

Illinois Longitudinal Data System Higher Education Consortium (HEC)
DRAFT Premises of Memorandum of Understanding **DRAFT**

*Higher Education institutions agree to form the **Illinois Longitudinal Data System Higher Education Consortium** based on the following:*

Purpose: The HEC forms the organization that establishes a longitudinal data system and data warehouse system for higher education institutions. The HEC enters into agreements to link higher education student unit records with early learning, elementary, and secondary school student unit records.

Timing: The P-20 longitudinal system needs to be in place by June 30, 2013. Non-public higher education institutions receiving MAP grants would participate by July 1, 2012, by sharing data with IBHE or through HEC.

Organization: Non-public institutions, community colleges, and public universities would submit data to the HEC for the purposes of data sharing, research and analysis. ICCB would function as a clearinghouse for community college data submissions to the Consortium. The IBHE would contract with HEC for the purpose of collecting data from participating institutions on its behalf and share that data with the P-20 ILDS. As authorized by law, the IBHE could collect data from other sources and share that data with the P-20 ILDS.

Oversight: The IBHE would engage in a cooperative planning process in establishing and maintaining the ILDS. It would consult with a committee of participating institutions to establish a data sharing arrangement with any external party.

Procedures: Through the Consortium, IBHE would establish procedures and requirements for submitting the data to the ILDS, including data specifications, quality, security, and timeliness.

- Individual institutions would have the right to opt out of specific uses of their data for reasons specified in the contract.
- Student-level data remain the property of the institution.
- A non-public institution would have the right to remove its data from the Consortium for reasonable cause. After redress, the data would be resubmitted to the Consortium.
- Data would be used only for agreed-upon purposes stated in the contract.

Data Sharing: The Consortium may share data with other entities to support research and evaluation activities per a data sharing agreement. The data sharing would:

- be permissible under privacy regulations,
- be approved by Consortium authorities,
- not permit the personal identification of an individual other than to authorized representatives with legitimate interests in the information,
- ensure the destruction or return of the data when no longer needed for the authorized purposes, and

- be based on a written agreement stipulating:
 - the purpose, scope, and duration of the data sharing arrangement;
 - the use be only for the purposes stated in the written agreement; and
 - the specific data access, use, and security restrictions in force.

The collection, use, maintenance, disclosure, and sharing of data would be conducted in accordance with privacy protection laws. Security measures and procedures would protect personal information from intentional or accidental release to unauthorized persons and from unauthorized uses.

Illinois P-20 Longitudinal Education Data System Act
Summary of Legislation Pertaining to Data Use and Data Sharing by Institutions
of Higher Education; Background Statements on FERPA and Use of SSN

Note: While the legislation speaks to a consortium of non-public institutions only, these summary materials are premised on the view that establishing a single consortium covering all higher education institutions is the optimal arrangement.

Summary – Purpose of the ILDS:

Senate Bill 1828, the P-20 Longitudinal Education Data System Act, was signed into law as Public Act 096-0107, effective July 30, 2009. This Act requires the Illinois State Board of Education (ISBE), the Illinois Community College Board (ICCB), and the Illinois Board of Higher Education (IBHE) -- the State Education Authorities (SEA) -- to establish a longitudinal data system (ILDS) and data warehouse by entering into agreements that link early learning, elementary, and secondary school student unit records with higher education student unit records. The system and warehouse are to be completed on or before June 30, 2013.

The SEA shall engage in a cooperative planning process in establishing and maintaining the ILDS.

Text of the legislation:

Section 15. Establishment of the longitudinal data system and data warehouse.

(a) The State Education Authorities shall jointly establish and maintain a longitudinal data system by entering into one or more agreements that link early learning, elementary, and secondary school student unit records with institution of higher learning student unit records.

To the extent authorized by this Section and Section 20 of this Act:

- (1) the State Board is responsible for collecting and maintaining authoritative enrollment, completion, and student characteristic information on early learning, public school (kindergarten through grade 12), and non-public school (kindergarten through grade 12) students;
- (2) the Community College Board is responsible for collecting and maintaining authoritative enrollment, completion, and student characteristic information on community college students; and
- (3) the Board of Higher Education is responsible for collecting and maintaining authoritative enrollment, completion, and student characteristic information on students enrolled in institutions of higher learning, other than community colleges.

(b) On or before June 30, 2013, subject to the availability purposes of this Act, the State Education Authorities shall improve and expand the longitudinal data system to enable the State Education Authorities to perform or cause to be performed all of the following activities and functions:

- (1) Reduce, to the maximum extent possible, the data programs, schools, school districts, and institutions of higher learning with access to their own student-level data, summary reports, and data that can be integrated with additional data maintained outside of the system to inform education decision-making.
- (2) Provide authorized officials of early learning programs, schools, school districts, and institutions of higher learning with access to their own student-level data, summary reports, and data that can be integrated with additional data maintained outside of the system to inform education decision-making.
- (3) Link data to instructional management tools that support instruction and assist collaboration among teachers and postsecondary instructors.
- (4) Enhance and expand existing high school-to-postsecondary reporting systems to inform school and school district officials, education policymakers, and members of the public about public school students' performance in postsecondary education.
- (5) Provide data reporting, analysis, and planning tools that assist with financial oversight, human resource management, and other education support functions.
- (6) Improve student access to educational opportunities by linking data to student college and career planning portals, facilitating the submission of electronic transcripts and scholarship and financial aid applications, and enabling the transfer of student records to officials of a school or institution of higher learning where a student enrolls or seeks or intends to enroll.
- (7) Establish a public Internet web interface that provides non-confidential data reports and permits queries so that parents, the media, and other members of the public can more easily access information pertaining to statewide, district, and school performance.
- (8) Provide research and reports to the General Assembly that assist with evaluating the effectiveness of specific programs and that enable legislators to analyze educational performance within their legislative districts.
- (9) Allow the State Education Authorities to efficiently meet federal and State reporting requirements by drawing data for required reports from multiple State systems.
- (10) Establish a system to evaluate teacher and administrator preparation programs using student academic growth as one component of evaluation.
- (11) In accordance with a data sharing agreement entered into between the State Education Authorities and the Illinois Student Assistance Commission, establish procedures and systems to evaluate the relationship between need-based financial aid and student enrollment and success in institutions of higher learning.
- (12) In accordance with data sharing agreements entered into between the State Education Authorities and health and human service agencies, establish procedures and systems to evaluate the relationship between education and other student and family support systems.
- (13) In accordance with data sharing agreements entered into between the State Education Authorities and employment and workforce development agencies, establish procedures and systems to evaluate the relationship between education programs and outcomes and employment fields, employment locations, and employment outcomes.

(c) On or before June 30, 2013, subject to the availability of funding through appropriations made specifically for the purposes of this Act, the State Board shall establish a data warehouse that integrates data from multiple student unit record systems and supports all of the uses and functions of the longitudinal data system set forth in this Act. The data warehouse must be developed in cooperation with the Community College Board and the Board of Higher Education and must have the ability to integrate longitudinal data from early learning through the postsecondary level in accordance with one or more data sharing agreements entered into among the State Education Authorities. The data warehouse, as integrated with the longitudinal data system, must include, but is not limited to, all of the following elements:

- (1) A unique statewide student identifier that connects student data across key databases across years. The unique statewide student identifier must not be derived from a student's social security number and must be provided to institutions of higher learning to assist with linkages between early learning through secondary and postsecondary data.
- (2) Student-level enrollment, demographic, and program participation information, including information on participation in dual credit programs.
- (3) The ability to match individual students' elementary and secondary test records from year to year to measure academic growth.
- (4) Information on untested students in the elementary and secondary levels, and the reasons they were not tested.
- (5) A teacher and administrator identifier system with the ability to match students to early learning, elementary, and secondary teachers and elementary and secondary administrators. Information able to be obtained only as a result of the linkage of teacher and student data through the longitudinal data system may not be used by a school district for decisions involving teacher pay or teacher benefits unless the district and the exclusive bargaining representative of the district's teachers, if any, have agreed to this use. Information able to be obtained only as a result of the linkage of teacher and student data through the longitudinal data system may not be used by a school district as part of an evaluation under Article 24A of the School Code unless, in good faith cooperation with the school district's teachers or, where applicable, the exclusive bargaining representative of the school district's teachers, the school district has developed an evaluation plan or substantive change to an evaluation plan that specifically describes the school district's rationale for using this information for evaluations, how this information will be used as part of the evaluation process, and how this information will relate to evaluation standards. However, nothing in this subdivision (5) or elsewhere in this Act limits or restricts
 - (i) a district's use of any local or State data that has been obtained independently from the linkage of teacher and student data through the longitudinal data system or
 - (ii) a charter school's use of any local or State data in connection with teacher pay, benefits, or evaluations.
- (6) Student-level transcript information, including information on courses completed and grades earned, from middle and high schools. The State Board shall establish a statewide course classification system based upon the federal School Codes for

Exchange of Data or a similar course classification system. Each school district and charter school shall map its course descriptions to the statewide course classification system for the purpose of State reporting. School districts and charter schools are not required to change or modify the locally adopted course descriptions used for all other purposes. The State Board shall establish or contract for the establishment of a technical support and training system to assist schools and districts with the implementation of this item (6) and shall, to the extent possible, collect transcript data using a system that permits automated reporting from district student information systems.

(7) Student-level college readiness test scores.

(8) Student-level graduation and dropout data.

(9) The ability to match early learning through secondary student unit records with institution of higher learning student unit record systems.

(10) A State data audit system assessing data quality, validity, and reliability.

(d) Using data provided to and maintained by the longitudinal data system, the State Education Authorities may, in addition to functions and activities specified elsewhere in this Section, perform and undertake the following:

(1) research for or on behalf of early learning programs, schools, school districts, or institutions of higher learning, which may be performed by one or more State Education Authorities or through agreements with research organizations meeting all of the requirements of this Act and privacy protection laws; and

(2) audits or evaluations of federal or State-supported education programs and activities to enforce federal or State legal requirements with respect to those programs. Each State Education Authority may assist another State Education Authority with audit, evaluation, or enforcement activities and may disclose education records with each other for those activities relating to any early learning through postsecondary program. The State Education Authorities may disclose student information to authorized officials of a student's former early learning program, school, or school district to assist with the evaluation of federal or State-supported education programs.

(e) In establishing, operating, and expanding the longitudinal data system, the State Education Authorities shall convene stakeholders and create opportunities for input and advice in the areas of data ownership, data use, research priorities, data management, confidentiality, data access, and reporting from the system. Such stakeholders include, but are not limited to, public and non-public institutions of higher learning, school districts, charter schools, non-public elementary and secondary schools, early learning programs, teachers, professors, parents, principals and administrators, school research consortiums, education policy and advocacy organizations, news media, the Illinois Student Assistance Commission, the Illinois Education Research Council, the Department of Commerce and Economic Opportunity, the Illinois Early Learning Council, and the Legislative Research Unit.

(f) Representatives of the State Education Authorities shall report to and advise the Illinois P-20 Council on the implementation, operation, and expansion of the longitudinal data system.

(g) Appropriations made to the State Education Authorities for the purposes of this Act shall be used exclusively for expenses for the development and operation of the longitudinal data system. Authorized expenses of the State Education Authorities may relate to contracts with outside vendors for the development and operation of the system, agreements with other governmental entities or research organizations for authorized uses and functions of the system, technical support and training for entities submitting data to the system, or regular or contractual employees necessary for the system's development or operation.

Summary – Establish ILDS:

The SEA shall collect and maintain data from their schools, colleges, and universities and shall share that data with the ILDS. As authorized by law, the SEA may collect data from other sources and share that data with the ILDS.

Non-public higher education institutions receiving MAP grants must participate by July 1, 2012, by sharing data with IBHE or through a consortium that has contracted with IBHE.

Text of the legislation:

Section 20. Collection and maintenance of data.

(a) The State Board is authorized to collect and maintain data from school districts, schools, and early learning programs and disclose this data to the longitudinal data system for the purposes set forth in this Act. The State Board shall collect data from charter schools with more than one campus in a manner that can be disaggregated by campus site. The State Board may also disclose data to the longitudinal data system that the State Board is otherwise authorized by law to collect and maintain.

On or before July 1, 2010, the State Board shall establish procedures through which State-recognized, non-public schools may elect to participate in the longitudinal data system by disclosing data to the State Board for one or more of the purposes set forth in this Act. Subject to the availability of funding through appropriations made specifically for the purposes of this Act, the State Board shall establish or contract for the establishment of a technical support and training system to assist school districts, schools, and early learning programs with data submission, use, and analysis.

Subject to the availability of funding through appropriations made specifically for the purposes of this Act, the State Board shall establish or contract for the establishment of a technical support and training system to assist school districts, schools, and early learning programs with data submission, use, and analysis.

(b) The Community College Board is authorized to collect and maintain data from community college districts and disclose this data to the longitudinal data system for the purposes set forth in this Act. The Community College Board may also disclose data to the longitudinal data system that the Community College Board is otherwise authorized by law to collect and maintain.

Subject to the availability of funding through appropriations made specifically for the purposes of this Act, the Community College Board shall establish or contract for the establishment of a technical support and training system to assist community colleges with data submission, use, and analysis.

(c) The Board of Higher Education is authorized to collect and maintain data from any public institution of higher learning, other than community colleges, and disclose this data to the longitudinal data system for the purposes set forth in this Act. The Board of Higher Education may also disclose data to the longitudinal data system that the Board of Higher Education is otherwise authorized by law to collect and maintain.

Beginning on July 1, 2012, the Board of Higher Education is authorized to collect and maintain data from any non-public institution of higher learning enrolling one or more students receiving Monetary Award Program grants, pursuant to Section 35 of the Higher Education Student Assistance Act, and disclose this data to the longitudinal data system for the purposes set forth in this Act. Prior to July 1, 2012, any non-public institution of higher learning may elect to participate in the longitudinal data system by disclosing data for one or more of the purposes set forth in this Act to the Board of Higher Education or to a consortium that has contracted with the Board of Higher Education pursuant to this subsection (c). [Section continues below]

Summary – Establish Consortium, Contract, and Procedures:

Non-public institutions may establish a consortium (or more than one) for the purposes of data sharing, research and analysis. Public universities and community colleges may also choose to participate in this consortium. ICCB will function as a clearinghouse for community college data submissions to the consortium and/or to IBHE. The IBHE may contract with that consortium for the purpose of collecting data from participating institutions on its behalf; institutions submitting data through the consortium do not have to submit data directly to IBHE. IBHE may consult with a committee of participating institutions to establish a data sharing arrangement with an external party.

The SEA shall establish procedures and requirements relating to the submission of data, including requirements for data specifications, quality, security, and timeliness such that:

- ***individual institutions shall have the right to opt out of specific uses of their data for reasons specified in the contract.***
- ***student-level data shall remain the property of the institution.***
- ***a non-public institution shall have the right to remove its data from the consortium for reasonable cause. After redress, the data shall be resubmitted to the consortium.***
- ***data must be used only for agreed-upon purposes as stated in the contract.***

Text of the legislation (Section 20 continued):

The Board of Higher Education may contract with one or more voluntary consortiums of non-public institutions of higher learning established for the purpose of data sharing, research, and analysis. The contract may allow the consortium to collect data from participating institutions on behalf of the Board of Higher Education. The contract may provide for consultation with a representative committee of participating institutions and a representative of one or more organizations representing the participating institutions prior to the use of data from the consortium for a data sharing arrangement entered into with any party other than a State Education Authority pursuant to Section 25 of this Act. The contract may further provide that individual institutions of higher learning shall have the right to opt out of specific uses of their data or portions thereof for reasons specified in the contract. Student-level data submitted by each institution of higher learning participating in a consortium that has contracted with the Board of Higher Education pursuant to this paragraph shall remain the property of that institution. Upon notice to the consortium and the Board of Higher Education, any non-public institution of higher learning shall have the right to remove its data from the consortium if the institution has reasonable cause to believe that there is a threat to the security of its data or its data is used in a manner that violates the terms of the contract between the consortium and the Board of Higher Education. In the event data is removed from a consortium pursuant to the preceding sentence, the data must be returned by the institution to the consortium after the basis for removal has been corrected. The data submitted from the consortium to the Board of Higher Education must be used only for agreed-upon purposes, as stated in the terms of the contract between the consortium and the Board of Higher Education. Non-public institutions of higher learning submitting student-level data to a consortium that has contracted with the Board of Higher Education pursuant to this paragraph shall not be required to submit student-level data to the Board of Higher Education.

Subject to the availability of funding through appropriations made specifically for the purposes of this Act, the Board of Higher Education shall establish or contract for the establishment of a technical support and training system to assist institutions of higher learning, other than community colleges, with data submission, use, and analysis. The Board of Higher Education may make available grant funding to a consortium of non-public institutions of higher learning to provide assistance in the development of a data collection system. The Board of Higher Education shall engage in a cooperative planning process with public and non-public institutions of higher learning and statewide higher education associations in connection with all of the activities authorized by this subsection (c).

(d)The State Education Authorities shall establish procedures and requirements relating to the submission of data authorized to be collected pursuant to this Section, including requirements for data specifications, quality, security, and timeliness. All early learning programs, schools, school districts, and institutions of higher learning subject to the data collection authority of a State Education Authority pursuant to this Section shall comply with the State Education Authority's procedures and requirements for data submissions. A State Education Authority

may require that staff responsible for collecting, validating, and submitting data participate in training and technical assistance offered by this State if data is not submitted in accordance with applicable procedures and requirements.

Summary – Data Sharing and Disclosure Policies:

The SEA may share data with other entities to support research and evaluation activities per a data sharing agreement. Under the agreement a data sharing arrangement must:

- ***be permissible under privacy regulations (See Appendix 1.),***
- ***be approved by the SEA authorities,***
- ***not permit the personal identification of an individual other than to authorized representatives with legitimate interests in the information (See Appendix 2.),***
- ***ensure the destruction or return of the data when no longer needed for the authorized purposes, and***
- ***be based on a written agreement stipulating:***
 - ***the purpose, scope, and duration of the data sharing arrangement;***
 - ***the use be only for the purposes stated in the written agreement;***
 - ***the specific data access, use, and security restrictions in force.***

The collection, use, maintenance, disclosure, and sharing of data must be conducted in accordance with privacy protection laws. Security measures and procedures must protect personal information from intentional or accidental release to unauthorized persons and from unauthorized uses.

Text of the legislation:

Section 25. Data sharing.

(a) The State Education Authorities may disclose data from the longitudinal data system collected pursuant to Section 20 of this Act only in connection with a data sharing arrangement meeting the requirements of this Section.

(b) Any State agency, board, authority, or commission may enter into a data sharing arrangement with one or more of the State Education Authorities to share data to support the research and evaluation activities authorized by this Act.

State Education Authorities may also enter into data sharing arrangements with other governmental entities, institutions of higher learning, and research organizations that support the research and evaluation activities authorized by this Act.

(c) Any data sharing arrangement entered into pursuant to this Section must:

- (1) be permissible under and undertaken in accordance with privacy protection laws;
- (2) be approved by the following persons:

- (A) the State Superintendent of Education or his or her designee for the use of early learning, public school, and non-public school student data;
 - (B) the chief executive officer of the Community College Board or his or her designee for the use of community college student data; and
 - (C) the executive director of the Board of Higher Education or his or her designee for the use of student data from an institution of higher learning, other than a community college;
- (3) not permit the personal identification of any person by individuals other than authorized representatives of the recipient entity that have legitimate interests in the information;
- (4) ensure the destruction or return of the data when no longer needed for the authorized purposes under the data sharing arrangement; and
- (5) be performed pursuant to a written agreement with the recipient entity that does the following:
- (A) specifies the purpose, scope, and duration of the data sharing arrangement;
 - (B) requires the recipient of the data to use personally identifiable information from education records to meet only the purpose or purposes of the data sharing arrangement stated in the written agreement;
 - (C) describes specific data access, use, and security restrictions that the recipient will undertake; and
 - (D) includes such other terms and provisions as the State Education Authorities deem necessary to carry out the intent and purposes of this Act.

Section 30. Subject to privacy protection laws.

The collection, use, maintenance, disclosure, and sharing of data authorized by this Act must be conducted in accordance with privacy protection laws. The State Education Authorities shall each develop security measures and procedures that protect personal information from intentional or accidental release to unauthorized persons and from intentional or accidental use for unauthorized purposes.

... [Act continues]

Section 505. The Illinois School Student Records Act is amended by changing Section 6 as follows:

(105 ILCS 10/6) (from Ch. 122, par. 50-6)

Sec. 6. (a) No school student records or information contained therein may be released, transferred, disclosed or otherwise disseminated, except as follows:

...

(4) To any person for the purpose of research, statistical reporting, or planning, provided that such research, statistical reporting, or planning is permissible under and undertaken in accordance with the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and no student or parent can be identified from the information released and the person to whom the information is released signs an affidavit agreeing to comply with all applicable statutes and rules pertaining to school student records;

... [Act continues].

Appendix 1a
Data Privacy and Protection
Common Practices Regarding Compliance with FERPA

No personally identifiable information is released except to authorized users. The CEO must authorize release of personally identifiable data to those users.

Student records are released only for the purposes of evaluation and audit of instructional programs.

The SSN is not stored with the general data, rather sequestered in a separate, secure location and accessed only when needed as a key identifier (for example, to link records from one source to another). See Appendix 2.

Data are destroyed or returned when no longer needed for the stated purpose.

Personally identifiable data must be stored in a secure location and shared through secure processes.

Appendix 1b

Presentation on Data Privacy and Protection: State Data Systems and FERPA Steven Y. Winnick, EducationCounsel LLC SHEEO, New Orleans, May 21, 2009

Key provisions of Winnick's presentation:

- FERPA authorizes state education authorities (including the SLDS) to use personally identifiable information from student education records at all levels of education in order to **evaluate or audit federal and state programs** (emphasis added) and to meet federal requirements related to those programs.
- Personally identifiable information provided to the SLDS may be reviewed and analyzed for these purposes by state education employees, or by contractors who are engaged by the SLDS to administer the data warehouse or to assist in performing these functions.
- FERPA applies to educational agencies and institutions (postsecondary institutions, schools, and school districts) that receive grant funds from the U.S. Department of Education (USED).
- FERPA prohibits educational agencies and institutions from disclosing students' education records without written parental consent, **unless the disclosure comes within one or more of a list of authorized disclosures in the law.** [Insert to original: See list below.]
- Once a student reaches 18 years of age or is attending a postsecondary institution, the consent required of and the rights accorded to parents under FERPA accrue to the student. ("Eligible Student")
- FERPA prohibits disclosure of personally identifiable information in students' education records.
- FERPA does not prohibit the disclosure of anonymous or de-identified data that cannot easily be traced to individual students.
- New FERPA regulations define "personally identifiable information" to include:
 - Information that alone or in combination would allow a reasonable person in the school community to identify the student with reasonable certainty, and
 - Information requested by a person who the education agency or institution reasonably believes knows the identity of the student to whom the education record relates.
- "Education records" subject to FERPA are broadly defined to include records, files, and other materials directly related to a student and maintained by an educational agency or institution or by a person acting for it.

However, FERPA does not authorize disclosures of education records to workforce (or other non-education) agencies for the purpose of strengthening workforce (or other) services. ... FERPA needs to be interpreted or, as necessary, amended to harmonize [with] state and federal policies.

Appendix 1c

Selected FERPA Guidelines per U.S. Department of Education

(downloaded 12-21-09; emphasis added)

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

- ❑ The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. ...
- ❑ Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, **FERPA allows schools to disclose those records**, without consent, **to the following parties** or under the following conditions (34 CFR § 99.31):
 - School officials with legitimate educational interest;
 - Other schools to which a student is transferring;
 - **Specified officials for audit or evaluation purposes;**
 - Appropriate parties in connection with financial aid to a student;
 - Organizations conducting certain studies for or on behalf of the school;
 - Accrediting organizations;
 - To comply with a judicial order or lawfully issued subpoena;
 - Appropriate officials in cases of health and safety emergencies; and
 - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Appendix 2

Draft statement: Use of student Social Security Number

Source: ILDS Higher Education Institutional Data element subcommittee

SSN Collection

Social Security Numbers (SSNs) should be collected as a part of the regularly scheduled higher education data submission process using a login and password protected restricted access\secure data transfer process (FTP\VPN). The record with the SSN should be used for initial administrative data matching and merging. As soon as possible after administrative data matching and merging takes place, the SSN should be replaced with a unique randomly generated or encrypted System ID number. A random number generator program or high level encryption program shall be used to create the new identifier (System ID). A look-up table shall be created to assure that the System ID number remains unique (not reused). Time is of the essence in replacing the SSN with the System ID.

The SSN and the newly created System ID shall be stored in a secure location in a server that is not directly connected to the internet with severely restricted access (e.g., 2 permanent full-time employees of the matching and merging administrative entity for the higher education data files). The System ID shall replace the SSN in all central data system files. The System ID shall function as the primary key field for the higher education database.

Criteria used by the federal government to safeguard SSNs and protect automated records shall be adhered to by any individual with access to the SSN.

Federal Office of Personnel Management 5 CFR Part 293

(6) Access to Social Security Numbers must be restricted to those individuals whose official duties require such access. A listing of all individuals with access authorization based on legitimate business needs must be maintained and reviewed for continued applicability.

(7) Agencies must ensure, through appropriate annual training and educational programs, including training on Privacy Act and Freedom of Information Act requirements, that those individuals who are authorized to access Social Security Numbers understand their responsibility to protect sensitive and personal information. This responsibility includes securing this information when working from home or another remote location.

(8) Agencies must use privacy and confidentiality statements that describe accountability clearly and warn of possible disciplinary action for unauthorized release of the Social Security Number and other personally identifiable information. These statements must be signed by all individuals who have access to Social Security Numbers.

§ 293.107 Special safeguards for automated records.

(a) In addition to following the security requirements of §293.106 of this part, managers of automated personnel records shall establish administrative, technical, physical, and security safeguards for data about individuals in automated records, including input and output documents, reports, punched cards, magnetic tapes, disks, and on-line computer storage. The safeguards must be in writing to comply with the standards on automated data processing

physical security issued by the National Bureau of Standards, U.S. Department of Commerce, and, as a minimum, must be sufficient to:

- (1) Prevent careless, accidental, or unintentional disclosure, modification, or destruction of identifiable personal data;
- (2) Minimize the risk that skilled technicians or knowledgeable persons could improperly obtain access to, modify, or destroy identifiable personnel data;
- (3) Prevent casual entry by unskilled persons who have no official reason for access to such data;
- (4) Minimize the risk of an unauthorized disclosure where use is made of identifiable personal data in testing of computer programs;
- (5) Control the flow of data into, through, and from agency computer operations;
- (6) Adequately protect identifiable data from environmental hazards and unnecessary exposure; and
- (7) Assure adequate internal audit procedures to comply with these procedures.

(b) The disposal of identifiable personal data in automated files is to be accomplished in such a manner as to make the data unobtainable to unauthorized personnel. Unneeded personal data stored on reusable media such as magnetic tapes and disks must be erased prior to release of the media for reuse.

<http://edocket.access.gpo.gov/2008/E8-858.htm> and

http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5cfr293_main_02.tpl

Q:\Policy Studies\ISEG and Longitudinal Data\SSN Collection Short.docx