DEPARTMENT OF JUSTICE
1162 Court Street NE
Justice Building
Salem, Oregon 97310
Telephone: (503) 378-4400
TDD: (503) 378-5938

August 4, 1993

No. 8226

This opinion responds to questions raised by the Workforce Quality Council (WQC). Those questions concern federal and state confidentiality requirements that may affect the proposed operation of a Shared Information System (SIS) by a group of state workforce development agencies, and the use of social security numbers in the SIS. We have been asked to base our opinion on the following assumptions[1] concerning the purpose and operation of the SIS:

(1) There will be ten participating agencies: Bureau of Labor and Industries (BOLI), Job Training Partnership Act Administration (JTPA), Department of Corrections (ODOC), Workers' Compensation Division (WCD), Adult and Family Services Division (AFSD), Employment Division (ED), Vocational Rehabilitation Division (VRD), Department of Education (ODE), Office of Community College Services (OCCS) and State System of Higher Education (OSSHE). Each participating agency will have an interagency agreement with the SIS[2].

(2) The SIS would be located within the Employment Division and would act as a limited agent on behalf of each of the participating agencies in that the SIS would be authorized only to collect data from each of the agencies, to match that data with the data from the other agencies and to distribute aggregate data, as described below. The SIS would not be authorized to distribute any data in the form in which it was originally collected or in any other personally identified form. The SIS would be responsible to a board consisting of members from each of the participating agencies. The SIS Board would be responsible to the WQC.

(3) Each participating agency would provide client and workforce-related information to the SIS by transmitting that information from the agency to the Department of Human Resources (DHR) computer. This information would have the client's social security number transformed into an alternative, individual identifier by

[1] These assumptions form an integral part of the opinion. If the actual operation of the SIS were to eviate from the assumptions, the conclusions reached in this opinion may no longer be valid.
[2] We use the term "the SIS" to refer both to the Shared Information System and to the state agency that will be operating the Shared Information System.

that agency's "encoder."[3] The encoding formula used by each participating agency would be unique to that agency; the formula would not be disclosed to any other agency, including the SIS.

(4) The DHR computer would be programmed with the decoding formula for each agency so that the client's social security number could be decoded for purposes of performing data matches only. Only DHR computer staff would have access to the decoding formulae; no SIS staff would have access to these formulae. Neither any DHR computer staff nor any SIS staff would have access t the encoded SIS data. Neither any SIS staff nor nay DHR computer staff would be able to use the decoding formulae to gain access to personally identifiable information.

(5) The SIS staff would determine whether a request for a data match meets WQC guidelines or has been approved by the WQC. If not, the request would be rejected. If so, the SIS staff would request the DHR computer staff to program the DHR computer to produce a report by decoding the necessary client information and matching the appropriate data[4].

(6) In producing a report, the client's social security numbers would be decoded and the data matched as part of a virtually simultaneous computer process. All decoded client social security numbers would be immediately re-encoded as soon as the match has been completed. Only the results of the data match would be transmitted to the SIS in the form of aggregate statistical and demographic data, without any personal identifiers. In order to further protect client identity, the DHR computers would be programmed to prevent it from reporting any results from a data match involving five or fewer clients.

(7)The WQC guidelines would authorize the SIS to generate reports of aggregate statistical and demographic data on education, training and other services provided to clients and the resulting client outcomes in order to facilitate the WQC's development and coordination of education and training programs for Oregon's workforce. The WQC staff could also approve requests for reports of aggregate data for other purposes, such as reports of aggregate data that would facilitate the participating agencies' program planning, performance evaluation and provision of services to Oregon's citizens. The SIS staff would analyze the aggregate data, according to the purposes for the request, and provide that analysis along with the data. The data produced by the SIS would not be used by any participating agency, or any other state agency or official, to make any decision or take any action directly affecting any individual.

---

[3] No personally identifiable client information(e.g, name, address), other than the social security number, would be providied to the SIS from the participating agency.

[4] Once a program for a particular report has been written by the DHR computer staff, it would be placed in the SIS software library so that the SIS staff could generate that report in the future by sending a command directly to the DHR computer.

(8) Adequate safeguards would be established to ensure the security of the information collected by the SIS and maintained in the DHR computer and to prohibit the disclosure of any confidential information in personally identifiable form. SIS data would have the highest level of security protection available from the IBM Resources Access Control Facility. The encoding formula used by the participating agencies would be changed periodically by those agencies.

FIRST QUESTION PRESENTED

> Would any federal laws or regulations or state laws prohibit or restrict the SIS participating agencies from transmitting encoded client information to the DHR computer for the proposed operation of the SIS without the consent of the individual who originally provided the information to the participating agency? If so, explain which laws and whether obtaining consent would obviate the prohibition or restriction.

ANSWER GIVEN

In the light of the assumptions governing the operation of the SIS set out above, we conclude there are no federal statutory or regulatory barriers that would prohibit the SIS participating agencies from transmitting encoded client information to the DHR computer or the computer's cross-matching of that information to produce aggregate statistical and demographic data for the SIS, with the possible exception of information gathered by ED from employers on behalf of the Bureau of Labor Statistics. Because this conclusion is not completely free from doubt, however, and because violation of federal confidentiality requirements could potentially subject participating agencies to the loss of federal funding, we recommend that the WQC consult with the federal agencies noted in our discussion below to ensure that those agencies concur with our conclusion.

We also conclude that there are no state statutes that would prohibit the participating agencies form transmitting encoded client information for use in the operation of the SIS, with the exception of ORS 285.183, governing JTPA participant records, and ORS 657.665, governing ED records. We recommend that the WQC seek amendments to these particular state statutes to explicitly permit disclosure of those records for use in the SIS. Because many other state statues pose a close question of interpretation, we further recommend that the WQC seek enactment of a blanket state statue authorizing the participating agencies to provide the SIS with client records in order to remove all doubt under state law. Obtaining individual, informed consent to release of the information to the SIS would obviate any statutory or regulatory barriers to disclosure, even if no statuary amendments were made.

SECOND QUESTION PRESENTED

Would federal or state law prohibit the participating agencies from using social security numbers as personal identifiers when providing information to the DHR computer for the proposed operation of the SIS? If so, explain whether there are any steps that the participating agencies may take to permit the use of social security numbers for these purposes.

ANSWER GIVEN

Section 7(b) of the Privacy Act of 1974, 5 USC § 552a, would prohibit the participating agencies form using their clients' social security numbers when providing information to the SIS, unless the agencies have provided notice to their clients describing that use of their social security numbers and obtained consent for such use.

THIRD QUESTION PRESENTED

What safeguards, if any, are required by federal or state law to ensure that the confidentially of data collected by the SIS is maintained?

ANSWER GIVEN

Neither federal nor state law require particular safeguards for the confidentiality of data that would be applicable to the SIS.

DISCUSSION

I. Introduction

The Oregon Workforce Quality Act (Workforce Quality Act) established the WQC and charged it to oversee the implementation of workforce development strategies, including primary and secondary school reform and professional and technical education reform as they relate to improving the education and training received by Oregon's workforce, OR Laws 1991, ch 667, § 6(1). The WQC is also charged with developing goals and a comprehensive statewide strategy to improve the quality of Oregon's workforce, Oregon Laws 1991, chapter 667, section 6(6), and overseeing the "[c]entralized delivery of employment and training services at the local level in response to local needs, including but not limited to developing a plan for centralizing state supported employment and training services at the local level." Or Laws 1991, ch 667, § 6(5).

Pursuant to Section 13 of the Workforce Quality Act, the WQC is designated as Oregon's occupational information coordinating committee formed in accordance with Executive Order 90-08 and 20 USC § 2422(b). Or laws 1991, ch 667, § 13. The WQC is expressly required to seek federal support and waivers, if necessary, to implement the Act. Or Laws 1991, ch 667, § 14.

The SIS is intended to further the purpose of the Workforce Quality Act by collecting client information from the participating agencies. That composite data pool would then be used by the SIS for computer matching and analysis to provide aggregate statistical and demographic data to the WQC, the participating agencies and other state agencies and officials for their use in developing education and training programs for Oregon's workforce. The SIS would not report out any information in a personally identifiable form, even to the participating agencies. Furthermore, the information collected by the SIS would not be used by the participating agencies or any other state agencies or officials to make any decision or take any action directly affecting any individual.

II. Prohibitions or Restrictions on Participating Agencies' Release of Information to the SIS

The SIS will involve the participation of at least ten state agencies. There are dozens of federal and state confidentiality statutes that restrict those agencies' disclosure of information records. Consequently, the question of disclosure of information to the SIS has no simple answer that will uniformly apply to all the participating agencies. For this reason, we address this question on an agency-by-agency basis.

Because it would be an enormous -- if not impossible -- task to discuss each kind of information that the SIS participating agencies might possess and whether that information is subject to federal or state confidentiality laws or regulations, the WQC has identified several kinds of information contained in the records of the participating agencies that are of interest to the SIS. Accordingly, we discuss only those federal and state statutes and federal regulations that apply to the kinds of information that have been identified for us. We set out in Appendix A a list of other statutes and regulations that are not discussed in this opinion, but that may prohibit or restrict the disclosure of information or records in the possession of the participating agencies. We do not discuss any administrative rules adopted by the participating agencies that might prohibit or restrict their disclosure of information to the SIS because we assume that, in the absence of federal or state law compelling such rules, each agency will appropriately amend its rules to permit its client information to be used in the operation of the SIS.

At the outset, it is important to set the context of the discussion relating to the disclosure of information by particular participating agencies. The statutes and regulations analyzed below prohibit or restrict the release or disclosure of information or records. These provisions represent a legislative intent to protect the confidentiality or privacy interests of the individuals about whom the information or records pertain. See. e.g., FERPA legislative history, below. In general, these statutes and regulations provide for some permissible releases or disclosures as exceptions to the general rule that the records and information in question are otherwise confidential. It is a long-standing tenet of statuary construction that exceptions should be narrowly construed.

See, e.g., Jensen v. Garvison, 241 F Supp 523, 526 (D Or 1965), cause remanded, 355 F2d 487 (9th Cir 1966); 2A Sutherland Statutory Construction § 47.11, at 165 (5th ed Singer 1992). That tenet informs the discussion below. Consequently, while much of the discussion relates to the concept of "disclosure," it must be kept in mind that, under these statues and regulations, confidentiality is the rule and disclosure is the exception.[5]

We note, however, that under the assumptions for the operation of the SIS , no decisions or actions directly affecting individuals would ever be based upon any encoded client information contained in the DHR computer, the cross-matching of that information by the DHR computer or the analyses of the aggregate data reported to the SIS. Assumptions 4, 7. In this regard, the proposed operation of the SIS is similar to the research and aggregate statistical data matching activities performed by some federal agencies prior to the enactment of the Computer Matching and Privacy Protection Act of 1988, 5 USC § 552a (West 1977 ans Supp 1993). See HR Rep No. 802, 100th Cong, 2d Sess 2-5, reprinted in 1988 US Code Cong & Admin News 3107, 3108-11. Even that Act , which restricts the use of federal records,[6] itself expressly exempts computer matches performed to "produce aggregate statistical data without any personal identifiers."[7] 5 USC § 552a (a)(8)(B)(i) (Supp 1993). See HR Rep No. 802, supar, 1988 US Code Cong & Admin News 3130.

A. The Principal-Agent Relationship

[5] These confidentiality provisions establish a framework that is in some ways the antithesis of the scheme set up under the Oregon Public Records Law, ORS 192.410 to 192.505. The Oregon Public Records Law establishes the general rule that all public records are subject to public disclosure unless they are explicitly exempt from disclosure. The Public Records Law contains express exemptions for records or information, the disclosure of which is prohibited by federal law or regulations, ORS 192.502(7), or prohibited or restricted or otherwise made confidential or privileged under Oregon law. ORS 192.502(8). Consequently, to the extent that disclosure of the reccords discussed below is prohbited or restricted by federal laws or regulations or by state law,their disclosure may not be compelled under the Oregon Public Records Law.

[6] The Computer Matching and Privacy Protection Act of 1988 applies only to federal agencies and to computer data provided by federal agencies to other agencies, including state agencies for purposes of performing "computer matches" leading to individualized determinations. As to such data, the Act reequires a state agency to enter into a written agreement with the federal agency not to "redisclose" the federal data within or outside the state agency, except where required by federal law or essential to the purpose of the coomputer matching program for which the data was disclosed to the state agency. 5 USC § 552a(o)(1)(H) (Supp 1993). As to any other data received from federal agencies, the state agency would need to receive clear direction from the federal agencies as to the permissibility of redisclosure.

[7] The computer Matching and Privacy Protection Act of 1988 does not provide any independent authorization for release or disclosure of information by federal agencies participating in a federal computer matching program. See HR Rep No. 802, 100th Ccong, 2d Sess 22, reprinted in 1988 US Code Cong & Admin News 3107, 3128. The Act merely adds an additional layer of procedural protections above and beyond the protections against disclosures that are contained in other relevant statutes. Therefore, while the computer Matching and Privacy Acct indicated that Congress was somewhat less worried about computer matches used only for statistical research purposes, the Act does not constitute any support for concluding that releasse or disclosures of otherwise confidential records are authorized simply because the records are used only for statistical or research purposes in a computer matching program. The confidentiality of records and the propriety of releasing or disclosing those records must be determined by analyzing the provisions of each participating aency's statutes.

One of the assumptions concerning the operation of the SIS is that it "would act as a limited agent on behalf of each of the [ten] participating agencies." Assumption 2.

An "agent" is someone who is authorized by a "principal" to act for the principal in relationships between the principal and third parties. Gaha v. Taylor-Johnson Dodge, 53 Or App 471, 476, 632 P2d 483 (1981); Restatement (Second) of Agency § 1 (1958). Because an agent's power to act is based upon the authority vested in him by the principal, an agent has no power to do anything that the principal is not authorized to do. For example, if AFSD could not lawfully disclose or use information about a particular individual's public assistance or employment status, the SIS, as AFSD's agent, could not lawfully disclose or use that information.

Although the SIS would act as an agent for each of the ten participating agencies, this relationship would not , in our opinion, present any legal problems arising from these multiprincipal-agent relationships. We understand that the designation of the SIS as a "limited agent" is intended to signify that the SIS would not only operate within the legal constraints that bind each of its principals, but would also be authorized by its principal only to collect data, to direct the matching of that data and to distribute aggregate data reports in the manner set out in Assumptions 2 through 8 above. See Assumption 2. Moreover, the SIS staff would not have access to any personally identifiable client information, nor would it be able to obtain, or be authorized to use, the decoding formulae to gain access to personally identifiable client information. Assumption 4.

Accordingly, we do not believe that the fact that the SIS is acting as an agent for more than one principal would itself present any breach of confidentiality.

B. The SIS Computer Matching Process

Before turning to the numerous confidentiality statutes, it is useful to first look at the discrete steps involved in the proposed operation of the SIS in order to understand where confidentiality or privacy may be implicated. There are four steps:

(1) a participating agency's transmittal of encoded client information to the DHR computer;

(2) the DHR computer's cross-matching of client information provided by two or more of the participating agencies to produce aggregate statistical demographic data;

(3) the computer's report to the SIS staff of the aggregate statistical and demographic data produced by its cross-matching;

(4) the SIS staff's disclosure of the aggregate data to the WQC, the participating agencies, other governmental agencies and officials and the public.

We do not believe that the first step, the mere transmittal of encoded client information to the DHR computer by a participating agency can implicate any privacy or confidentiality laws. At this step, the computer merely receives and stores the information. In its encoded form within the DHR computer, the client information is not generally accessible; the computer will only release or process that information upon instruction. Whether privacy or confidentiality interests might be transgressed will depend upon what is done with the information after it is in the DHR computer. If the proposed use of the information is permitted under the participating agency's statutes, there is no violation of law; if not, then there would be a violation.

The second step is the computer cross-matching of client information to produce aggregate data. The DHR computer staff would be authorized only to accede to requests from the SIS staff to decode the social security numbers and to cross-match client information with that provided by one or more of the other participating agencies to produce aggregate statistical and demographic data. This cross-matching of client information would take place only within the computer; only the computer would "see" the client information being matched. As soon as the data match was completed, the computer would immediately re-encoded the client social security numbers. Because, at this step, no client information is revealed to anyone, we do not believe that a release of client information can be said to have occurred. However, it is certainly arguable that the information is being "inspected" or "used" by the computer, albeit not by any persons, either DHR computer staff, SIS staff, participating agency staff or anyone else. Whether this step would constitute a violation of any of the participating agencies' confidentiality statutes will depend upon an analysis of those statues.

The last two steps involve only the aggregate statistical and demographic data produced by the computer cross-matching. The aggregate data from data matches involving no less than six clients would be reported by the DHR computer to the SIS staff. Based on that aggregate data, the SIS staff would prepare its own report and recommendations to the WQC, the participating agencies, other agencies and officials and the public. Because only aggregate data, without personal identifiers or any means to identify the individuals to whom the data pertains, would be involved in these two steps, no privacy or confidentiality interest can be contravened.

Thus, we next discuss for each participating agency any federal or state statutes that may prohibit or restrict the cross-matching of client information by the DHR computer to produce aggregate data.

C. Bureau of Labor Industries

Unlike several of the other participating agencies, BOLI has neither federal statutes nor a general state confidentiality statue applicable to its records. There are, however, several state confidentiality statutes covering particular kinds of information possessed by BOLI. We have been informed that, at this time, the DHR computer

would not be used to analyze the kinds of information covered by most of those state statutes.[8] Accordingly, we focus on only two types of information contained in BOLI records that we understand are relevant for SIS purposes and that have confidentiality restrictions: information used to determine or enforce prevailing wage rates and apprentices' training school records.

1. Prevailing Wage Rate Information

BOLI is directed by state law to "determine the prevailing rate of wage for workers in each trade or occupation in each locality under ORS 279.348 at least once each year and make this information available. " ORS 279.359(1). To make these determinations, BOLI may require employers and labor organizations to submit reports of workers' wages.

> Notwithstanding ORS 192.410 to 192.505 [the Oregon Public Records Law], all information or records provided to the commissioner under [ORS 279.359] are confidential and shall not be available for inspection by the public.

(Emphasis added.)

BOLI also is authorized to enforce the prevailing wage rate on public works projects. ORS 279.355. BOLI may inspect contractors' and subcontractors' payroll and other records. ORS 279.355(2). Again, "notwithstanding" the Public Records Law, any records obtained by BOLI under this statuary provision "shall not be open to inspection by the public." ORS 279.355(3).

ORS 279.355(3) and 279.359(3) prohibit "inspection by the public" of the information and records used to determine or enforce prevailing wage rates. In light of this statutory language, we conclude that the scope of the confidentiality provisions in these two statutes is limited to prohibiting disclosure of the information to the public. We do not believe that these statues prohibit BOLI from transmitting this information to the DHR computer in an encoded form, or prohibit the cross-matching of that information by the computer, inasmuch as no "public" inspection of the workers' wage or payroll records would be involved. The specific reference to the Public Records Law, which gives every "person" the right to inspect public records, ORS 192.420, further suggests that the legislature was concerned only with disclosure to the public, not with other possible uses to which the state may put the information. In this regard, we note that the statutes contain no restrictions or prohibition on the state's use of this information for purposes unrelated to prevailing wage rates and we find no policy implicit in the prevailing wage rate statutes that would suggest such a restriction so long as no personally identifiable information is disclosed to the public.

[8] We have listed each of those statutes in Appendix A, but do not analyze their restrictions.

Because of our conclusion that BOLI is not prohibited from providing information on workers' wages to the DHR computer in an encoded form, it is not necessary for BOLI to obtain consent from the employers, organizations, or individuals that provided the wage records or that are identified in those records. However, notwithstanding our interpretation of the confidentiality provisions in ORS 279.355(3) and 279.359(3), if any information that was obtained by BOLI in determining or enforcing prevailing wage rates is to be used in the operation of the SIS, the WQC may wish to seek amendments to these two statutory provisions to explicitly permit BOLI to provide to the DHR computer.[9]

2. Apprenticeship and Training Program Records

BOLI and other government entities (e.g., State Apprenticeship and Training Council, Department of Education, State Board of Education, district school boards) are authorized to administer apprenticeship and training programs under ORS chapter 660 and to maintain records regarding the programs and participants. ORS chapter 660 does not contain any express confidentiality provisions. Therefore, as a general rule, information in apprenticeship program records maintained by BOLI may be provided to the DHR computer.

ORS 660.020 requires that every apprentice, the apprentice's employer and the local joint apprenticeship committee sign a written apprenticeship agreement, which must be registered with the State Apprenticeship and Trained Council. The agreement must include

> [a] waiver by the apprentice granting permission for release of related training school records to the appropriate joint apprenticeship committee for the purpose of evaluation.

ORS 660.060(9).

This statutory provision appears to prohibit an apprenticeship committee from reviewing any apprentice's training school records for evaluative purposes unless the apprentice has authorized release of the records to the committee. We do not believe that this statutory provision prohibits BOLI from providing this information to the DHR computer in an encoded form inasmuch as no human inspection of personally identifiable information would be involved, and no decision or action directly affecting the apprentice would be made based upon the aggregate statistical and demographic data that would be produced by the computer.

---

[9] As drafted, HB 3617 in the current legislative session would authorize the SIS participating agencies, inlcuding BOLI, to provide the SIS with information "relating to job training and edcuation programs" HNB 3617, § 2(1). In light of the information that we understand would be of interest to the SIS, we recommend that the scocpe of this provision in HB 3617 be broadened to authorize the aencies to provide the SIS with "information for the development of statistical and demographic data to facilitate the creation of strategies to improve the education, training and quality of Oregon's workforcce."

However, to remove any uncertainty, the WQC may wish to seek legislation that expressly permits BOLI and other state government entities to provide information from apprentices' training school records to the DHR computer.[10]

D. Oregon Department of Corrections

There are several confidentiality statutes pertaining to ODOC. We have listed these statutes in Appendix A. Because the WQC has informed us that, at this time, the SIS would not be interested in the kinds of information covered by those confidentiality statutes, we do not analyze their restrictions. As a general rule, ODOC may provide all other inmate information to the DHR computer.[11] No inmate consent is needed.

E. Workers' Compensation Division

There are no federal or state confidentiality statutes directly pertaining to records of the Workers' Compensation Division (WCD).[12] However, ORS 656.702 provides that the "records of the State Accident Insurance Fund Corporation [SAIF], expecting employer account records and claimant files, shall be open to public inspection. (Emphasis added.) Therefore, if WCD obtains employer account records and claimant files from SAIF, those documents could not be open to public inspection and would be exempt from disclosure under the Oregon Public Records Law. ORS 192.502(8). See also ORS 192.502(2) and (9).

The prohibition in ORS 656.702 on "public inspection" of these records suggests that the legislature was concerned with disclosure to the public, and not with other possible uses to which the information may be put by SAIF or other state agencies. We find no policy implicit in ORS 656.702 , when read in context with the Workers' Compensation Law, ORS chapter 656, that would suggest a restriction on the use of the information by the state so long as no personally identifiable information is released or disclosed to the public. Accordingly, we conclude that the confidentiality provision in ORS 656.702 does not prohibit WCD from providing information in employer account records and claimant files to the DHR computer in an encoded form for the proposed operation of the SIS inasmuch as no "public" disclosure of individual records, files or information would be involved. Thus, no individual's confidentiality interests under the statute would be affected.

---

[10] See note 9.

[11] We have been informed that there are some ODOC records, the inspection or disclosure of which is not prohibited by law but, nevertheless, would be subject to restrictions by ODOC because disclosure would jeopardize the safety, security and order of ODOC institutions, staff, inmates, and members of the public. See OAR 291-35-005 to 291-35-020, and 291-39-005 to 291-39-015.

[12] Appendix A to this opinion lists federal and state statutes and federal regulations applicable to certain information in the possession of SIS participating agencies, including WCD. We have not analyzed those disclosure restrictions because we understand that the SIS is not interested in the information to which the restrictions apply.

In light of our conclusion, it is not necessary to obtain consent from the individuals about whom the records pertain. However, notwithstanding our interpretation of ORS 656.702, the WQC may wish to seek to have this statute amended to explicitly permit WCD to provide the information to the DHR computer.[13]

F. Job Training Partnership Act Programs

Both federal and state statues and regulations apply to records concerning the confidentiality of records maintained by the JTPA program.

1. Federal Law

The Job Training Reform Amendments of 1992 amended section 165(a) of the Job Training Partnership Act by adding the following provisions.

> (3) * * *[R]ecipients shall maintain standardized records for all individual participants * * *.
>
> (4)(A) Except as provided in subparagraph (B), records maintained by recipients pursuant to this subsection shall be made available to the public upon request.
>
> (B) Subparagraph (A) shall not apply to--
>
> (i) information, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; * * *

29 USC § 1575(a) (Supp 1993) (emphasis added).

The united States Department of Labor recently promulgated regulations to implement the Job Training Reform Amendments of 1992. 20 CFR § 627.463(b) provides, in relevant part:

> (b) Exceptions. A record maintained by a recipient [state] or subrecipient [Service Delivery Area] pursuant to section 165(a) of the Act shall not be made available to the public, notwithstanding the provisions of State or local law, where such record is:
>
> (1) Information, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; * * *

The phrase "clearly unwarranted invasion of personal privacy" is not defined in either the Act or the rules.

---

[13] See note 9.

Because of the confidentiality safeguards that would be employed in the transmittal, handling and use of client information under the proposed operation of the SIS, we do not believe that the Economic Development Department's transmittal of JTPA participants' records to the DHR computer in an encoded form, and the computer's cross-matching of SIS participating agencies' client information, would be a "clearly unwarranted invasion of personal privacy." As noted previously, only the DHR computer would "see" the client information being matched. The computer would simply cross-match information provided by two or more of the participating agencies to produce aggregate statistical and demographic data. As soon as the data match was completed, the computer would immediately re-encode the client social security numbers. The computer would not reveal to anyone - not even to the participating agencies, DHR computer staff or SIS staff - any client information. No such information would be available to be used in any way to make decisions directly affecting an individual.

Accordingly, we conclude that federal JTPA law would not be violated by the proposed operation of the SIS.

2. State Law

ORS 285.183 provides:

> (1) All participant records maintained by the local service delivery area providers or any public or private agency involved in Job Training Partnership Act programs shall be confidential *** and shall be open for inspection only in accordance with such rules as the [Economic Development Department] shall adopt.
>
> (2) A participant may provide written consent for the examination or release of any record pertaining to the participant.
>
> * * * * *
>
> (4) The department may adopt rules to provide the circumstances under which participant names or records may be made available for inspection when:
>
> * * * * *
>
> (c) Necessary to provide information to state and local agencies administering ORS chapters 418 and 657.
>
> (d) Necessary for programstaff work or studies of a statistical or demographic nature.

(e) Necessary to carry out the planning and coordinating functions between state and local agencies required by the federal Job Training Partnership Act (29 U. S. C. 1501), as amended, and the State Job Training Partnership Administration within the department.

(Emphasis added)

If the participant or the participant's parent, legal guardian or surrogate if the participant is under 18 years of age, consents to release, all records pertaining to that participant may be examined or released. ORS 285.183(2); OAR 123-70-230(3). Without such consent, a participants record s may be examined or released only if one of the exceptions in ORS 285.183(4) applies and the Economic Development Department (EDD) has adopted rules permitting disclosure or release of the records under such circumstances.

With respect to other confidentiality statutes discussed in this opinion, we have concluded that state statutory restrictions on "public inspection" of agency records would not prohibit the transmitting of the records to the DHR computer in an encoded form inasmuch as no public inspection of personally identifiable information would be involved. In contrast, ORS 285.183 prohibits the inspection of JTPA participant records except for limited purposes, even where the inspection of the records is not by the public, but by another state agency, ORS 285.183(4)(c), or for statistical studies, ORS 285.183(4)(d), and, then, only if EDD rules permit such inspection.

"Participant records" are defined as records relating to matters such as grades, conduct, personal and academic evaluations, results of psychometric testing, counseling, disciplinary actions, if any, and other personal matters.

ORS 285.180(3). This broad definition appears to encompass all personal information concerning participants. See also OAR 123-70-220(2)-(4).

The legislative history of ORS 285.183 indicates that its confidentiality provisions are intended to serve the following purposes:

SB 3A requires that records of participants in the Job Training Partnership Act programs be kept confidential and allows the Economic Development Department to establish rules regarding circumstances under which records may be open for inspection [for the purposes described in ORS 285.183(4)].

Staff Measure Analysis, Trade and Economic Development Committee (SB 3), Michelle Wong, Senior Legislative Assistant (June 8 and 10, 1987).

In the light of the broad definition of "participant records" in ORS 285.180(3), the limited exceptions to confidentiality for state agencies provided in ORS 285.183(4)(c)-(e), and the legislative history of this statute, we conclude that the statute prohibits

even the DHR computer's "inspection" and cross-matching of the data unless their use by the SIS comes within one of the statutory exceptions. See 40 Op Atty Gen 96, 98-99 (1979) (where statute prohibits "public inspection" of CSD records and specifies who may inspect, agency acting in "official capacity" may not review records). To conclude otherwise would render the provisions of ORS 285.183(4)(c)-(e) virtually meaningless, contrary to the well-established rule of statuary interpretation that,

> where there are several provisions or particulars [in a statute] such construction is, if possible, to be adopted as will give effect to all.

ORS 174.010.

Thus, we next discuss the three statutory exceptions, ORS 285.183(4)(c) -(e), that might apply to the SIS.

ORS 285.183(4)(c) authorizes release of participant records when necessary to provide information to the state agencies administering ORS chapters 418 and 657. This provision permits release of information from participant records to AFSD, which administers the Aid to Dependent Children program, ORS 418.035 to 418.149, and to ED, which administers the unemployment compensation and employment services programs, ORS chapter 657, but only when such information is "necessary" for those agencies to administer their respective programs. Even if transmittal participant records to the DHR computer were determined to be necessary for the administration of those AFSD and ED programs, the SIS could not instruct the DHR computer to "inspect" those records in order to cross-match information on JTPA participants for any purpose that would not be "necessary" to the administration of the ORS chapter 418 or 657 programs. We understand that this limitation on the use of the records by the SIS could significantly compromise the purpose of the SIS. If the legislature were to create the SIS as an ED program in ORS chapter 657, however, ORS 285.183(4)(c) would then permit release of JTPA participant records to ED to the extent necessary to administer the SIS, which could include the use of information in JTPA participant records for WQC purposes.

ORS 285.183(4)(d) authorizes release of participant records when "[n]essary for program * * * studies of a statistical or demographic nature". We interpret this provision to permit release of such information only when the statistical or demographic study is "necessary" for JTPA program purposes. If the EDD were to conclude that such a study is necessary for JTPA purposes, JTPA participant records could be released under this provision. Again, the SIS could not use information obtained under this provision to do studies or analyses for non-JTPA purposes.

ORS 285.183(4)(e) authorizes release of participant records when necessary to carry out the planning and coordinating functions between state and local agencies "required by" the federal JTPA and the State Job Training Partnership Administration.

The Governor is required to submit a coordination plan to the federal Secretary of Labor that establishes criteria for coordinating JTPA activities.

> with programs and services provided by State and local education and training agencies (including vocational education agencies), public assistance agencies, the employment service, rehabilitation agencies, programs for the homeless, postsecondary institutions, economic development agencies, and such other agencies as the Governor determines to have a direct interest in employment and training and human resources utilization within the State.

29 USC § 1531(b)(1)(Supp 1993). This list of agencies would appear to include all of the SIS participating agencies. If the EDD were to make a determination that release of JTPA participants' records to the SIS is "necessary" for the coordination of JTPA activities, and provide for such by rule, those records could be released under ORS 285.183(4)(e), but they could only be used for cross-matching by the DHR computer to the extent necessary for JTPA coordination.

Unless the EDD finds that all of the analyses desired by the SIS are "necessary" for JTPA purposes or "necessary" for JTPA coordination, ORS 285.183(4)(d), (e), information from JTPA participant records may not be released to the SIS without the consent of the participants. Despite any favorable findings that the EDD may make, the WQC may wish to seek an amendment to ORS 285.183 explicitly to permit the release of JTPA participants' records to the SIS.[14]

G. Adult and Family Services Division

1. Social Security Act Programs

AFSD administers several need-based programs that receive federal funding under the Social Security Act, e.g., Aid to Dependent Children (ACD),[15] Job Opportunities and Basic Skills Training (JOBS), Medicaid and refugee assistance programs. Because we understand that the SIS is interested primarily in records on JOBS participants and other ADC applicants and recipients,[16] and because the confidentiality provisions for each of the other AFSD programs are very similar to those for the ADC program, we have focused our analysis on the statutes and regulations for the ADC programs.

a. Federal law

---

[14] See note 9.

[15] Whereas Oregon statutes use the term "Aid to Dependent Children" (ADC), ORS 418.035 to 418,149, the Social Security Act uses the term "Aid to Families with Dependent Children" (AFDC), 42 USC §§ 601-687, for this same program. For ease of reference, we use the term ADC.

[16] In order to be a JOBS particicpant and receive JOBS services, an individual must be an ADC applicant or recipient. Most ADC applicants and recipients, however, are not JOBS participants.

The Social Security Act requires that states administering ADC programs

> provide safeguards which restrict the use or disclosure of information concerning applicants or recipients to purposes directly connected with (A) the administration of the plan of the State approved under this part [ADC] (including activities under part F [JOBS] of this subchapter), the plan or program of the State under part B {Child Welfare], D [Child Support] or E [Foster Care] of this subchapter, or under subchapter I [Old-Age Assistance], X [Aid to the Blind], XIV [Aid to Permanently and Totally Disabled], XVI [Supplemental Income Program], XIX [Medicaid], or XX [Black Grants] of this chapter, or the supplemental security income program established by subchapter XVI of this chapter, (B) any investigation, prosecution or criminal or civil proceeding, conducted in connection with the administration of any such plan or program, (C) the administration of any other Federal or federally assisted program which provides assistance, in cash or in kind, or services, directly to individuals on the basis of need, and (D) any audit or similar activity conducted in connection with the administration of any such plan or program by any governmental entity which is authorized by law to conduct such audit or activity, (E) reporting and providing information pursuant to paragraph (16) to appropriate authorities with respect to known or suspected child abuse or neglect; and the safeguards so provided shall prohibit disclosure, to any committee or legislative body * * *, of any information which identifies by name and address any such applicant or recipient; * * *.

42 USC § 602(a)(9) (Supp 1993).[17]

[17] The federal regulation implementing this statutory provision, 45 CFR § 205.50(a)(1)(i), also permits the use and disclosure of information cerning ADC applicants and recipients for "purposes directly connected with: & & & [t]he administration of a State unemployment compensation program." This regulation permits disclcosure of information from ADC records to ED for the purpose of administering the state's unemployment program. Such disclosure of information is mandated by 42 USC § 1320b-7, which requires states that operate ADC, food stamp, Medicaid, unemployment compensation or supplemental income programs to have an income and eligibility verification system (IEVS) to exchange information between those programs that "may be of use in establishing or verifying eligibility of benefit amounts." See 42 USC § 602(a)(25) (Supp 1993).

The IEVS statute requires the state to ensure that "the information exchanged by the State agencies is made available only to the extent necessary to assist in the valid administrative needs of the program receiving such information" and that the "information is adequately protected against unauthorized disclosure for other purposes." 42 USC 1320b-7(a)(5)(A)-(B) (West 1991) (emphasis added). This limitation on disclosure must be read into the ADC regulation that permits disclosure of ADC information to ED, since the authority for that regulation is the IEVS statute. Consequently, we conclude that any information concerning ADC applicants and recipients that AFSD provides to ED in conjunction with IEVS must be used solely for the "valid administrative needs" of the unemployment compensation program and that further disclosure or use for other purposes is prohibited.

We note, however, that an amendment to the IEVS statute is not necessary to ermit the disclosure to and use of ADC records by the SIS to the extent that we have determined in this opinion that AFSD may release that information to the SIS. Such releases would be made directly by AFSD to the SIS and would not involve information obtained via IEVS.

At first blush, the statute appears to be very restrictive. The literal terms of the statute restrict the "use or disclosure of information concerning applicants or recipients to purposes directly connected with" the administration of the ADC program (including its JOBS component) and other programs administered by AFSD[18]. This language could be interpreted to prohibit all uses and disclosures of client information contained in AFSD records except for purposes directly connected with the administration of the AFSD programs. The legislative history of this language, however, leads us to conclude Congress only intended to restrict uses or disclosures of client information that would embarrass or disadvantage particular individuals.

The confidentiality language was added to the Social Security Act in 1939 as part of a substantial overhaul of the Social Security system. The pertinent legislative history is sparse, but what exists supports the conclusion that Congress intended to prohibit only uses or disclosures of information that relate back to the particular individual applicant or recipient. The Social Security Board, then responsible for administering the Social Security Act, submitted a Report dated December 30, 1938, to the President recommending proposed changes to the Act. This Report was forwarded by the President to Congress and it provided a focal point for the 1939 amendments to the Social Security Act.

The Social Security Board's Report contained the following recommendation regarding the disclosure of confidential information:

> The Board recommends that State public assistance plans be required, as one of the conditions for the receipt of Federal grants, to include reasonable regulations governing the custody and use of its records, designed to protect their confidential character. The Board believes that such provision is necessary for efficient administration, and that it is also essential in order to protect beneficiaries against humiliation and exploitation such as resulted in some States where the public has had unrestricted access to official records. Efficient administration depends to a great extent upon enlisting the full cooperation of both applicants and other persons who are interviewed in relation to the establishment of eligibility; this cooperation can only be assured where there is

[18] The federal statutory confidentiality provisions for each of the other Social Security Act programs also permit the use of applicant and recipient reccords only for purposes "directly connected with the administration" of its own program. The federal Medicaid Act requires the state plan to "provide safeguards which restrict the use or disclosure of information concerning applicants and recipients to purposes directly conneced with the administration of the plan." 42 USC§ 139a(a)(7) (Supp 1993).

The federal confidentiality provisions for state old-age assistance, aid to the blind, aid to the permanently and totally dissabled and supplemental income programs were part of the same across-the-board enactment by Congress. See Pub L No. 92-603, § 413, 86 Stat 1329, 1492 (1972) (amending titles I, X, XIV, and XVI with identical language). These provisions require the respective state plans to "provide safeguards which permit the use or disclosure of information concerning applicants sor recipients only (A) to public officials who require such information in connection with their official duties, or (B) to other persons for purposes directly connected with the administration of the State plan." 42 USC§ 302(a)(7) (West 1991), § 1202(a)(9) (West 1991), § 1352(a)(9) (West 1991), and § 1382(a)(7) (West 1992).

> complete confidence that the information obtained will not be used in any way to embarrass the individual or jeopardize his interests. Similar considerations are involved in safeguarding the names and addresses of recipients and the amount of assistance they receive. Experience has proved that publication of this information does not serve the avowed purpose of deterring ineligible persons from applying for assistance. The public interest is amply safeguarded if this information is available to official bodies.

Report of the Social Security Board, HR Doc No. 110, 76th Cong, 1st Sess 22 (1939).

This report show that the Social Security Board was concerned primarily about protecting applicants and recipients from embarrassment or adverse actions against their particular individual interests. Thus, the Social Security Board was concerned about uses or disclosures of client information that could harm the particular applicant or recipient, not uses of applicant or recipient information for general programmatic planning purposes by state officials.

In fact, in his testimony before the House Committee on Ways and Means, Dr. Altmeyer, Chairman of the Social Security Board, stated that it was not the intent of the Board to restrict official uses of this information, but rather only to protect these records from indiscriminate use or publication for political purposes or other purposes totally unrelated to administration of public benefit laws. Dr Altmeyer stated :

> Well, we believe that they [applicant or recipient records] should be used only for official purposes; that they should be open, of course, to the officials charged with the direct administration of the law, available to the officials charged with the administration of other laws designed for the relief of the unemployed and destitute, generally<u>so that the cooperation between the various agencies would not be hampered</u>.

<u>Hearings Relative to the Security Act Amendments of 1939 Before the House Comm</u> on <u>Ways & Means</u>, 76th Cong, 1st Sess 2408 (1939) (Testimony of Dr. Arthur J. Altmeyer, Chairman, Social Security Board) (emphasis added.) Dr. Altmeyer further testified:

> There would be no thought, and there is no thought of restricting the official use of all of this information; and by "official" I mean not only the use by the States, but by these local officials that you mention. It is merely to protect these records against their indiscriminate use, for purposes not at all related to the administration of the law in question, or of companion laws.

<u>Id.</u> Dr. Altmeyer explained that the indiscriminate uses of concern included use of old-age assistance recipient lists by political candidates for campaign purposes and newspaper publication of the names of persons who received old-age assistance

simply to publicize the names as a matter of public interest. Therefore, he recommended that Congress set out in general terms the requirement that State plans include reasonable regulations governing the custody and use of applicant/recipient records. Id. at 2407-09.

Congress enacted the confidentiality provisions contained in the Social Security Act Amendments of 1939 with little further direct attention. The members of Congress were primarily concerned with other issues involved in the larger changes being made to the Social Security Act. See Social Security Act Amendments of 1939, HR Rep No. 728, 76th Cong, 1st Sess 77 (1939); S Rep No. 734, 76th Cong, 1st Sess 88-89 (1939). Thus, it appears from the available legislative history that Congress was presented with and considered only concerns about the indiscriminate publication or use of applicant/ recipient information for purposes of social stigma or political reasons when it enacted the confidentiality protections of the Social Security Act.

This legislative history supports the conclusion that Congress only intended to prohibit the disclosure or use of applicant/recipient information when that information can be related back to the particular applicant/recipient i.e., that the purpose of the confidentiality provisions is to protect the individual applicant/recipient, not to prevent programmatic or planning uses of information relating to applicant/recipient when that information will not be used to make decisions directly affecting individual.

This interpretation comports with the analysis given to those statutory provisions by courts. In Stivahtis v. Juras, 13 Or App 519, 511 P2d 421 (1973), the Oregon Court of Appeals determined that the purpose served by making welfare record confidential is to protect the welfare recipient from exploitation or embarrassment. In reaching this conclusion, the court addressed the confidentiality safeguards required by 42 USC § 602(a)(9) stating:

> The objective of the required safeguards has been variously described as " * * * the protection of applicants and recipients from exploitation and embarrassment," In re Cager, 251 Md 473, 482. 248, A2d 384 (1968); " * * * to save recipients from any embarrassment * * *," In re Will of Mellion, 58 Misc 2d 441, 295 NYS2d 822, 824 (1968) to prohibit " * * * any use of such records 'for commercial or political purposes,' Finance Committee of Falmouth v. Falmouth Board of Public Welfare, 345 Mass 579, 584, 188 NE2d 848, 852 (1963); Annotation, 165 ALR 1302, 1330-31 (1946).

13 Or App at 525 - 26. Thus, courts in Oregon and in other state jurisdictions also have determined that the federal confidentiality safeguards are intended to protect individual applicant/recipients from harm to their particular interests. The proposed operation of the SIS is designed to avoid all potential for any such harm to applicant/recipient particular interests.

In our discussion above, we noted the cross-matching performed by the DHR computer arguably would constitute a "use" of the client information involved, but that the "use" would be only by the computer itself and not by any persons, either DHR computer staff, SIS staff, participating agency staff or anyone else. Because individual client information would not be accessible to anyone, it would not be available for commercial, political or socially stigmatizing purposes. We further noted that the only "use" of this client information would be to produce aggregate statistical and demographic data; individual client information could not and would not be "used" in any way that would directly affect the individual client to whom the information relates. Rather, the cross-matching of the information within the computer at the direction of state officials would produce only aggregate data in order to facilitate the creation of strategies to improve the education, training and quality of Oregon's workforce, thereby relieving unemployment and destitution. Under these circumstances, we conclude that the brief, mechanical "disclosure" and "use" of client information involved in the cross-matching done by the DHR computer does not constitute the type of "disclosure" and "use" Congress intended to prohibit by enacting the Social Security Act confidentiality provisions.

Therefore, we conclude that the proposed SIS would not violate the federal Social Security Act confidentiality restrictions. Because this conclusion is not without some uncertainty, and in light of the substantial federal funds that would be jeopardized for violation of the federal law, we recommend that AFSD seek the concurrence of the Department of Health and Human Services in our conclusion.

b. State Law

The state statues relating to the confidentiality of records concerning ADC applicants and recipients (and, therefore, JOBS participants) are similar to the federal law. ORS 411.320 provides:

> For the protection of applicants for and recipients of public assistance, the Adult and Family Services Division and the county public welfare boards shall not disclose or use the contents of any records, files, papers or communications for purposes other than those directly connected with the administration of the public assistance laws of Oregon, and these records, files, papers, and communications are considered confidential * * *. In any judicial proceedings, except proceedings directly connected with the administration of public assistance laws, their contents are considered privileged communications.

ORS 418.130 similarly restricts the use and disclosure of information from ADC records only for "purposes directly connected with the administration of aid to dependent children * * *."[19]

[19] ORS 418.130, which applies to information concerning ADC applicants and recipients, provides:

In Stivahtis v. Juras, supra, 13 Or App at 523 - 24, the Oregon Court of Appeals determined that ORS 411.320 is expressly intended only to protect the individual applicant/recipient. The court further concluded that ORS 418.130 is also intended to protect the applicant/recipient. Id. After reviewing the language and legislative history of these state statutes, the court concluded that the Oregon legislature intended to bring state law into conformity with the federal statutory provisions discussed above. Id. at 524-26.

The proposed operation of the SIS would preclude the possibility that anyone could obtain access to any applicant or recipient information in a personally identifiable form. Consequently, there would be no opportunity for embarrassment or exploitation or any applicant or recipient. Furthermore, the proposed operation of the SIS also would ensure that no information in the SIS would be used to make any decisions or take any actions that directly affect any individual. These built-in structural safeguards lead us to conclude that the proposed SIS would not violate these state confidentiality protections.

However, our conclusion that the proposed operation of the SIS would not violate these provisions of state law is not completely free from doubt. We suggest, therefore, that the WQC attempt to eliminate any potential conflict with these state law provisions by seeking specific statutory authority for AFSD to provide the SIS with information from AFSD applicant/recipient records. As we have noted, House Bill 3617 in the current legislative session would authorize AFSD to provide the SIS with applicant/recipient information. However, in its current form HM 3617 appears to conflict with the applicable information between state agencies. See HB 3617, § 3 (1993). We recommend this provision be deleted from the proposed bill.

2. Food Stamps

The food stamp program is subject to confidentiality requirements that are very similar to those applicable to the ADC program. Federal law requires the state food stamp plan to contain "safeguards which limit the use or disclosure of information obtained from applicant households to persons directly connected with administration or enforcement of the provisions of this chapter, regulations issued pursuant to this chapter, Federal assistance programs, or federally assisted State programs," except for audits by the United States and investigations of alleged violations of the food stamp law or regulations. 7 USC § 2020(e)(8)(West 1988) (emphasis added).

No person shall, except for purposes directly connected with the administration of aid to dependent children ***solicit, disclose, receive, make use of, or authorize, knowingly permit, participate in, or acquiesce in the use of, any list of, or names of or any information concerning, persons applying for or receiving such aid, directly or indirectly derived from the records, papers, files or communications of the Adult and Family Services Division * * * or acquired in the course of the performance of official duties.

The federal food stamp regulations restrict the use or disclosure of information obtained from food stamp applicant or recipient households to persons directly connected with the administration or enforcement of the provisions of the Food Stamp Act or assistance on a means-tested basis to low income individuals, or general assistance programs which are subject to the joint processing requirements in 7 CFR § 273.2(j)(2)(public assistance, general assistance and categorically eligible household applications to be processed at the same time as food stamp applications.) 7 CFR §272.1(c)(1)(i).

These federal food stamp confidentiality provisions are functionally equivalent to the confidentiality requirements of the Social Security Act programs, using substantially the same terminology. Our review of the legislative history of these provisions has not disclosed anything to dissuade us from the conclusions that we reached regarding the Social Security Code Cong & Admin News 1704, 1704-2547. The only state statute concerning food stamp records is ORS 411.320, which we discussed above, concluding that it would not be violated by the proposed operation of the SIS. Accordingly, we conclude that AFSD may provide information obtained from food stamp applicant's or recipients' households to the SIS under the assumptions upon which this opinion are based without violating either federal or state food stamp confidentiality laws. Again, as an exercise of caution, we would advise the agency to seek confirmation that the federal Department of Agriculture agrees with out conclusion and to seek changes in state law that would explicitly permit the disclosure to and use of food stamp records by the SIS.

H. Employment Division

1. Unemployment Compensation and Employment Services

ED administers the unemployment compensation program and the employment service program for the State of Oregon. Oregon's unemployment compensation program is fundamentally a state program. However, if the state's program fails to meet the standards required by the Federal Unemployment Tax Act (FUTA), 26 USC §§ 3301-3311, the states employer's will lose the benefit of the FUTA tax credit. See generally Salem College & Academy v. Employment Division, 298 Or 471, 476-78, 695 P2d 25 (1985). Also, availability of federal funds for state employment services under the Wagner-Peyser Act depends on, among other things, the state's compliance with federal unemployment compensation laws.[20] 29 USC § 49d(b)(1) (Supp 1993).

Because failure of state law to conform to the federal requirements would cause employers in Oregon to lose the benefit of the FUTA tax credit and jeopardize the

[20] The state employment servivces plan also must be certified by the state job training coordinating counsel established under 29 USC §§ 1501-1781 as consistent with the Governor's coordination and special services plan under JTPA. 29 USC § 49g(b) (Supp 1993).

funding for the employment services program, we first address the applicable federal confidentiality restrictions.

Title III of the Social Security Act, 42 USC §§ 501-504, contains the federal requirements with which a state's unemployment compensation laws must comply. Unlike other titles of the Social Security Act, Title III contains no express mandate to safeguard the confidentiality of records, although there are some specific record-sharing requirements.[21] The employment service side of ED is governed by the Wagner-Peyser Act, 29 USC § 49-49n, which similarly lacks any statutory confidentiality requirement. The federal regulations only address the income and eligibility verification system requirements in 42 USC § 1320b-7, discussed at note 17, supra. 20 CFR Part 603 (1992). Currently, then, there are no comprehensive federal confidentiality restrictions.

Recently, however, the Department of Labor exercised its authority under 42 USC § 503(a)(1) and the Wagner-Peyser Act to promulgate comprehensive draft regulations on the subject of confidentiality of records. 57 Fed Reg 10064 (March 23, 1992) (to be codified at 20 CFR Part 603) (hereinafter "Proposed Regulations"). As Proposed Regulations, they are not binding on the states; but the drafters' commentary and the Proposed Regulations provide useful insight into the department's policy perspective on confidentiality that is relevant here.

The basic policy of confidentiality, is set out in the Proposed Regulations, for section 603.11 at 10066, states that the methods of administration must include provision for maintaining the absolute confidentiality of all information of whatever kind or form in the records of the state agency, subject to the mandatory disclosure requirements and those disclosures explicitly permitted by the terms of the proposed regulation. A key exception allows the disclosure of any information "to any public official * * * for use in the performance of such public official's duties, and for the purpose which does not involve administration or enforcement" of the state's unemployment compensation laws, provided that disclosed information is used solely in connection with a law being

[21] Federal law requires some specific kinds of information to be shared with other agencies. The state unemployment compensation agency must participate in the federal income and eligibility verification system (IEVS), 42 USC § 1320b-7; wage information may be disclosed to state or local child support enforcement agencies, 42 USC § 1320b-7; wage informatio may be disclosed to state or local child support enforcement agencies, 42 USC § 503(e); certain information may be disclosed to the food stamp program, 42 USC § 503(d); the state must provide information to the Secretary of Labor and to any federal agency charged with the administration of public works or assistance through employment, 42 USC § 503(a)(6), (7); and the state must disclose information to housing authorities, 42 USC § 503(I). Furthermore, 29 USC § 49c (the Wagner-Peyser Act) requires state unemployment insurance and employment service offices to furnish, upon request by the public agency administering or supervising administration of state plan approved under title IV-A (ADC), IV-D (SED) or the food stamp program, information as to (1) whether an individual has received or applied for unemployment compensation and the amount of compensation received, (2) the individual's home address, and (3) whether the individual has refused an offer of employment and information about any refused employment. See Proposed Regulations, 20 CFR §§ 603.100 to 603.105, and 603.110 to 603.115. However, each specific statute authorizing such disclosure is accompanied by a requirement that such information be used by the recipient only for the purpose it was disclosed.

administered or enforced by such public official. Proposed Regulations § 603.11(c)(1)(i), at 10068. This exemption is also limited by two conditions: disclosure of the specific information requested must be authorized by state law, Proposed Regulations, section 603.11(c)(I)(i)(A)(1), at 10069, and the state agency must determine that disclosure would not violate any other law of the state or significantly hinder or delay the efficient administration of the unemployment compensation laws. Id. § 603.11(c)(1)(i)(A)(2), at 10069. Moreover, funds received by the state under 42 USC § 502 (a) may not be used to pay any of the costs of making a disclosure under this exception, Proposed Regulations, section 603.12(2), at 10069, and the recipient of the information is required to safeguard the information against unauthorized redisclosure, Proposed Regulations, section 603.13, at 10070, and to enter into a written agreement with specified terms and conditions. Id. § 603.14, at 10071.

The state statutory provisions addressing the confidentiality of ED records appear to be consistent with the proposed federal requirements.[22] ORS 657.665(1)(a) sets out a general rule of confidentiality as follows:

> (1) Information secured from employing units, employees or other individuals pursuant to this chapter:
>
> (a) Shall be confidential and for the exclusive use and information of the assistant director in the discharge of duties and shall not be open to the public (other than to public employees in the performance of their public duties under state or federal laws for the payment of unemployment insurance benefits and to public employees in the performance of their public duties under the recognized compensation and retirement, relief of welfare laws of this state), except to the extent necessary for the presentation of a claim and except as required by [federal law].

(Emphasis added.) The provision restricting ED records "for the exclusive use and information of" ED would prevent this agency from being a contributing participant in the SIS. That is, the proposed functions of the SIS are to collect data from each of the participating agencies and, at the request of the WQC or a participating agency, to cross-match agencies' data to produce aggregate statistical and demographic data to assist the agencies in fostering the improvement of Oregon's workforce. Assumptions 2, 3, 5-7. The restrictions in ORS 657.665(1) on use of ED records would severely limit the agency's ability to transmit information to the DHR computer for cross-matching.

[22] The proposed federal regulations are not binding upon the state. If the regulations are adopted by the Department of Labor in their current form, we do not see any conflict with existing state statutes or with the proposed operation of the SIS. However, the proposed regulations may be revised prior to their adoption as final rgulations or may be given some further interpretation by the federal agency that would alter our assessment of the existence of a conflict.

However, ORS 657.665(3) provides an exception, analogous to the exception contained in the draft federal regulations, as follows:

> Notwithstanding subsection (1) of this section information secured from employing units pursuant to this chapter may be released to agencies of this state, and political subdivisions, acting alone or in concert in city, county, metropolitan, regional or state planning to the extent necessary to properly carry out governmental planning functions * * * . Information provided [to] such agencies shall be confidential and shall not be released by such agencies in any manner that would be identifiable as to individuals, claimants, employees or employing units. Costs of furnishing information pursuant to this subsection * * * shall be borne by the parties requesting the information.

(Emphasis added.) ORS 657.665(3) would authorize ED to release information from its records to the SIS for "planning" purposes, but only from information "secured from employing units."[23] Employing units must submit quarterly payroll data, pursuant to ORS 657.660, that identifies workers by social security number and reports the wages paid and weeks of work during the quarter. While ED may have additional information about employing units, ORS 657.665(3) only permits release of data obtained from employing units. Moreover, this subsection does not encompass information obtained from unemployment compensation applicants or recipients, or from any other sources. Thus, for example, even though ED may have a statement of benefit charges for each employer, indicating which former employees are receiving unemployment benefits, and even though an employing unit may be entitled to obtain that information from ED, that information is not "information secured from employing units," so it would not be available for use by the SIS pursuant to ORS 657.665(3).

Accordingly, the WQC may wish to seek an amendment to ORS 657.665 to permit disclosure of all information in ED records that would be useful to the SIS. Such an amendment would not appear to contravene the federal confidentiality policy set out in the proposed federal regulations.

We note that HB 3617, as drafted, would authorize the SIS participating agencies, including ED, to provide the SIS with information "relating to job training and education programs." HB 3617, § 2(1). However, this provision would not be broad enough to encompass all of the above-mentioned types of information possessed by ED about employing units, unemployment compensation applicants and recipients. We recommend that HB 3617 be amended to include an amendment to ORS 657.665 to authorize ED to provide the SIS with all relevant records[24] or, alternatively, that the

[23] Since ORS 657.665(3) would auathorize ED to release information from its records to the SIS for "planning" purposes, we believe this would permit the use of that information by the SIS as currently proposed.

[24] The proposed operation of the SIS is cocnsistent with the requirement in ORS 657.665(3) that information provided to governmental planning entities "shall not be released by such agencies in any manner that would

scope of HB 3617, section 2(1), be broadened to permit all SIS participating agencies, including ED, to provide the SIS with "information for the development of statistical and demographic data to facilitate the creation of strategies to improve the education, training and quality of Oregon's workforce."

While we conclude that the proposed operation of the SIS is not prohibited by state employment division law, ED's ability to participate in the SIS is limited by restrictions in current law. One of the conditions for disclosure of confidential information under the proposed federal regulations is that "[d]isclosure of the specific information requested in any case is authorized by the State law." Proposed Regulations § 603.11(c)(1)(i)(1), at 10068. The WQC, therefore, may wish to seek express legislative approval for disclosure of information by ED to the SIS. This legislation could be similar to the agency-specific authority contained in ORS 657.665(4) to (6), and (8) to (10), which permit disclosure to BOLI, Public Employes' Retirement System, Department of Revenue, Department of Insurance and Finance, and Construction Contractors Board, respectively.

2. Labor Statistics

ED also participates in the gathering of information from employers on behalf of the Bureau of Labor Statistics (Bureau) pursuant to a Cooperative Agreement between the state and the Bureau. The Cooperative Agreement mandates that state employment security agencies (SESAs) comply with the Bureau's policy on confidentiality:

> To safeguard statistical data, SESAs must comply with BLS Commissioner's Order 2-80, "Confidential Nature of Bureau Records," July 3, 1980, which explains the Bureaus policy on confidentiality: "In accordance with existing law and Departmental regulations, it is the policy of the Bureau of Labor Statistics that data collected or maintained by, or under the auspices of, the Bureau under the pledge of confidentiality shall be treated in a manner that will assure that individually identifiable data will be accessible only to authorized persons and will be used for statistical purposes or for other purposes made known in advance to the respondent. The protection of this information is essential because BLS statistical programs are built on the voluntary cooperation of respondents in providing the information.
>
> Confidential data include all identifiable respondent submissions and any other information in any medium and format that would disclose the identity

---

be identifiable as to individuals, claimants, employees or employing units." See Assumptions 2-8. We note that ORS 657.665(3) also contains a requirement that the costs of furnishing information to governmental planning entities "shall be borne by the parties requesting the information." This is consistent withe proposed federal regulations discussed above.

> of any participant in a statistical program under the auspices of BLS. This does not apply to Unemployment Insurance System data that are collected solely under State authority by the States and in the States' possession, used in the ES-202 program. * * * All data collected by the States as part of the ES-202 program under the sole or joint BLS authority, however, are covered by the BLS Commissioner's Order.
>
> To protect the data collected and maintained under the auspices of BLS, the SESA agrees that it shall:
>
> *****
>
> Assure that confidential data will not be divulged, published, reproduced, or otherwise disclosed orally or in writing, in whole or in part to any person, organization, or establishment, other than those needing such information to perform the work provided for in this Agreement and authorized by the Bureau***.

Fiscal Year 1992 Labor Market Information Cooperative Agreement, Bureau of Labor Statistics and Oregon State Employment Division, at I-10 through I-11 (emphasis added) (Cooperative Agreement). The Commissioner's Order 2-80 defines "individually identifiable data" as "all elements of information (including but not limited to names and addresses) which might identify participants in a statistical program."

The terms of the Commissioner's Order 2-80 and the Cooperative Agreement preclude the use of "individually identifiable" data collected by ED under the authority of the Bureau of Labor Statistics, unless informed consent has been received from the person or organization providing the information and the Commissioner of Labor Statistics authorizes the particular use of such information. In view of the Bureau's strong and broad policy on protecting the confidentiality of data collected on its behalf, it is questionable whether the cross-matching of such data by the SIS, even with the proposed confidentiality safeguards, would be permissible. This is because the data that is cross-matched is individually identifiable at the time the data match occurs -- if it were not, it could not be cross-matched. Accordingly, we recommend that the WQC seek an interpretation of the Commissioner concerning the applicability of Order 2-80 and the Cooperative Agreement to the proposed operation of the SIS.

I. Vocational Rehabilitation Division

VRD administers two distinct programs: rehabilitation services and disability determinations. We address each program separately.

1. Rehabilitation Services

States are eligible to receive federal funds for the delivery of vocational rehabilitation services only after detailed state plans are determined to conform to federal standards. 29 USC § 721 (West 1985 and Supp 1992). The federal vocational rehabilitation statutes do not contain express confidentiality provisions. Federal regulations, however, do set forth the standards of protection, use and release of personal information with which state plans must comply.

34 CFR § 361.49 provides in part:

> (a) General provisions. The State plan must assure that the State unit will adopt and implement policies and procedures to safeguard the confidentiality of all personal information, including photographs and lists of names. These policies and procedures must assure that:
>
> (1) Specific safeguards protect current and stored personal information;
>
> * * * * *
>
> (b) State program use. All personal information in the possession of the State agency or the designated State unit must be used only for purposes directly connected with the administration of the vocational rehabilitation program. Information containing identifiable personal information may not be shared with advisory or other bodies which do not have official responsibility for administration of the program. * * *

(Emphasis added.)

Although this regulation requires that "personal information" be used only for purposes directly connected with the administration of the vocational rehabilitation program, it further states that "information containing identifiable personal information" may not be shred with bodies that do not have official responsibility for administration of the program. 34 CFR § 361.49(b) (1992). We believe this distinction between the use of "personal information" and the sharing of "information containing identifiable personal information" to be significant.

The history of the regulation shows it was intended to protect the privacy rights of persons with disabilities, not be prohibit the use of information about such clients for general planning purposes. In 1979, the Department of Health, Education and Welfare (DHEW) proposed amendments to the then existing regulations to bring them into their current form. In proposing the amendments, DHEW stated:

> The revisions to this section have been made to bring about administrative consistency with the requirements of the Privacy Act and to deal with specific problems of information sharing which have been

> identified in recent years but which have not been resolved by the existing regulations. These revisions strengthen the safeguards for the rights of handicapped individuals to maintain the confidentiality of their personal information and emphasize the need for securing the consent of the individual before information may be released.

44 Fed Reg 68568 (1979). Thus, the changes in the regulations were motivated by a desire to protect the privacy rights of individuals with disabilities by limiting the "release" of personal information, not to prohibit all use of information about such clients.

When we analyze the proposed operation of the SIS in light of these regulations, we conclude that the safeguards that will be employed in the handling, transmittal and use of client information satisfy the regulatory requirements. First, as we noted above, the mere transmittal of encoded client information to the DHR computer would not involve a breach of privacy or confidentiality; the client information would not be accessible to anyone. Consequently, at this stage of the SIS process, there would be no release of any information.[25]

The second step of the proposed operation of the SIS, the cross-matching performed by the DHR computer, arguably would constitute a "use" of the client information. However, we conclude above that this mechanical "disclosure" and "use" of client information would not breach similar use restrictions contained in the Social Security Act because the only "disclosure" and "use" of the client information would be to produce aggregate statistical and demographic data. We also note that, under the proposed operation of the SIS, individual client information could not and would not be "used" in any way that would directly affect the individual client to whom the information relates. We adhere to that analysis here and conclude that the proposed computer cross-matching of client information by the SIS would not violate the requirement in 34 CFR § 361.49(b) that personal information "be used only for purposes directly connected with the administration of the vocational rehabilitation program."

Nor would this step of the proposed operation of the SIS violate the requirement in that same regulation that "[i]nformation containing identifiable personal information may not be shared with * * * bodies which do not have official responsibility for administration of the program." 34 CFR § 361.49(b) (1992). The encoded client information is not "identifiable" personal information. Even at the moment that information would be decoded and matched, no identifiable personal data would be "shared" with the SIS or the SIS participating agencies; it merely would be cross-matched within the computer to produce nonidentifiable, aggregate data.

---

[25] The federal regulation also addresses the permissible "release" of personal information for purposes of audit, evaluation and research, 34 CFR § 361.49(d), and the "release" of information to other programs or authorities. 34 CFR § 361.49(e). Because the proposed operation of the SIS does not involve the release of personal information, we do not analyze whether release of such information would be for a purpose that would significantly improve the quality of life of handicapped persons within the meaning of 34 CFR 361.49(d).

The final two steps in the operation of the SIS also would not violate the federal regulations. Computer reports of aggregate statistical and demographic data and any further disclosures of such aggregate data do not constitute the release of personal information prohibited by the provisions of 34 CFR § 361.49. The only information released at this stage would be aggregate, nonpersonal information.

It is possible that the Secretary of Education would not agree with our interpretation that the proposed operation of the SIS does not violate the proscriptions of 34 CFR § 361.49, since our interpretation of federal laws and regulations is not as authoritative as our interpretation of state law issues. Because the consequence of noncompliance with the federal regulations is significant -- loss of federal funding for VRD's vocational rehabilitation services -- we would advise the VRD to consult with the Department of Education to determine whether it agrees with our analysis, or, if necessary, whether an amendment or waiver of the federal regulations could be obtained.

State law also imposes confidentiality requirements on VRD records. ORS 344.600 provides:

> Except for purposes directly connected with the administration of vocational rehabilitation, and in accordance with the rules and regulations of the division, no person shall solicit, disclose, receive, make use of or authorize, knowingly permit, participate in or acquiesce in the use of, any list of or names of, or any information concerning persons applying for or receiving vocational rehabilitation directly or indirectly derived from the records, papers, files or communications of the state or subdivisions or agencies thereof, or acquired in the course of the performance of official duties.

This statutory language is virtually identical to the provisions of ORS 418.130 addressed above in relation to AFSD's participation in the proposed SIS. We conclude above, based upon our review of relevant case law and legislative history, that the proposed operation of the SIS would not violate the restrictions in ORS 418.130. We have found nothing in the legislative history of ORS 344.600 to persuade us that we should reach any other conclusion regarding this statute. Therefore, we conclude that the proposed operation of the SIS does not violate ORS 344.600.

This conclusion, like our conclusion regarding ORS 418.130, is not free from doubt. We recommend that the WQC seek specific statutory authority to allow VRD to provide the SIS with information from VRD applicant/recipient records. A blanket statute such as that proposed in HB 3617 would suffice. However, as drafted, HB 3617 presents potential conflicts with the federal requirements discussed above because it allows for the sharing of personally identifiable information between state

agencies. See HB 3617, § 3. We recommended that this provision be deleted from the proposed bill.[26]

2. Disability Determinations

States may make the disability determinations for the Social Security and Supplemental Security Income programs, subject to compliance with federal regulations. 42 USC § 421 (West 1991), § 1383 (e) (West 1992). The federal regulations for both of those programs require states to comply with the confidentiality requirements described in 20 CFR part 401. See 20 CFR § § 404.1631, 416.1931 (1993),

20 CFR § 401.310(a) permits a state disability determination unit to disclose information, without consent of the individual, to any other party for "routine uses."[27] "Routine use" means the disclosure of a record "for a purpose which is compatible with the purpose for which the record was collected." 20 CFR § 401.310(b) (1993) (emphasis in original). The Social Security Administration (SSA) considers other programs to be "compatible" when they

> have the same purposes as SSA programs if the information concerns eligibility, benefit amounts or other matters of benefit status in a social security program and is relevant to determining the same matters in the other program. For example, we disclose information to the Railroad Retirement Board for pension and unemployment compensation programs, to the Veterans Administration for its benefit program, to worker's compensation programs, to the Veterans Administration for its benefit program, to worker's compensation programs, to State general assistance programs, and to other income maintenance programs at all levels of government; we also disclose for health-maintenance programs like Medicare and Medicaid, and in appropriate cases, for epidemiological and similar research.

20 CFR § 401.310(c) (1993). Although the broader governmental purposes served by the SIS may not be deemed to fall reasonably within the scope of "routine uses" under this regulations, we conclude that the regulation does not prohibit the proposed operation of the SIS because there is no "use" inasmuch as no individual determination

[26] As drafted, HB 3617 would authorize the Sis participating agencies, including VRD, to provide the SIS with information "relating to job training and education programs." HB 3617 § 2(1). In light of the information that we understand would be of interest to the SIS, we also recommend that the scope of this provision in HB 3617 be broadened to authorize the agencies to provide the SIS with "information for the development of statistical and demographic data to facilitate the creation of strategies to improve the education, training and quality of Oregon's workforce."

[27] This regulation is based upon the Privacy Act of 1974. 5 USC § 552a. That Act affects federal agencies and geneerally is not drectly applicable to a state or state agency. When a state agency acts as an agent of the Social Security Administration for purposes of making disability determinations, however, the Privacy Act becomes applicable to that state agency's disability determinations unit.

of eligibility, benefit amount, etc. will be made. The proposed operation of the SIS also does not involve a prohibited disclosure.

20 CFR § 401.325 permits the disclosure of information for statistical and research purposes, distinguishing between personally identifiable and nonpersonally identifiable information. Records may be released "if there are safeguards that the record will be used solely as a statistical or research record and the individual cannot be identified from any information in the record." 20 CFR § 401.325(a)(1993) (emphasis added).

We believe the confidentiality safeguards that would be employed in the transmittal, handling and use of client information under the proposed operation of the SIS would satisfy the requirements of 20 CFR § 401.325(a). Each SIS participating agency would transmit client information to the DHR computer in an encoded form. The individual could not be identified from any of the transmitted information except the encoded social security number. However, only the DHR computer staff would have access to the decoding formulae, and they would not have access to client information. Rather, the DHR computer staff would program the computer with the decoding formulae so that the individual's social security number could be decoded for purposes of performing data matches. Only the computer would "see" the client information being matched. The computer would simply cross-match information provided by two or more of the participating agencies to produce aggregate statistical and demographic data. As soon as the data match was completed, the computer would immediately re-encode the client social security numbers. The computer would not reveal to anyone any client information. No such information would be available to be used in any way to make any decisions directly affecting an individual. Under these circumstances, no individual could be identified by anyone from any information that would be transmitted by VRD to the DHR computer.[28]

Accordingly, we conclude that the proposed operation of the SIS is consistent with 20 CFR § 401.325(a). The WQC may wish to seek the Social Security Administration's concurrence with this conclusion.

J. Educational Institutions

Because the confidentiality requirements for student records maintained by the educational institutions under OSSHE, OCCS and ODE are similar, our discussion in this section covers all three of those participating agencies. We address the federal statutes and regulations first and then the state statutes for each agency.

[28] Because the proposed operation of the SIS does not involve the release of identifiable personal information, we do not analyze whether the release of such information would be permissible under 20 CFR § 401.325(b), which applies to the release of personally identifiable information.

1. Federal law

The Family Educational Rights and Privacy Act (FERPA), 20 USC § 1232g, governs the release of student records for all educational institutions or agencies to which funds have been made available by the Secretary of Education. This includes virtually all educational institutions within the state, including those institutions within the purview of OSSHE, OCCS and ODE.[29]

The enforcement mechanism contained in FERPA is monetary -- no federal funds shall be made available to any educational agencies or institutions that have policies regarding the release of education records that violate its proscriptions. 20 USC § 1232g(b)(1)(West 1990). The provisions of FERPA do not create private rights enforceable by individual students or student family members. Fay v. South Colonie Cent. School Dist., 802 F2d 21 (2d Cir 1986). The potential penalty of loss of federal funding, however, is of such substantial magnitude that the educational institutions participating in SIS would be well served to ensure that the Secretary concurs with our conclusions that encoded student record information may be transmitted to the DHR computer, cross-matched with other data and compiled in aggregate, statistical reports by the SIS. We have previously stated that when we engage in interpretations of FERPA and the federal regulations promulgated thereunder, our interpretation is not as authoritative as our interpretation of state law issues. See Letter of Advice dated November 1, 1984, to Gerald G. Johnson, Technical Services Section Manager, Children's Services Division (OP-5642). While we believe our interpretation of the federal law is correct, the conclusions set out below must be read with this caveat in mind.

FERPA generally prohibits the release of personally identifiable information from student records without consent from the student or the student's parents.[30] 20 USC § 1232g(b) provides, in pertinent part:

---

[29] We understand that OCCS and ODE do not maintain student records, but may provide direction to the educational institutions regarding the release of such records.

[30] 20 USC § 1232g(b)(1)(F) does provide an exception to the federal prohibition against the release of personally identifiable information from student records. It allows educational institutions to disclose personally identifiable information from educational reocrds to:

> organizations cocnducting studies for, or on behalf of, educational agencies or institutions for the purpose of devleoping, validating, or administering predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations and such information will be destroyed when no longer needed for the purpose for which it is conducted[.] We conclude, however, that the operation of the SIS does not fit within this exception. The purpose of the SIS is to cross-match client information in order to generate reports of aggregate data for the WQC to facilitate the WQC's development and coordination of education and training programs for Oregon's workforce and for the participating agencies, including the non-educational agencies, to facilitate their program planning, performance evaluation and provision of services. The operation of the SIS, therefore, serves purposes that are unrelated to

(1) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information, as defined in paragraph (5) of subsection (a) of the section) of students without the written consent of their parents to any individual, agency, or organization * * *

(2) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information, or as is permitted under paragraph (1) of the subsection unless --

(A) there is written consent from the student's parents specifying records to be released * * *, or

(B) such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena * * * .

These provisions are less than clear. On the one hand, they can be read broadly to prohibit the release of all information contained in education records, with a particular emphasis on prohibiting the release of personally identifiable information in those records. On the other hand, they can be read more narrowly to prohibit only the release of personally identifiable student records or personally identifiable information contained in those records.

The legislative history of FERPA supports the more narrow reading. These confidentiality provisions were enacted as part of the Buckley/Pell Amendment to FERPA. The Joint Statement in Explanation of the Buckley/Pell Amendment explained its purpose and the meaning of the term "education records" as follows:

The purpose of [FERPA] is two-fold - to assure parents of students, and students themselves if they are over the age of 18 or attending an institution or [sic] postsecondary education, access to their education records and to protect such individuals' rights to privacy by limiting the transferability of their records without their consent.

* * * * *

* * * "Education records" are described as those records, files, documents, and other materials directly related to a student which are maintained by a school or by

---

developing predictive educational tests, administering student aid programs or improving educational instruction.

> one of its agents. This definition is a key element in the amendment. An individual should be able to know, review, and challenge all information - with certain limited exceptions - that an institution keeps on him, particularly when the institution may make important decisions affecting his future, or may transmit such personal information to parties outside the institution.

Joint Statement in Explanation of the Buckley/Pell Amendment, S Res 40, 93d Cong, 2d Sess, 120 Cong Rec 39859, 39862 (1974) (emphasis added).

This legislative history shows that Congress intended the disclosure restrictions relating to student records to protect the individual privacy interests of students and their parents. Those privacy interests are not affected by the transmittal of student record information that cannot be related back to the individual student.

The Joint Statement further noted that the then existing provisions of FERPA restricted only the transfer of personally identifiable information concerning a student.

> Section 438(b)(1) of existing law restricts transfer, without the consent of parents of students, of personally identifiable information concerning a student to other educational agencies or institutions, other school officials, auditors from the General Accounting Office and the Department of Health, Education, and Welfare, and in connection with the application for or receipt of student financial aid under certain specified conditions. It has become apparent in the last several months that these restrictions are too narrow and, if strictly applied, would seriously interfere in the operation of educational institutions. Therefore, after consultation with numerous educational representative as well as students, the authors of these amendments have included a series of other potential recipients of student information, without the necessity of securing individual parents' consent.

120 Cong Rec at 39863 (emphasis added). Thus, the Buckley/Pell Amendment was intended to broaden the number of parties to whom personally identifiable student information could be transferred without first obtaining consent from the student or the student's parents. It would be anomalous to believe that the Buckley/Pell Amendment actually made student record information less available by broadening the disclosure prohibition to preclude the transfer of all information contained in education records without prior consent. Therefore, we conclude that FERPA prohibits only the disclosure of personally identifiable information from student records without prior consent.

This interpretation is also consistent with the federal regulations promulgated by the Secretary of Education pursuant to FERPA. 34 CFR § 99.30(a) provides:

> Except as provided in § 99.31, an educational agency or institution shall obtain a signed and dated written consent of a parent of an eligible student before it discloses personally identifiable information from the student's education records.

(Emphasis added.) 34 CFR § 99.31 sets out several exceptions to the general prohibition against disclosure of personally identifiable information that parallel the exceptions in FERPA. See 34 CFR § 99.31 (1993); 20 USC § 1232g(b)(1) and (2) (West 1990).

The federal regulations are addressed solely to disclosures of personally identifiable information from student records. 34 CFR § 99.3 defines "[p]ersonally identifiable information," in pertinent part, as including but not limited to:

> (a) The student's name;
>
> * * * * *
>
> (d) A personal identifier, such as the student's social security number or student number;
>
> (e) A list of personal characteristics that would make the student's identity easily traceable; or
>
> (f) Other information that would make the student's identity easily traceable.

Based upon the legislative history of FERPA and the federal regulations promulgated thereunder, we conclude that FERPA precludes only the disclosure of personally identifiable information from student records. We now discuss how this applies to the proposed operation of the SIS.

Above, we concluded that no privacy or confidentiality interests would be implicated when a participating agency merely transmits encoded client information to the DHR computer, because the DHR computer is analogous to an agent of the participating agency. We adhere to that analysis here and conclude that educational institutions would not violate FERPA by transmitting student record information to the DHR computer. The student information would not be accessible to anyone at that point.

The computer cross-matching of student record information also would not constitute a release, transmittal or disclosure of personally identifiable information. Although the DHR computer would decode the students' social security numbers to cross-match information, no one would be able to gain access to any personally identifiable information before that identifier again would be encoded. Nor would anyone be able to link the encoded social security number, or any information attached to that encoded identifier, to any particular individual. Consequently, there would be no

disclosure of personal information or personal identifiers because no one could use the encoded identifier to determine the student's identity.

The broad definition of disclosure contained in the federal regulations does not change our conclusion. 34 CFR § 99.3 provides:

> Disclosure means to permit access to or the release, transfer, or other communication of education records, or the personally identifiable [sic] information contained in those records, to any party, by any means, including oral, written, or electronic means.

We concluded above that, as used in FERPA, the term "education records" means records that are personally identifiable and can be related back to a particular student. Because regulations must be interpreted consistent with the status they implement, we give the same meaning to the term "education records" in this regulation.

The proposed operation of the SIS would not "permit access to or the release, transfer, or other communication of" any student record information in a personally identifiable form by any "party.' Only the DHR computer would have access to the encoded records. The only information released, transferred or communicated from the DHR computer would be to the SIS and that would be only in an aggregated, nonpersonally identifiable form. And, the SIS's reports to the WQC, the participating agencies and other entities necessarily would consist only of aggregate statistical and demographic data that cannot be related back to any individual.

Accordingly, we conclude that the operation of the SIS would not involve the disclosure of "education records" or the personally identifiable information contained in those records. The proposed operation of the SIS would not violate FERPA's confidentiality provisions. However, we would advise the educational institution participating in the SIS to consult with the Department of Education to determine whether it agrees with our conclusion.

2. State Law

FERPA sets out the minimum standards that states and state educational agencies must meet regarding disclosures of student records; but states may be more restrictive. See Joint Statement in Explanation of the Buckley/Pell Amendment, supra, 120 Cong Rec 39862 (1974). Although Oregon law is more restrictive in some particulars than FERPA, for the reasons set out below, we conclude that the state statutes relating to the disclosure of student records would not impede the proposed operation of the SIS.[31] Therefore, the WQC need not necessarily seek an

[31] HB 2062 is pending before the legislature. This bill directs the state Board of Education and the State Baord of Higher Education to adopt rules regarding student records that are consistent with the requirements of "applicable federal and state law." HB 2062, § 3 (1993).

amendment to any of these statutes to allow the use of student record information for the proposed operation of the SIS to the fullest extent permitted under federal law, though we encourage the WQC to seek explicit statutory authority for educational institutions to provide information to the SIS in order to eliminate all doubt.

a. Higher Education Institutions

Access to student records for the educational institutions under OSSHE is governed by ORS 351.070. ORS 351.070(2)(e) provides that the State Board of Higher Education may, for each institution under its control,

> adopt rules relating to the use of and access to student records of the institutions * * * . However, except for directory information, records containing information kept by the institution, division or department concerning a student and furnished by the student or by the institution, division or department, including, but not limited to, information concerning discipline, counseling, membership activity, academic performance or other personal matters, shall not be available to public inspection or disclosure for any purpose except with the written consent of the student who is the subject of the record or upon order of a court of competent jurisdiction or, in an emergency, to appropriate persons if such information is necessary to protect the health or safety of the student or other persons. Nothing contained in this paragraph prohibits authorization of the inspection of such records by institution officials or employees who have a legitimate educational interest in inspecting student records, or by any representative of a state or federal governmental agency that is required by law to inspect student records.

(Emphasis added.)

We previously have noted that the 1979 Legislative Assembly adopted ORS 351.070 to bring Oregon law into conformance with the federal law governing student records. See Letter of Advice dated October 1, 1982, to Richard S. Jones, Executive Secretary, Teachers Standards and Practices Commission (OP-5239). It is reasonable to conclude, therefore, that the Oregon legislature intended ORS 351.070(2)(e) generally to authorize access to student records if the access does not involve "public inspection or disclosure" and is otherwise permissible under FERPA.[32] We conclude above that the proposed operation of the SIS would not involve any release, transmittal or disclosure of personally identifiable student record information in violation of the confidentiality provisions of FERPA. For those same reasons, we now conclude that the operation of the SIS does not involve public inspections or disclosures of records

[32] We note that ORS 351.070(2) sets out a prohibition against the disclosure of student records that is broader than that in FERPA. Although FERPA contains an exception allowing educational institutions to disclose student records to organizations conductinng stuides designed to improve instruction, 20 USC § 1232g(b)(1)(F), there is no analogous exception in ORS 351.070(2). This discrepancy, however, does not change the result of our analysis.

concerning a student that would violate the provisions of ORS 351.070(2).[33] The operating assumptions of the SIS would ensure that no public inspection or disclosure of any student record information relating to any identifiable student would occur.

Because this conclusion is not free from all doubt, however, we recommend that the WQC seek enactment of a statute that would explicitly allow the state's higher education institutions to provide the SIS with student record information. See note 9, supra.

b. Community College Institutions

Access to student records maintained by community colleges is governed by ORS 341.290. ORS 31.290(17)(a) provides that the board of education of a community college district may:

> Prescribe rules for the use and access to public records of the district that are consistent with ORS 192.420. However, the following records shall not be made available to public inspection for any purpose except with the consent of the person who is the subject of the record, student or faculty, or upon order of a court of competent jurisdiction:
>
> (a) Student records relating to matters such as grades, conduct, personal and academic evaluations, results of psychometric testing, disciplinary actions, if any, an other personal matters.
>
> (Emphasis added.)

ORS 341.290(17) prohibits "public inspection" of community college student records. As noted above in our discussion of prevailing wage rate information obtained by BOLI, the operation of the SIS would not involve the "public inspection" of any records. Consequently, we conclude that ORS 341.290(17)(a) would not create any additional barriers to providing community college student records to the SIS beyond the FERPA restrictions, and no changes to this statute would be required to permit the operation of the SIS. Notwithstanding this interpretation of the confidentiality provisions in ORS 341.290(17), the WQC may wish to seek amendment of this statutory provision explicitly to permit community colleges to provide student record information to the SIS. See not 9, supra.

ORS 341.290(17) would authorize Oregon's community colleges to promulgate administrative rules providing for reporting student record information to the SIS. We

[33] This conclusion does not mean that disclosure of personally identifiable information about a student for educational research purposes is permissible under ORS 352.070(2); rather, the conclusion is limited to research conducted under the assumptions for the proposed operation of the SIS upon which this opinion is based.

caution, however, that the community colleges cannot establish disclosure policies in their rules that violate the FERPA restrictions without subjecting themselves to the possible loss of federal funding.[34]

c. School Districts

Access to student records maintained by elementary schools, secondary schools, educational institutions and education service districts is governed by ORS 336.185 to 336.215. ORS 336.195(1) provides:

> All student records maintained by a school, educational institution or education service district shall be confidential, and except as hereinafter provided shall be open for inspection only in accordance with such rules as the board shall adopt

(Emphasis added.)

This statute makes "confidential" all student records maintained by elementary schools, secondary schools, educational institutions and education service districts. We concluded above that providing student record information to the SIS, under the assumptions upon which this opinion is based, would not constitute a disclosure that would violate the student's right to confidentiality. Under the proposed operation of the SIS, no one would have access to any individual student's records. Consequently, the fact that ORS 336.195(1) makes student records "confidential" would not preclude school districts from providing student record information to the SIS.

However, the statute also restricts inspection of student records. While the computer cross-matching to be performed by the DHR computer arguably would involve "inspection" of student records by the computer, no person would have access to or be able to see any student records at any time in the process. Such a mechanical "inspection" by the computer (with no possibility of "inspection" by any human) does not involve any breach of confidentiality that we perceive to be protected by ORS 336.195(1). Therefore, we conclude that the computer cross-matching of data does not violate the terms of the statute. Furthermore, we note that ORS 336.195(1) also contains the explicit proviso that the confidentiality of these student records is circumscribed by "such [inspection] rules as the [school] board shall adopt." This language appears to empower each local school board to determine the limits of the

[34] ORS 341.290(17) does not contain any affirmative requirements regarding disclcosures of student records that would violate FERPA's restrictions. ORS 341.290(17) requires community colleges to prescribe rules for access to records that are consistent with ORS 192.420, which incorporates the disclosure and exemption provisions of Oregon's Public Records Law. While the Public Records Law establishes a general rule requiring disclosure of all public records, ORS 192.502(7) expressly exempts from disclosure:

> Any public records or information the disclosure of which is prohibited by federa law or regulations[.]

Thus, ORS 341.290(17) does not require disclosures of records that are prohibited by federal law, including FERPA.

confidentiality of its students' records by promulgating administrative rules that could allow for such a mechanical "inspection". Again, however, we caution that local school boards cannot establish disclosure policies in their rules that violate the FERPA restrictions without subjecting themselves to the possible loss of federal funding.

Thus, the literal language of this statute already appears to enable local school districts to participate in the SIS to the fullest extent permitted under federal law. Consequently, we do not believe that any changes to existing state law are necessary to allow Oregon's school districts to participate in the proposed SIS. In order to eliminate any doubt about this conclusion, however, we again recommend that the WQC seek enactment of a state statute that would explicitly permit school districts to provide the SIS with information from students records. See note, 9 supra. The WQC also should encourage the state's school districts to promulgate consistent administrative rules enunciating appropriate policies for school districts to follow in their participation in the SIS. This will ensure consistency between school districts and will avoid any potential litigation about the need for prior rulemaking to establish such policies.

K. Recommendations

Although we have concluded that, except for certain JTPA and ED records, the SIS participating agencies' transmittal of encoded client information to the DHR computer, and the computer's cross-matching of that information to produce aggregate statistical and demographic data for the SIS, would not violate the disclosure or confidentiality provisions of the relevant privacy and confidentiality laws, these are close questions, and our conclusions are not free of uncertainty. Several federal confidentiality statutes and regulations, and state statues, restrict access or use of client information to purposes "directly connected with the administration" of the agency's programs. These laws pose the closest question of interpretation, requiring us to rely on legislative history that could be interpreted differently by the federal agencies responsible for administration of the programs or by a court. Accordingly, to the extent the WQC wishes to proceed with the proposed operation of the SIS, we recommend that the WQC and the participating agencies take the following action to remove possible statutory and administrative barriers and eliminate legal uncertainties:

1. The WQC and participating agencies should seek state legislative action to amend existing confidentiality laws to expressly authorize the SIS participating agencies to release client information to the SIS for cross-matching to produce aggregate statistical and demographic data for the WQC. We recommend that such state legislation consist of:

(a) a blanket statute authorizing specified state agencies to release client information from their records for the operation of the SIS[35], and/or

[35] See note 9.

(b) amendments to each of the separate confidentiality statutes discussed above that currently restrict the disclosure, release or use of agency records, to explicitly permit or require, as appropriate, the release of client information from those records for the operation of the SIS.

2. In a few instances in this opinion, we have recommended that the WQC and SIS participating agencies seek confirmation from federal agencies that the proposed operation of the SIS would not contravene restrictions on disclosure, release or use of agency records or information under the federal confidentiality statutes and regulations. When we engage in interpretations of federal statutes and regulations, our interpretation is not as authoritative as our interpretation of state law issues. While we believe our interpretation of the federal law in this opinion is correct, the potential penalty of loss of federal funding for violation of any of those laws is sufficiently significant that the affected participating agencies would be well served to ensure that the appropriate federal agency concurs with our conclusions that the proposed operation of the SIS will not violate the federal statutes or regulations. Where those statutes or regulations, on their face, may be interpreted to prohibit the use of client records in the proposed operation of the SIS, only a federal regulation or other binding pronouncement from the appropriate federal agency(ies) authorizing such use can entirely remove the risk of the federal disallowance of funds.[36]

If a federal agency advises the WQC that the proposed operation of the SIS would contravene a federal statute or regulation, the affected SIS participating agencies will need to obtain written, informed consent from the individual clients or students before releasing client information for the operation of the SIS.[37]

---

[36] The federal government cannot be estopped by reliance on a representation by a federal official that is contrary to a published regulation, let alone a statute. See Federal Crop Insurance Corp. v. Merrill, 332 US 380, 68 Ct 1, 92 L Ed 10 (1947), see also Office of Personnel Management v. Richmond, 496 US 414, 110 S Ct 2465, 110 L Ed2d 387 (1990).

[37] This opinion addresses federal statutes and regulations and state statutes that would prohibit or restrict the disclosure, release or use of agency records. There are two other areas of consideration: tort and contract.

Any nonconsenual disclosure, release or use of sensitive, personal information could give rise to a variety of tort actions. Although "unreasonable invasion of privacy" is not a tort in Oregon at the present time, Jordan v. MVD, 308 Or 422, 446 n 2, 781 P2d 1203 (1989), several related theories remain viable, such as breach of cocnfidence, wrongful appropriation of property or intentional infliction of mental or emotional distress. See Anderson v. Fisher Broadcasting Co., 300 Or 452, 712 P2d 803 (1986); see also Humphers v. First Interstate Bank, 298 Or 706, 717-21, 696 P2d 527 (1985) (person or government agency that discloses confidential information in violation of a statutory, contractual or other legal duty of cocnfidentiality may be held liable for a wrongful breach of confidence). If the participating agency has obtained informed consent from the individual for disclosure, release and use of personal information for the stated purposes of the SIS, or statutes specifically authorize such a release or use of information, the agency should not be liable in tort for the crosss-matching of that information b the SIS or the DHR computer.

A nonconcensensual disclosure, release or use of information that was obtained under an agreement or commitment that the information would be held in confidence could constitute a breach of the agreement, and give rise to an action in contract. Before disclosing, releasing or usinng such "confidential" information for the operation of the SIS, a participating agency may need to obtain informed consent or to amend the

Alternatively, the WQC would be required to seek federal waivers in order to implement the Workforce Quality Act. See OR Laws 1991, ch 667, § 14.

III. Use of Social Security Numbers as Personal Identifiers when Providing Information to the SIS

A. Relevant Statutes

Public concern about the invasion of privacy associated with social security numbers prompted Congress to enact the Privacy Act of 1974. 5 USC § 552a (West 1977). Section 7 of the Act provides:

> (a)(1) It shall be unlawful for any Federal, State or local government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.
>
> (2) the provisions of paragraph (1) of this subsection shall not apply with respect to --
>
> (A) any disclosure which is required by Federal statute, or
>
> (B) the disclosure of a social security number to any Federal, State or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual
>
> (b) Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Pub L No. 93-579, § 7, 88 State 1896, 1909 (1974) (reprinted in 5 USC § 552a note) (emphasis added) (hereinafter referred to as "section 7 of the Privacy Act").

---

agreement, depending upon the nature of the agreement or commitment. A statute that authorizes, but does not require, disclosure, release or use of such information for the operation of the SIS may not be sufficient to aboid a breach of agreement. Moreover, a statute that requires disclosure, release or use of information for the SIS is likely to be effective only as to agreements entered into after the effective date of the statute.

The actual likelihood of tort or contract liability would depend upon the content of the records disclosed or released, and the extent of the disclosure and use, and is beyond the scope of this opinion. The participating agencies should consult their contract attorneys.

In 1976, the Social Security Act was amended to expand upon the states' authority to require the disclosure of, and to use, social security number as follows:

> (1) It is the policy of the United States that any State (or political subdivision thereof) may, in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction, utilize the social security numbers issued by the Secretary for the purpose of establishing the identification of individuals affected by such law, and may require any individual who is or appears to be so affected to furnish to such State (or political subdivision thereof) or any agency thereof having administrative responsibility for the law involved, the social security account number * * * issued to him by the Secretary.
>
> * * * * *
>
> (v) For purposes of clause (I) of this subparagraph an agency of a State (or political subdivision thereof) charged with the administration of any general public assistance, driver's license, or motor vehicle registration law which did not use the social security account number for identification under a law or regulation adopted before January 1, 1975, may require an individual to disclose his or her social security number to such agency solely for the purpose of administering [such] laws * * * and for the purpose of responding to requests for information from an agency operating pursuant to the provisions of a part A [ADC] or D [Child Support] of subchapter IV of this chapter.

42 USC 405 (c)(2)(I)(v)(Supp 1993), (emphasis added); see also HR Con Rep No. 1515, 94th Cong, 2d Sess 490-91, reprinted in 1976 US Code Cong & Admin News 2897, 4194-95.

In 1990, the Social Security Act was amended further to tighten the requirements for use of social security numbers by government officials. This amendment provides, in part:

> (I) Social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number or related record.
>
> * * * *
>
> (III) For purposes of this clause, the term "authorized person" means an officer or employee of the United States, an officer or employee of any

State, political subdivision of a State, or agency of a State or political subdivision of a State,and any other person(or officer or employee thereof), who has or had access to social security account numbers or related records pursuant to any provision of law enacted on or after October 1, 1990For purposes of their subclause, the term "officer or employee" includes a former officer or employee.

(IV) For purposes of this clause, the term "related record" means any record, list, or compilation that indicates, directly or indirectly, the identity of any individual with respect to whom a social security account number is maintained pursuant to this clause.

Pub L No. 101-624, 1735(b), 104 State 3359, 3792 (1990) (codified as 42 USC 405 (c)(2)(C)(vii)(emphasis added (hereafter referred to as the "1990 amendment").

B. Application to the SIS and the Participating Agencies

We note first that the law governing the confidentiality of agency records, discussed in Part II above, is not made any less restrictive by the statutes pertaining to social security numbers. For example, if the law governing VRD restricts the use or disclosure of its records to purposes directly connected to the administration of the vocational rehabilitation program, section 7 of the Privacy Act does not expand that agency's authority to disclose records for other purposes merely by providing their section 7(b) notice of the uses to be made of the number.

Each agency must continue to operate within its legal authority and restrictions with regard to the disclosure of personally identifiable client information, including social security numbers. Where the statutes concerning the disclosure and use of social security numbers are more restrictive, however, those statutes will control. For example, if no federal or state law restricts the disclosure of ODOC records, and those records contain social security numbers, ODOC would nonetheless have to comply with the federal statutes governing the disclosure and use of the social security number within those otherwise disclosable records. Department of Veterans' Affairs (OP-5300) (social security number on record does not exempt entire document from disclosure, but requires deletion of number from non-exempt portion of record).

1. Mandatory and Voluntary Disclosures

Acknowledging the widespread use of social security numbers, Congress intended the Privacy Act to curtail their use by federal and state agencies and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiersSee Doyle v. Wilson, 529 F Supp 1343, 1348 (D Del 1982) (quoting legislative history). The Senate report notes the conclusions of a committee formed by the Secretary of Health, Education and Welfare

(now Health and Human Services), which oversees the Social Security Administration, as follows:

> If the SSN [social security number] is to be stopped from becoming a de facto Standard Universal Identifier, the individual must have the option not to disclose his number unless required to do so by the Federal Government for legitimate Federal program purposes, and there must be legal authority for his refusal. Since existing law offers no such clear authority, we recommend specific, preemptive, Federal legislation providing that the individual has the right to refuse to disclose his SSN to any person or organization that does not have specific authority provided by Federal statute to request it. . . and the right to redress if his lawful refusal to disclose his SSN results in the denial of a benefit.

S Rep No. 1183, 93d Cong, 2d Sess, reprinted in 1974 US Code cong & Admin News 6916, 6945. Thus, a clear distinction was drawn between mandatory disclosure required or authorized by federal law and voluntary disclosure which can be refused without penalty and carries with it a right to redress if a lawful refusal results in a denial of a benefit.

A state agency may require a client to disclose his or her social security number only if:

1. A federal statute requires disclosure (Privacy Act § 7(a)(2)(A));
2. A federal or state statute or regulation adopted prior to January 1, 1975, requires disclosure to an agency maintaining a system of records in existence and operating before that date, in order to verify identity (Privacy Act § 7(a)(2)(B)0; or
3. Disclosure is required to establish the identification of individuals for purposes of administering any state tax, general public assistance, driver's license or motor vehicle registration law (42 USC § 405(c)(2)(C)(i), (v) (Supp 1993)).

The clients of the participating agencies may not be required to disclose their social security numbers to the participating agencies for use in the operation of the SIS under any of these authorized mandatory disclosure categories. No federal law authorizes the SIS, much less requires the disclosure of social security numbers for purposes of the SIS; the SIS and its proposed system of records were not in existence before January 1, 1975; and the administration needs of the state's tax, general public assistance, driver's license or motor vehicle registration laws are much narrower and more restricted than the broader governmental purposes of the SIS.

Of course, some of the participating agencies already have their clients' social security numbers under the authority of one of the mandatory disclosure provisions, e.g., AFSD. We do not believe that the use of an individual's social security number for purposes of the SIS is an authorized extension of that same mandatory disclosure.

Therefore, any disclosures by clients of their social security numbers for use in the operation of the SIS must be voluntary.

2. Notice of/Consent to Intended Uses

Whether the client's disclosure of his or her social security number is mandatory or voluntary, a government agency must comply with the requirements of section 7(b) of the Privacy Act. This section requires any federal, state or local government agency that requests an individual to disclose his or her social security number to inform that individual: 1) whether that disclosure is mandatory or voluntary, 2) by what statutory or other authority the number is solicited, and 3) what uses will be made of it.

There is little doubt that Congress intended agencies to provide this notice in advance of the agency's use of the social security number. Doe v. Sharp, 491 F Supp 346, 349-50 (D Mass 1980) (citing 1974 US Code Cong & Admin News 6196-99). See also Doyle v. Wilson, supra, 529 F Supp at 1350 (state must make affirmative efforts to inform of potential uses at or before time of request). Moreover, that notice must specify all uses that the agency will make of the records. See Greater Cleveland Welfare Rights Organization v. Bauer, 462 F Supp 1313 (ND Ohio 1978) (notice not "meaningful" because ADC recipients not informed that their social security numbers would be used to verify employment information).

The programmatic consequence of failing to provide meaningful notice is to prevent the use of the social security number, at least until an adequate notice is provided to each individual. See Doe v. Registrar of Motor Vehicles, 528 NE2d 880, 888 (1988); Yeager v. Hackensack Water Co., 615 F Supp 1087, 1092 (D NJ 1985). There is also a risk of federal criminal penalties for disclosing, using or compelling disclosure of social security numbers of any person in violation of section 7(b) of the Privacy Act. 42 USC § 408 (a)(8) (West 1991).[38]

In order for the participating agencies to obtain and/or use their clients' social security numbers for the SIS, notice must be provided to each individual whose social security number is to be used for that purpose. The notice must be given to each individual, not simply published in an agency regulation or policy manual. Doe v. Sharp, supra, 491 F Supp at 349. The notice must provide meaningful notice of the intended uses for the social security number, with some degree of specificity, and give the individual the opportunity to decide whether to allow such use of his or her social security number. Id. at 350.

[38] The unlawful use or disclosure or compleling the disclosure of social security numbers, the unauthorized willful disclosure of social security account numbers and related records obtained or maintained by an authorized person pursuant to a provision of law enacted on or after October 1, 1990, and the willful offer of any item of material value in exchange for any such social security number or related record are all felonies. 42 USC § 408(a)(8) (Supp 1993), 42 USC § 405(c)(2)(C)(vii) (Supp 1993), 26 USC § 7213(a)(1)-(3) (Supp 1993). Each is punishable, upon convication, by a fine not exceeding $5000 or imprisonment of not more than 5 years. Id.

In general, the notice could be a separate notice exclusively for purposes of the SIS or it could be added onto existing notices used by the participating agencies. One complication will be the potential overlap between when an agency may mandate a client to disclose his or her social security number and when the same agency may request the client to voluntarily disclose the number for use by the SIS, For example, AFSD requires provision of a social security number as a condition of eligibility for food stamps for ADC. Clearly, an ADC applicant could not be denied ADC benefits for refusing to permit his or her social security number to be used by the SIS. For such an agency, we do not believe that the mere notice of the agency's intent to use the number for the SIS will be sufficient. The agency must obtain actual consent from its clients for the use of their social security numbers by the SIS. The agency must also avoid any implication that a refusal to consent could result in ineligibility for food stamp or ADC benefits.

In a Letter of Advice dated January 11, 1988, to Ross Laybournm, Jr., Department of Justice, Charitable Activities Section (OP-6197), we conclude that just as a government agency must have statutory or regulatory authority to request a social security number,[39] an agency may use a social security number obtained from a person pursuant to that authority for no other purpose than those authorized by statute or administrative rule at the time the number is requested. Consequently, in order for the participating agencies to use clients' social security numbers for the SIS, those agencies will either need a statute or they will need to promulgate an administrative rule authorizing them to do so. This statute or rule must be cited in the notice. Privacy Act, § 7(b).

3. 1990 Amendment

The 1990 amendment to the Social Security Act provides that social security numbers and related records[40] obtained or maintained by any person who has access to such numbers or records "pursuant to any provision of law, enacted on or after October 1, 1990, shall be confidential, and no [such] person shall disclose any such social security account number or related record." 42 USC § 405 (c)(2)(C) (vii) (Supp

[39] Section 7(b) of the Privacy Act requires an agency to advise an individual "by what statutory or other authority" a social security number is solicited.

[40] A key feature of the 1990 amendment is that the confidentiality requirement includes not only social security numbers but also "related records." The amendment defines "related recor" as:

> [A]ny record, list, or cocmpilation that indicates, directly or indirectly, the identity of any individual with respect to whom a request for a social security account number is maintained pursuant to this clause.

42 USC § 405(c)(2)(C)(vii)(IV) (Supp 1993). Because of our conclusion that the particicpating agencies must obtain consent for use of their social security numbers by the SIS, we do not explore the ramifications of the inclusion of related records in the confidentiality requirement. We recommend that the agencies include a reference to related records in their notice/consent.

1993). Although we have found no legislative history or case law interpreting the 1990 amendment, we believe that the phrase "any provision of law, enacted on or after October 1, 1990" would include both statutes and administrative rules adopted after that date. Because of our conclusion above that the participating agencies will need either a statute or administrative rule authorizing them to use their clients' social security numbers for the SIS, we believe this prohibition of redisclosure would apply not only to social security numbers obtained on or after October 1, 1990, but also to those obtained before October 1, 1990, but authorized to be used by the participating agencies for purposes of the SIS after that date.

One possible reading of the 1990 amendment is that absolutely no re-disclosure of social security numbers or related records is permitted. However, section 7(b) of the Privacy Act expressly permits the use of social security numbers (and, thus, presumably their redisclosure) as long as the notice of intended use is legally sufficient. Moreover, the criminal penalties for violation of the 1990 amendment only apply to "unauthorized willful disclosure." 42 USC 405(c)(2)(C)(vii)(II)(Supp 1993). Similarly, the criminal penalties under 42 USC 408(a)(8) apply only to "violation of the laws of the United States," and the Privacy Act is not violated if the use (or redisclosure) of numbers is supported by a proper notice under section 7(b) of the Privacy Act. Thus, it is reasonable to conclude that only unauthorized redisclosures, i.e., redisclcosures for which there is no consent, are prohibited.

Although we conclude above that the proposed operation of the SIS would not involve "disclosure" of client information in violation of various statutes restricting the participating agencies' disclosure of information and records, the legislative history of the Privacy Act suggests a different conclusion with respect to social security numbers. Rather than the concern with public disclosure of personally identifiable information found in the legislative history of the agency program statutes, the legislative history of the Privacy Act and Social Security Act provisions on the use of social security numbers reflects a concern with their growing use as a common identifier. In the proposed operation of the SIS, the social security number is intended to be the common identifier; and it would be the decoding and "disclosure" of this number that would enable the cross-matching of the client information maintained by each of the separate participating agencies. It is just such a data matching scheme that these provisions arguably were intended to proscribe.

However, we need not resolve whether this "disclosure" of social security numbers in the proposed operation of the SIS is prohibited by the 1990 amendment because of our conclusion above that section 7(b) of the Privacy Act would require the participating agencies to obtain informed consent from their clients before using their social security numbers for the SIS in any event. Such consent would satisfy any prohibition to "disclosure."

4. Necessary Steps

We conclude that informed consent is required to permit clients' social security numbers to be used by the SIS. As we understand the proposed operation of the SIS, the participating agencies will have direct contact with their individual clients, but the SIS, acting as the recipient of the information from the participating agencies, will not. Based upon this understanding, we describe the necessary steps the participating agencies must take.

First, the participating agencies mist have statutory or administrative rule authority to request the social security number for use by the SIS. The enactment of a statute or the adoption of an administrative rule must precede a request to the client for the disclosure to, or the consent for use by the participating agency, of that social security number for purposes of the SIS.

Second, the participating agencies must provide notice to each individual who is being asked to disclose his or her social security number, or to consent to its use, for purposes of the SIS. The notice must identify that use and give the individual the opportunity to decide whether to allow such use of his or her social security number. For those participating agencies that do not already have their clients'' social security numbers, a meaningful notice, in response to which the client may or may not choose to provide a social security number, should suffice. However, for those agencies that do have their clients' social security number, either voluntarily disclosed for other purposes or disclosed in response to mandatory disclosure authority, we believe that the clients' signed consent to use the number for the SIS will be necessary. We have attached, as Appendix B, a draft of a notice that might be used by all participating agencies for this purpose.[41]

IV. Safeguards to Ensure Confidentiality of Information Collected by the SIS

We have found no state laws that prescribe any particular security measures for safeguarding the confidentiality of data in computer information systems.

Both the Privacy Act of 1974, 5 USC§ 552a, and the Computer Matching and Privacy Protection Act of 1988, 5 USC§ 552a(o), contain general requirements for the safeguarding of records. Although we do not believe that either of these federal statutes would apply to the SIS, we set forth their relevant provisions below for whatever guidance they might provide.

The Privacy Act of 1974 governs the responsibilities of federal agencies that collect, store and disseminate personal information about individuals. This Act provides only that each agency that maintains a "systems of records"[42] shall

[41] We assume that those agencies that currently obtain their clients social security numbers already use a notice meeting the requirements of section 7(b) of the Privacy Act. A notice such as the one in Appendix B would be a necessary supplement.

[42] A "system of records' means

establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained[.]

5 USC § 552a(e)(10)(West 1977).

The Computer Matching and Privacy Protection Act of 1988 prohibits the disclosure to a state agency of any record contained in a "system of records" for use in a "computer matching program," except pursuant to a written agreement that specified:

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;

(H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;

(I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program[.]

5 USC § 552a)o)(1)(F)-(I) (Supp 1993).

The safeguards required by these two federal statutes do not appear to apply to the operation of the SIS. The Privacy Act of 1974 pertains only to federal agencies. The Computer Matching and Privacy Protection Act of 1988 applies only to computer data contained in a federal agency's "system of records" that is provided to other agencies, including state agencies, for purposes of "computer matching programs." HR Rep No. 802, 100th Cong 2d Sess 23, reprinted in 1988 US Code Cong & Admin News 3107, 3129. The proposed operation of the SIS is not a 'computer matching program" under the Act's definition, which specifically excludes:

---

a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particcular assigned to the individual.

(i) matches performed to produce aggregate statistical data without any personal identifiers;

(ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals[.]

5 USC § 552a(a)(8)(B)(i) and (ii) (Supp 1993).

Although the federal requirements for safeguarding personally-identifiable records do not appear applicable to the SIS, they may serve as a helpful guide to the participating agencies -- not only as an example of safeguards they could adopt for records provided to the SIS, but also to facilitate computer matching with federal records in the future. See also Computer Security Act of 1987, Pub L No. 100-235, 101 State 1724 (1987).

/s/ Theodore R. Kulongoski
THEODORE R. KULONGOSKI

Attorney General

APPENDIX A

The following is a list of records the disclosure of which in a personally-identifiable form to the SIS without the individual's consent is prohibited or restricted by federal laws or regulations or state laws. The WQC has informed us that it is not interested in these records at this time for the operation of the SIS. Accordingly, we do not discuss in this opinion the applicability of any confidentiality statutes to these records. The statutory or regulatory citations provided are for reference only and not intended to be complete.

General

1. Expunged juvenile court records. ORS 419.835,419.838.

Bureau of Labor and Industries (BOLI)

1. Investigatory information regulating to any complaint filed with BOLI under ORS 659.040 (unlawful employment practices) or 659.045 (discrimination in housing, places of public accommodation, or private vocational, professional or trade schools).

2. Examination papers of applicants for licenses to maintain an employment agency. ORS 658.042(5).

3. Identities of public employees who disclose information under ORS 659.510(1)(b) or 659.525(2) (whistleblowing). ORS 659.535.

Department of Corrections (ODOC)

1. Presentence investigation reports. ORS 137.077.

2. Reports on criminal offenders and juveniles submitted by circuit, district or county courts to ODOC pursuant to ORS 179.045.

3. Inmate medical/psychological/psychiatric records. ORS 179.495, 179.505.

4. Criminal history information contained in the Law Enforcement Data System (LEDS). 28 CFR§§ 20.33, 20.38.

5. Alcohol and drug abuse treatment records. ORS 179.495, 179.505, 426.460(5); 42 USC§§ 290dd-3 and 290ee-3.

6. HIV testing information. ORS 179.495, 179.505, 433.045(3), 433.055.

7. Complaints filed with the Corrections Ombudsman. ORS 423.430.

Department of Insurance and Finance
Workers' Compensation Division (WCD)

1. "Data generated by or received in connection with [WCD's oversight of managed care organizations' medical review] activities, including written reports, notes or records of any such activities, or of the director's review thereof[.]" ORS 656.260(6).

2. Information obtained by WCD from inspections of books, records and payrolls of employers under ORAS 656.726(8).

Adult and Family Services Division (AFSD)

1. Agency evaluation of information about a particular individual.

2. Medical data, including diagnosis and past history of disease or disability concerning a particular individual.

3. The contents of any records, files, papers or communications connected with the establishment and enforcement of child support obligations.

4. Income and eligibility verification system records.

5. HIV status.

Employment Division (ED)

1, The contents of any records, files, papers or communications connected with the establishment and enforcement of child support obligations.

2. Income and eligibility verification system records.

3. Drug and alcohol abuse information received from a federally funded treatment facility may not be retained or released by ED without the written consent of the patient.

Vocational Rehabilitation Division

1. Alcohol and drug patient records. 42 CFR Part 2.

APPENDIX B

CONSENT TO DISCLOSURE OF SOCIAL SECURITY NUMBER
FOR USE IN THE SHARED INFORMATION SYSTEM

[ORS/ORS] authorizes participating agency to request that you voluntarily provide your social security number to this agency for use in the Shared Information system. Failure to provide your social security number will not be used as a basis to deny you any right, benefit, or privilege provided by law. If you provide your social security number and consent to its use in the Shared Information system, it will be used only in the following manner. The Shared Information system will collect client and workforce-related information from the participating agencies (including this agency), analyze that information and provide the participating agencies and other state agencies and officials with statistical data, including education, training, and other services provided to clients and the resulting client outcomes, in order to aid the agencies' program planning for providing services to Oregon's citizens. The Shared Information System will release only aggregate statistical information, without any personal identifiers, such as a name or social security number. Furthermore, the data produced by the Shared Information System will not be used by any participating agency, or any other state agency or official, to make any decision or take any action directly affecting any individual, including you.

I hereby consent to disclose my social security number and related records to participating agency for use in the Shared Information System as described above.

Client

Signature Social Security Number

Date

****