lead to the termination of this agreement.

VII. METHOD AND PROCEDURES OF SSA REQUESTS

SSA will access DWD via the Network Data Mover (NDM) link between SSA and the state computer (Info-Tech in the Wisconsin Department of Administration). No changes will be done to the type and/or format of the CARES queries. SSA employees authorized to access these queries will obtain the information obtained in these queries in the same manner as other state authorized workers using these queries.

DWD agrees to:

- A.** Provide SSA with the technical requirements so that SSA field offices can access the queries identified in Section V.
- B.** Use existing DWD procedures for obtaining Logon ID and passwords required for SSA's CARES and KIDS access.
- C.** Provide training for educating SSA employees on procedures to access and use CARES and KIDS systems and data.
- D.** Provide training materials for accessing CARES and KIDS data. DWD will provide, based on need, one train-the-trainer session per year and desk top aids to SSA while this agreement is in force.
- E.** Safeguard all information submitted by employees of the SSA as part of the state's computer access registration requirements. It is further agreed that all information collected in fulfillment of the registration requirement will be protected in accordance with applicable Federal, State, and/or local privacy regulations. DWD will use any personal identifying information (e.g., name, social security number and related data) solely for the purpose of registering employees for online access to State records. Access to the data will be restricted to only those authorized employees and officials who need it to perform their official duties in connection with the intended use of the data. Misuse of the collected information may lead to the termination of this agreement.

SSA Agrees to:

- A. Limit SSA field office access to the queries identified in Section V to SSA employees who receive Logon ID and passwords.
- B. In accordance with SSA regulations and operating instructions, access the queries identified in Section V only when that information is needed by SSA to process claims for benefits and related programs.
- C. Monitor SSA employee use of the queries to ensure that data obtained from the queries is used only for SSA benefit claims and related programs.
- D. SSA will retain the identifiable records received from DWD only for the period of time required for any processing related to the electronic query and will then destroy the records. The records must be destroyed unless the information has to be retained in the individual's file folders in order to meet evidentiary requirements. In the latter instance, SSA will retire any identifiable records in accordance with applicable Federal Records Retention Schedule (44 U.S.C. 3303a).

VIII. REIMBURSEMENT FOR COSTS INCURRED BY DWD IN PROVIDING INFORMATION

Reimbursements will be made by SSA to DWD for all reasonable costs incurred by DWD in providing information pursuant to this agreement. The amounts, type of billing and time frame for such reimbursements are to be mutually agreed upon in advance of providing such services.

SSA shall not be responsible for any financial loss incurred by DWD, whether directly or indirectly, through the use of any data furnished pursuant to this agreement. DWD shall not be responsible for any financial loss or other liability incurred by SSA, whether directly or indirectly, through or by the use of any data furnished to SSA pursuant to this agreement.

Neither party agrees to indemnify the other for any liability that the other party incurs as a result of use of any data under this agreement.

IX. PROTECTION OF CONFIDENTIALITY: PROTECTION AGAINST UNAUTHORIZED ACCESS OR DISCLOSURE

SSA agrees to comply with the following measures to protect the confidentiality of any information provided under this agreement and to protect such information against unauthorized access or disclosure.

- A. The information subject to this agreement shall be used only to the extent necessary to assist in the valid administrative needs of SSA and shall be disclosed only for the purposes as defined in this agreement;
- B. SSA will not use the information for any purposes not specifically authorized under this agreement;
- C. The information shall be stored in a place physically secure from access by unauthorized persons in conformance with the DWD Bureau of Information and Technology Services' (BITS) security system rules;

- D. Information in electronic format shall be processed in such a way that unauthorized persons cannot retrieve the information by means of computer, remote terminal or other means;
- E. Only authorized personnel shall be given access to online files; and,
- F. SSA personnel that have access to the data identified in Section V agree to the confidentiality of this data as set forth in applicable state statutes (particularly Chapter 49 Wisconsin statutes) and DWD administrative rules. See Addendum D for legal citations.

X. CONFIDENTIALITY ACKNOWLEDGMENT

The SSA regional commissioner, on behalf of SSA, attests that all personnel with access to the information covered by this agreement will adhere to the policies and procedures of DWD regarding confidentiality.

XI. DISCLOSURE OF INFORMATION

In accordance with this agreement and in compliance with federal and state law; SSA will not disclose any information obtained through this agreement without prior written approval from DWD.

XII. COMPLIANCE: ON SITE INSPECTION

Pursuant to Sec. 1137(a)(5B) of the Deficit Reduction Act of 1984, SSA agrees to permit authorized personnel of DWD to make on-site inspections to ensure adherence to federal statutes and regulations applicable to this agreement. DWD agrees to notify the SSA data exchange coordinator at least one full work day in advance of any inspection.

XIII. SUSPENSION OF THIS AGREEMENT BY DWD FOR DEFAULT

Notwithstanding the terms of this agreement as specified in Article II, DWD shall suspend this agreement in accordance with state and federal requirements, or within 45 days if no state and/or federal requirements apply, in the event of any of the following:

- A. SSA uses any information provided under this agreement for a purpose not specified herein;
- B. SSA fails to protect the confidentiality of information provided and/or to protect such information against unauthorized access or disclosure as provided by Article IX;
- C. SSA violates Article X of this agreement;
- D. SSA fails to abide by the disclosure provisions of Article XI; and,
- E. SSA fails to allow on-site inspections authorized by Article XII.

XIV. CURE DEFAULT TO REINSTATE AGREEMENT

Any suspension of this agreement for any one or more of the reasons specified in Article XIII shall last until DWD is satisfied that SSA is again in compliance with the terms and conditions of this agreement, or until a new agreement between DWD and SSA is

reached. If a new agreement is required, all drafting and associated work will be the responsibility of the DWD data stewards.

XV. SUSPENSION OR TERMINATION OF THIS AGREEMENT BY SSA

Upon 45 days written notice to DWD, SSA may suspend or terminate this agreement without cause.

XVI. SURVIVAL

The confidentiality and disclosure requirements in Articles IX., X. and XI. of this agreement survive the termination, for whatever reason, of the agreement itself, subject to applicable state and federal laws.

XVII. AMENDMENT OF THIS AGREEMENT

All or part of this agreement may be amended at any time by written amendment signed by the administrator of SSA and the secretary or deputy secretary of DWD. It is acknowledged that this agreement is subject to federal and state law, both of which are subject to change. If either applicable state or federal law changes, this agreement will be considered immediately modified in accordance with each such change, without notice or written amendment.

This provision for automatic amendment will not apply where one party provides written notice to the other party of the federal or state law change that it desires to challenge such change or that it believes that such change will render its performance under this agreement illegal, impractical or impossible. upon the giving of the required notice, SSA and DWD agree to negotiate as to the effect the particular federal or state law change will have on the future implementation and continuation of this agreement.

XVIII. YEAR 2000 (Y2K) AFFIRMATION

DWD has made changes to properly process Year 2000 data and affirms that calendar year information for all dates in our records will be a full four-digit field, including the millennium and century. Should there be calendar year information expressed as a two digit field, DWD/DES must tell SSA how to determine that year's millennium and century. By signing this agreement, SSA assures DWD that SSA computer systems will be Y2K compliant by December 31, 1999, thus ensuring the integrity of DWD systems.

IXX. SIGNATORIES TO THIS AGREEMENT

Each party agrees to give the other party written notice within thirty (30) days after becoming aware of any state or federal law change which may impact upon the performance of either party under this agreement.

Approval of this Agreement is given by the:


For the Social Security Administration:



James F. Martin
Regional Commissioner

3/1/99
Date

For the Wisconsin Department of Workforce Development:



Orlando Cantó
Deputy Secretary

2/23/99
Date

ADDENDUM A
TO THE
DATA EXCHANGE AGREEMENT
BETWEEN
SSA AND DWD
FOR THE RELEASE OF SPECIFIED DATA RELATING
TO THE
TANF (W-2), CHILD SUPPORT, FOOD STAMP, AND MEDICAID
PROGRAMS

SSA DATA COORDINATORS AND DWD DATA STEWARDS

1. The Administrator, Social Security Administration hereby designates Ron J. Konkol to serve as the SSA data exchange coordinator as specified in Article III. D. of this agreement.

2. DWD, Division of Economic Support designates Peter H. Van Ness and Todd Kummer to serve as the DWD/DES data stewards for the CARES and KIDS systems, respectively, as specified in Article III. E. of this agreement.

ADDENDUM B
TO THE
DATA EXCHANGE AGREEMENT
BETWEEN
SSA AND DWD
FOR THE RELEASE OF SPECIFIED DATA RELATING
TO THE
TANF (W-2), CHILD SUPPORT, FOOD STAMP, AND MEDICAID
PROGRAMS

The following CARES screens are authorized for SSA query access:

ANID	AFEI	AFUI	AFSE
ACCH	AALA	AAVA	AARP
AAPP	AABA	ACCH	

ALL AE QUERIES WHICH INCLUDE:

AQCS	AQCM	AQAS	AQAM	AQAE
AQIP	AQIE	AQIN	AQCW	AQOE
AQOI	ACDF	AQCT	AQCP	AQCX
AQWI				

SSA will also have change access to the CMMM screen to communicate with economic support workers about specific cases.

**ADDENDUM C
TO THE
DATA EXCHANGE AGREEMENT
BETWEEN
SSA AND DWD
FOR THE RELEASE OF SPECIFIED DATA RELATING
TO THE
TANF (W-2), CHILD SUPPORT, FOOD STAMP, AND MEDICAID PROGRAMS**

SSA staff will receive "general inquiry" access to the KIDS system.

ADDENDUM D
TO THE
DATA EXCHANGE AGREEMENT
BETWEEN
SSA AND DWD
FOR THE RELEASE OF SPECIFIED DATA RELATING
TO THE
TANF (W-2), CHILD SUPPORT, FOOD STAMP, AND MEDICAID PROGRAMS

ADDITIONAL LEGAL CITATIONS

Social Security Act

TITLE II

- 202 (42 U.S.C. 402) Old Age Benefits
- 203 (42 U.S.C. 403) Reduction of Insurance Benefits
- 205 (42 U.S.C. 405) Evidence, Procedure and Certification
- 216 (42 U.S.C. 416) Other Definitions (Relationship)
- 216 (42 U.S.C. 416)(i)(1) Disability, Period of Disability

TITLE XVI

- 1106 (42 U.S.C. 1306) Disclosure of Information in Possession of an Agency
- 1611 (42 U.S.C. 1382)(a)(1) and 1611 (a)(2) Definition of Eligible Individual
- 1611 (42 U.S.C. 1382)(b)(1)(2) Amounts of Benefits
- 1612 (42 U.S.C. 1382)(a) Meaning of Income
- 1613 (42 U.S.C. 1382)(b) Meaning Resources

Chapter 19 Wisconsin Statutes

- 19.36 Limitations on Access and Withholding

Chapter 49 Wisconsin Statutes Confidentiality Provisions

- 49.32 (9) Monthly Report of Recipients
- 49.32 (10) Release of Information to Law Enforcement Officers
- 49.32 (10m) Release of Addressess of Recipients Involved in Legal Proceedings
- 49.81 Public Assistance Recipients' Bill of Rights
- 49.83 Limitation on Giving Information

Chapter 943 Wisconsin Statutes

- 943.70 Computer Crimes

PROGRAMS IN CHAPTER 49 WISCONSIN STATUTES

s. 49.124 Food Stamp Administration	ss. 49.141-49.161 Wisconsin Works
s. 49.19 Aid to Families with Dependent Children	s. 49.22 Child & Spousal Support
s. 49.45 Medical Assistance	s. 49.665 Badger Care
s. 49.77 Supplemental Payments	

CONFIDENTIALITY PROVISIONS CONTAINED IN CHAPTER 49

49.32 (9) Monthly Reports of Recipients of Aid to Families with Dependent Children [*this provision also includes W-2*]

(a) Each county department under s. 46.215, 46.22 or 46.23 administering aid to families with dependent children shall maintain a monthly report at its office showing the names of all persons receiving AFDC together with the amount paid during the preceding month. Each Wisconsin works agency administering Wisconsin works under ss. 49.141 to 49.161 shall maintain a monthly report at its office showing the names of all persons receiving benefits under s. 49.148 together with the amount paid during the preceding month. Nothing in the paragraph shall be construed to authorize or require the disclosure in the report of any information (names, amounts of aid or otherwise) pertaining to adoptions, or aid furnished for the care of children in foster homes or treatment foster homes under s. 46.261 or 49.19(10).

(b) The report under par. (a) shall be open to public inspection at all times during regular office hours and may be destroyed after the next succeeding report becomes available. Any person except any public officer, seeking permission to inspect such report shall be required to prove his or her identity and to sign a statement setting forth his or her address and the reasons for making the request and indicating that he or she understands the provisions of par. (c) with respect to the use of the information obtained. The use of a fictitious name is a violation of this section. Within 7 days after the record is inspected, or on the next regularly scheduled communication with that person, whichever is sooner, the county department or Wisconsin works agency shall notify each person making such inspection. County departments under ss. 46.215, 46.22 and 46.23 administering AFDC and Wisconsin works agencies administering Wisconsin works under ss. 49.141 to 49.161 may withhold the right to inspect the name of and amount paid to recipients from private individuals who are not inspecting this information for purposes related to public, educational, organizational, governmental or research purposes until the person whose record is to be inspected is notified by the county department or Wisconsin works agency, but in no case may the county department or Wisconsin works agency withhold this information for more than 5 working days. The county department or Wisconsin works agency shall keep a record of such requests. The record shall indicate the name, address, employer and telephone number of the person making the request. If the person refuses to provide his or her names, address, employer and telephone number, the request to inspect this information may be denied.

(c) It is unlawful to use any information obtained through access to such report for political or commercial purposes. The violation of this provision is punishable upon conviction as provided in s. 49.83.

49.32 (10) Release of information to Law Enforcement Officers

(a) Each county department under s. 46.215, 46.22 or 46.23 may release the current address of a recipient of food stamps or of aid under s. 49.19, and each Wisconsin works agency may release the current address of a participant in Wisconsin works under ss. 49.141 or 49.161 or, if administering the food stamp program, of a food stamp recipient, to a law enforcement officer if the officer meets all of the following conditions:

1. The officer provides, in writing, the name of the recipient or participant.
 2. The officer satisfactorily demonstrates, in writing, all of the following:
 - a. That the recipient or participant is a fugitive felon under 42 USC 608 (a) (9), is violating a condition of probation, extended supervision or parole imposed under state or federal law or has information that is necessary for the officer to conduct the official duties of the officer.
 - b. That the location or apprehension of the recipient or participant under subd. 2. a. is within the official duties of the officer.
 - c. The officer is making the request in the proper exercise of his or her duties under subd. 2. b.
- (b) If a law enforcement officer believes, on reasonable grounds, that a warrant has been issued and is outstanding for the arrest of a Wisconsin works participant, the law enforcement officer may request that a law enforcement officer be notified when the participant appears to obtain his or her benefits under the Wisconsin works program. At the request of a law enforcement officer under this paragraph, an employee of a Wisconsin works agency who disburses benefits may notify a law enforcement officer when the participant appears to obtain Wisconsin works benefits.

GENERAL DUTIES OF PUBLIC OFFICIALS

harassment was insufficient. *State ex rel Ledford v Turcotte*, 195 W (2d) 244, 536 NW (2d) 110 (Ct. App. 1995).

The amount of prepayment required for copies may be based on a reasonable estimate. *State ex rel Hill v Zimmerman*, 196 W (2d) 419, 538 NW (2d) 608 (Ct. App. 1995).

The *Forst* decision does not automatically exempt all records stored in a closed prosecutorial file. The exemption is limited to material actually pertaining to the prosecution. *Nichols v Bennett*, 199 W (2d) 268, 544 NW (2d) 428 (1996).

There is no blanket exception under the open records law for public employe disciplinary or personnel records. There must be a balancing of interests on a case by case basis. *Wisconsin Newspapers, Inc. v. School District of Sheboygan Falls*, 199 W (2d) 769, 546 NW (2d) 143 (1996).

Custodian may not require requester to pay cost of unrequested certification. Unless fee for copies of records is established by law, custodian may not charge more than actual and direct cost of reproduction. 72 Atty. Gen. 36.

Copying fee but not location fee may be imposed on requester for cost of computer run. 72 Atty. Gen. 68.

Fee for copying public records discussed. 72 Atty. Gen. 150.

Public records relating to employe grievances are not generally exempt from disclosure. Nondisclosure must be justified on case-by-case basis. 73 Atty. Gen. 20.

Disclosure of employe's birth date, sex, ethnic heritage and handicapped status discussed. 73 Atty. Gen. 26.

Department of regulation and licensing may refuse to disclose records relating to complaints against health care professionals while the matters are merely "under investigation"; good faith disclosure of same will not expose custodian to liability for damages; prospective continuing requests for records are not contemplated by public records law. 73 Atty. Gen. 37.

Prosecutors' case files are exempt from disclosure. 74 Atty. Gen. 4.

Relationship between public records law and pledges of confidentiality in settlement agreements discussed. 74 Atty. Gen. 14.

See note to 146.50, citing 78 Atty. Gen. 71.

19.36 Limitations upon access and withholding.

(1) APPLICATION OF OTHER LAWS. Any record which is specifically exempted from disclosure by state or federal law or authorized to be exempted from disclosure by state law is exempt from disclosure under s. 19.35 (1), except that any portion of that record which contains public information is open to public inspection as provided in sub. (6).

(2) LAW ENFORCEMENT RECORDS. Except as otherwise provided by law, whenever federal law or regulations require or as a condition to receipt of aids by this state require that any record relating to investigative information obtained for law enforcement purposes be withheld from public access, then that information is exempt from disclosure under s. 19.35 (1).

(3) CONTRACTORS' RECORDS. Each authority shall make available for inspection and copying under s. 19.35 (1) any record produced or collected under a contract entered into by the authority with a person other than an authority to the same extent as if the record were maintained by the authority. This subsection does not apply to the inspection or copying of a record under s. 19.35 (1) (am).

(4) COMPUTER PROGRAMS AND DATA. A computer program, as defined in s. 16.971 (4) (c), is not subject to examination or copying under s. 19.35 (1), but the material used as input for a computer program or the material produced as a product of the computer program is subject to the right of examination and copying, except as otherwise provided in s. 19.35 or this section.

(5) TRADE SECRETS. An authority may withhold access to any record or portion of a record containing information qualifying as a trade secret as defined in s. 134.90 (1) (c).

(6) SEPARATION OF INFORMATION. If a record contains information that is subject to disclosure under s. 19.35 (1) (a) or (am) and information that is not subject to such disclosure, the authority having custody of the record shall provide the information that is subject to disclosure and delete the information that is not subject to disclosure from the record before release.

(7) IDENTITIES OF APPLICANTS FOR PUBLIC POSITIONS. (a) In this section, "final candidate" means each applicant for a position who is seriously considered for appointment or whose name is certified for appointment and whose name is submitted for final consideration to an authority for appointment to any state position, except a position in the classified service, or to any local public office, as defined in s. 19.42 (7w). "Final candidate" includes, whenever there are at least 5 candidates for an office or position, each of the 5 candidates who are considered most qualified for the office or position by an authority, and whenever there are less than 5 candi-

dates for an office or position, each such candidate. Whenever an appointment is to be made from a group of more than 5 candidates, "final candidate" also includes each candidate in the group.

(b) Every applicant for a position with any authority may indicate in writing to the authority that the applicant does not wish the authority to reveal his or her identity. Except with respect to an applicant whose name is certified for appointment to a position in the state classified service or a final candidate, if an applicant makes such an indication in writing, the authority shall not provide access to any record related to the application that may reveal the identity of the applicant.

(8) IDENTITIES OF LAW ENFORCEMENT INFORMANTS. (a) In this subsection:

1. "Informant" means an individual who requests confidentiality from a law enforcement agency in conjunction with providing information to that agency or, pursuant to an express promise of confidentiality by a law enforcement agency or under circumstances in which a promise of confidentiality would reasonably be implied, provides information to a law enforcement agency or, is working with a law enforcement agency to obtain information, related in any case to any of the following:

a. Another person who the individual or the law enforcement agency suspects has violated, is violating or will violate a federal law, a law of any state or an ordinance of any local government.

b. Past, present or future activities that the individual or law enforcement agency believes may violate a federal law, a law of any state or an ordinance of any local government.

2. "Law enforcement agency" has the meaning given in s. 165.83 (1) (b), and includes the department of corrections.

(b) If an authority that is a law enforcement agency receives a request to inspect or copy a record or portion of a record under s. 19.35 (1) (a) that contains specific information including but not limited to a name, address, telephone number, voice recording or handwriting sample which, if disclosed, would identify an informant, the authority shall delete the portion of the record in which the information is contained or, if no portion of the record can be inspected or copied without identifying the informant, shall withhold the record unless the legal custodian of the record, designated under s. 19.33, makes a determination, at the time that the request is made, that the public interest in allowing a person to inspect, copy or receive a copy of such identifying information outweighs the harm done to the public interest by providing such access.

(9) RECORDS OF PLANS OR SPECIFICATIONS FOR STATE BUILDINGS. Records containing plans or specifications for any state-owned or state-leased building, structure or facility or any proposed state-owned or state-leased building, structure or facility are not subject to the right of inspection or copying under s. 19.35 (1) except as the department of administration otherwise provides by rule.

History: 1981 c. 335; 1985 a. 236; 1991 a. 39, 269, 317; 1993 a. 93; 1995 a. 27. Separation costs must be borne by agency. 72 Atty. Gen. 99.

Computerized compilation of bibliographic records discussed in relation to copying law; requester is entitled to copy of computer tape or printout of information on tape. 75 Atty. Gen. 133 (1986).

Federal exemption was not incorporated under (1). 77 Atty. Gen. 20.

Sub. (7) is an exception to the public records law and should be narrowly construed. In sub. (7) "applicant" and "candidate" are synonymous. "Final candidates" are the five most qualified unless there are less than five applicants in which case all are final candidates. OAG 6-93.

Public access to law enforcement records. Fitzgerald. 68 MLR 705 (1985).

19.365 Rights of data subject to challenge; authority corrections. (1) Except as provided under sub. (2), an individual or person authorized by the individual may challenge the accuracy of a record containing personally identifiable information pertaining to the individual that is maintained by an authority if the individual is authorized to inspect the record under s. 19.35 (1) (a) or (am) and the individual notifies the authority, in writing, of the challenge. After receiving the notice, the authority shall do one of the following:

(a) Concur with the challenge and correct the information.

943.70 Computer crimes. (1) DEFINITIONS. In this section:

(a) "Computer" means an electronic device that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network.

(b) "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of 2 or more interconnected computers.

(c) "Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

(d) "Computer software" means a set of computer programs, procedures or associated documentation used in the operation of a computer system.

(dm) "Computer supplies" means punchcards, paper tape, magnetic tape, disk packs, diskettes and computer output, including paper and microform.

(e) "Computer system" means a set of related computer equipment, hardware or software.

(f) "Data" means a representation of information, knowledge, facts, concepts or instructions that has been prepared or is being prepared in a formalized manner and has been processed, is being processed or is intended to be processed in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, punched cards and as stored in the memory of the computer. Data are property.

(g) "Financial instrument" includes any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or credit card, transaction authorization mechanism, marketable security and any computer representation of them.

(h) "Property" means anything of value, including but not limited to financial instruments, information, electronically produced data, computer software and computer programs.

(i) "Supporting documentation" means all documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.

(2) OFFENSES AGAINST COMPUTER DATA AND PROGRAMS. (a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies data, computer programs or supporting documentation.
2. Destroys data, computer programs or supporting documentation.
3. Accesses data, computer programs or supporting documentation.
4. Takes possession of data, computer programs or supporting documentation.
5. Copies data, computer programs or supporting documentation.
6. Discloses restricted access codes or other restricted access information to unauthorized persons.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2., 3. or 4. applies.
2. A Class E felony if the offense is committed to defraud or to obtain property.
3. A Class D felony if the damage is greater than \$2,500 or if it causes an interruption or impairment of governmental operations or public communication, of transportation or of a supply of water, gas or other public service.
4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(3) OFFENSES AGAINST COMPUTERS, COMPUTER EQUIPMENT OR SUPPLIES. (a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

2. Destroys, uses, takes or damages a computer, computer system, computer network or equipment or supplies used or intended to be used in a computer, computer system or computer network.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2., 3. or 4. applies.
2. A Class E felony if the offense is committed to defraud or to obtain property.
3. A Class D felony if the damage to the computer, computer system, computer network, equipment or supplies is greater than \$2,500.
4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(4) COMPUTER USE RESTRICTION. In addition to the other penalties provided for violation of this section, a judge may place restrictions on the offender's use of computers. The duration of any such restrictions may not exceed the maximum period for which the offender could have been imprisoned; except if the offense is punishable by forfeiture, the duration of the restrictions may not exceed 90 days.

(5) INJUNCTIVE RELIEF. Any aggrieved party may sue for injunctive relief under ch. 813 to compel compliance with this section. In addition, owners, lessors, users or manufacturers of computers, or associations or organizations representing any of those persons, may sue for injunctive relief to prevent or stop the disclosure of information which may enable another person to gain unauthorized access to data, computer programs or supporting documentation.

History: 1981 c. 293; 1983 a. 438, 541; 1987 a. 399. Judicial Council Note, 1988: [In (2) (b) 4. and (3) (b) 4.] The words "substantial risk" are substituted for "high probability" to avoid any inference that a statistical likelihood greater than 50% was ever intended. [Bill 191-S]

This section is constitutional. Copyright law does not give a programmer a copyright in data entered into the programmer's program, and copyright law does not preempt prosecution of the programmer for destruction of data entered into the program. State v. Corcoran, 186 W (2d) 616, 522 NW (2d) 226 (Ct. App. 1994).

Criminal liability for computer offenses and the new Wisconsin computer crimes act. Levy. WBB March 1983.



943.70 Computer crimes. (1) DEFINITIONS. In this section:

(a) "Computer" means an electronic device that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network.

(b) "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of 2 or more interconnected computers.

(c) "Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

(d) "Computer software" means a set of computer programs, procedures or associated documentation used in the operation of a computer system.

(dm) "Computer supplies" means punchcards, paper tape, magnetic tape, disk packs, diskettes and computer output, including paper and microform.

(e) "Computer system" means a set of related computer equipment, hardware or software.

(f) "Data" means a representation of information, knowledge, facts, concepts or instructions that has been prepared or is being prepared in a formalized manner and has been processed, is being processed or is intended to be processed in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, punched cards and as stored in the memory of the computer. Data are property.

(g) "Financial instrument" includes any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or credit card, transaction authorization mechanism, marketable security and any computer representation of them.

(h) "Property" means anything of value, including but not limited to financial instruments, information, electronically produced data, computer software and computer programs.

(i) "Supporting documentation" means all documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.

(2) OFFENSES AGAINST COMPUTER DATA AND PROGRAMS. (a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies data, computer programs or supporting documentation.
2. Destroys data, computer programs or supporting documentation.
3. Accesses data, computer programs or supporting documentation.
4. Takes possession of data, computer programs or supporting documentation.
5. Copies data, computer programs or supporting documentation.

6. Discloses restricted access codes or other restricted access information to unauthorized persons.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2., 3. or 4. applies.
2. A Class E felony if the offense is committed to defraud or to obtain property.
3. A Class D felony if the damage is greater than \$2,500 or if it causes an interruption or impairment of governmental operations or public communication, of transportation or of a supply of water, gas or other public service.
4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(3) OFFENSES AGAINST COMPUTERS, COMPUTER EQUIPMENT OR SUPPLIES. (a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

2. Destroys, uses, takes or damages a computer, computer system, computer network or equipment or supplies used or intended to be used in a computer, computer system or computer network.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2., 3. or 4. applies.
2. A Class E felony if the offense is committed to defraud or obtain property.
3. A Class D felony if the damage to the computer, computer system, computer network, equipment or supplies is greater than \$2,500.
4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(4) COMPUTER USE RESTRICTION. In addition to the other penalties provided for violation of this section, a judge may place restrictions on the offender's use of computers. The duration of any such restrictions may not exceed the maximum period for which the offender could have been imprisoned; except if the offense is punishable by forfeiture, the duration of the restrictions may not exceed 90 days.

(5) INJUNCTIVE RELIEF. Any aggrieved party may sue for injunctive relief under ch. 813 to compel compliance with this section. In addition, owners, lessors, users or manufacturers of computers, or associations or organizations representing any of those persons, may sue for injunctive relief to prevent or stop the disclosure of information which may enable another person to gain unauthorized access to data, computer programs or supporting documentation.

History: 1981 c. 293; 1983 a. 438, 541; 1987 a. 399.
Judicial Council Note, 1988: [In (2) (b) 4. and (3) (b) 4.] The words "substantial risk" are substituted for "high probability" to avoid any inference that a statistical likelihood greater than 50% was ever intended. [Bill 191-S]
This section is constitutional. Copyright law does not give a programmer a copyright in data entered into the programmer's program, and copyright law does not pre-empt prosecution of the programmer for destruction of data entered into the program.
State v. Corcoran, 186 W (2d) 616, 522 NW (2d) 226 (Cl. App. 1994).
Criminal liability for computer offenses and the new Wisconsin computer crimes act. Levy. WBB March 1983.