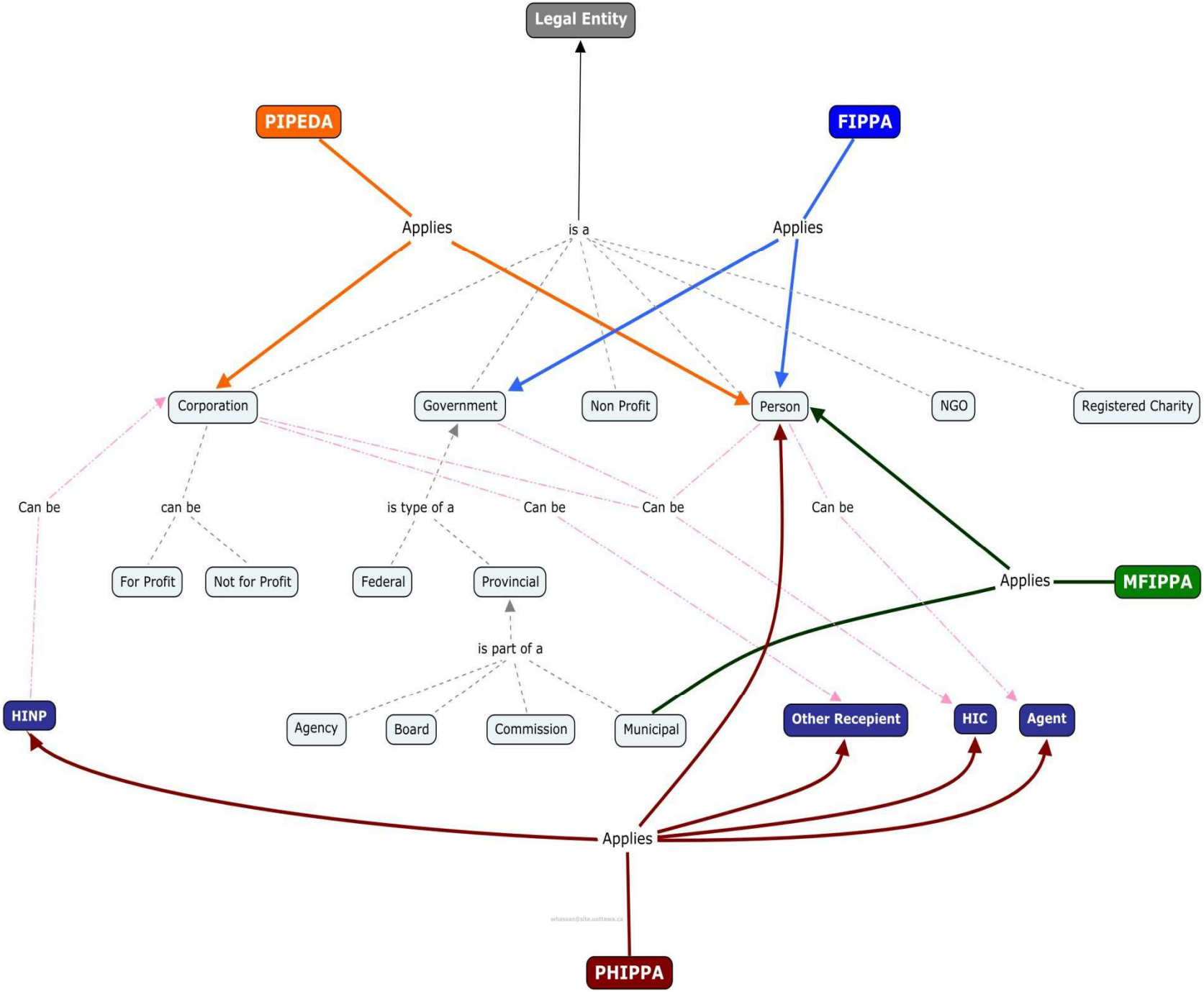
Integrating Data to Inform Public Policy: Legal Issues

John Petrila, J.D., LL.M.
Professor, University of South Florida
petrila@usf.edu


Legal Entity
PIPEDA
FIPPA
Applies
is a
Applies
Corporation
Government
Non Profit
Person
NGO
Registered Charity
Can be
can be
is type of a
Can be
Can be
Can be
For Profit
Not for Profit
Federal
Provincial
Applies
MFIPPA
is part of a
HINP
Agency
Board
Commission
Municipal
Other Recepient
HIC
Agent
Applies
PHIPPA

Overview of Paper

- Privacy
- Security
- Enforcement
- Some potential changes in Common Rule and FERPA

Some Basic Points About Law and Privacy

- Many sources of law regarding privacy/confidentiality
- Source of law depends on the information in question
- Nearly all information is available in some form
- De-identified information is usually easier to get than identifiable information
- Privacy and security are both important

Some Basic Sources of Law

- The Common Rule
- The Federal Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Education Rights and Privacy Act (FERPA)
- Substance abuse and alcohol (42 CFR Part 2)
- Homeless Management Information System (HMIS)
- Child Abuse Treatment and Prevention Act (CAPTA)
- State Law
  - Arrest records
  - Medicaid records

Definitional Issues

- Privacy Act: “personally identifiable information”
- HIPAA: “protected health information”
- FERPA: “personally identifiable information”
- 42 CFR Part 2: “any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program”
- HMIS: “protected personal information”

HMIS Definition of Protected Personal Information

- Identifies, directly or indirectly, a specific individual;
- Can be manipulated by a reasonably foreseeable method to identify an individual; *or*
- Can be linked with other available information to identify an individual.

FERPA Definition Personally Identifiable Information

- a) The student's name.
  b) The name of the student's parent or other family members.
  c) The address of the student or student's family.
  d) A personal identifier, such as a social security number, student number, or a biometric record: a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, i.e., fingerprints, handwriting, etc.
  e) A list of personal characteristics.
  f) Other information that would make a student's identity easily traceable.

Some General Considerations

- Does the applicable law provide access for research?
- If two laws might apply, which must I follow?
- Is a data use agreement or memorandum of understanding required?

Access is Usually Possible

42 CFR Part 2 permits access for research *if* the researcher

- Is qualified to conduct the research;
- Has a research protocol under which the patient identifying information will meet security requirements and will not be re-disclosed except as permitted by 42 CFR Part 2 and
- Has provided a satisfactory written statement that a group of three or more individuals who are independent of the research project has reviewed the protocol and determined that the rights and welfare of patients will be adequately protected; and that the risks in disclosing patient identifying information are outweighed by the potential benefits of the research.

Consent Requirements

IRB may waive or alter consent requirements when

- (1) The research involves no more than minimal risk to the subjects;
- (2) The waiver or alteration will not adversely affect the rights and welfare of the subjects;
- (3) The research could not practicably be carried out without the waiver or alteration; and
- (4) Whenever appropriate, the subjects will be provided with additional pertinent information after participation (45 CFR 46.116(c) (2).

Choice of Law

- HIPAA only applies to protected health information under control of a “covered entity”
- Covered entities include health care providers that transmit information in electronic form, health plan, or health care clearinghouse
- State law providing more stringent protection of privacy applies to PHI

HIPAA and FERPA

- **Protected Health Information excludes Individually Identifiable Health Information in education records covered by the Family Educational Right and Privacy Act**

Data Use and Research Agreements

- HMIS requires written research agreement
  - Establish rules and limitations processing and security of PPI during research
  - Provide for return or disposal of PPI at conclusion of research
  - Restrict further use or disclosure of PPI except where required by law
  - Require that data recipient formally agree to comply with conditions

Data Use Agreements

- HIPAA requires DAU with Limited Data Sets
- A DUA
- Establish who is permitted to use or receive the limited data set.
- Provide that the limited data set recipient will:
  - Not use the information in a matter inconsistent with the DUA or other laws.
  - Employ safeguards to ensure that this does not happen.
  - Report to the covered entity any use of the information that was not stipulated in the DUA.
  - Ensure that any other parties, including subcontractors, agree to the same conditions as the limited data set recipient in the DUA.
  - Not identify the information or contact the individuals themselves.

Using Non-Identifying Data

- HIPAA
  - De-identified data sets
    - Remove 18 data elements
    - Various identifiers such as email addresses, account numbers, geographic subdivision information, social security numbers, medical records numbers, etc
  - Limited data sets

Limited Data Set

- Protected health information from which certain specified direct identifiers of the individual and their relatives, household members and employers have been removed.
- All of the direct patient identifiers are removed like de-identified information but it may contain dates, city and full 5 or 9-digit zip codes.
- A limited data set requires a Data Use Agreement (DUA) as the authority for its use or disclosure.

Patient Data Posted Online in Major Breach of Privacy

- The spreadsheet included names, diagnosis codes, account numbers, admission and discharge dates, and billing charges for patients seen at Stanford Hospital's emergency room during a six-month period in 2009

HITECH Act

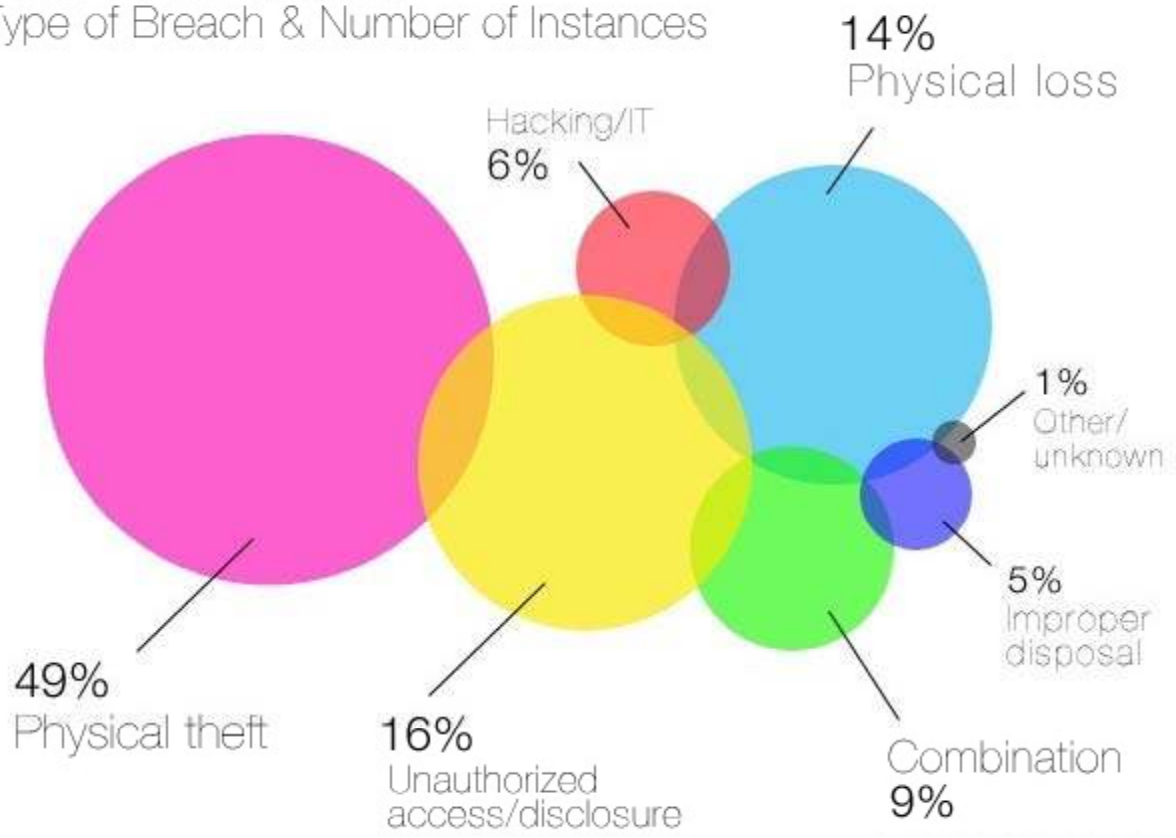
- Health Information Technology for Economic and Clinical Health Act
- Part of the American Recovery and Reinvestment Act of 2009
- Four categories of violations that reflect increasing levels of culpability;
- Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and
- A maximum penalty amount of $1.5 million for all violations of an identical provision.

HIPAA Security Rule Risk Analysis

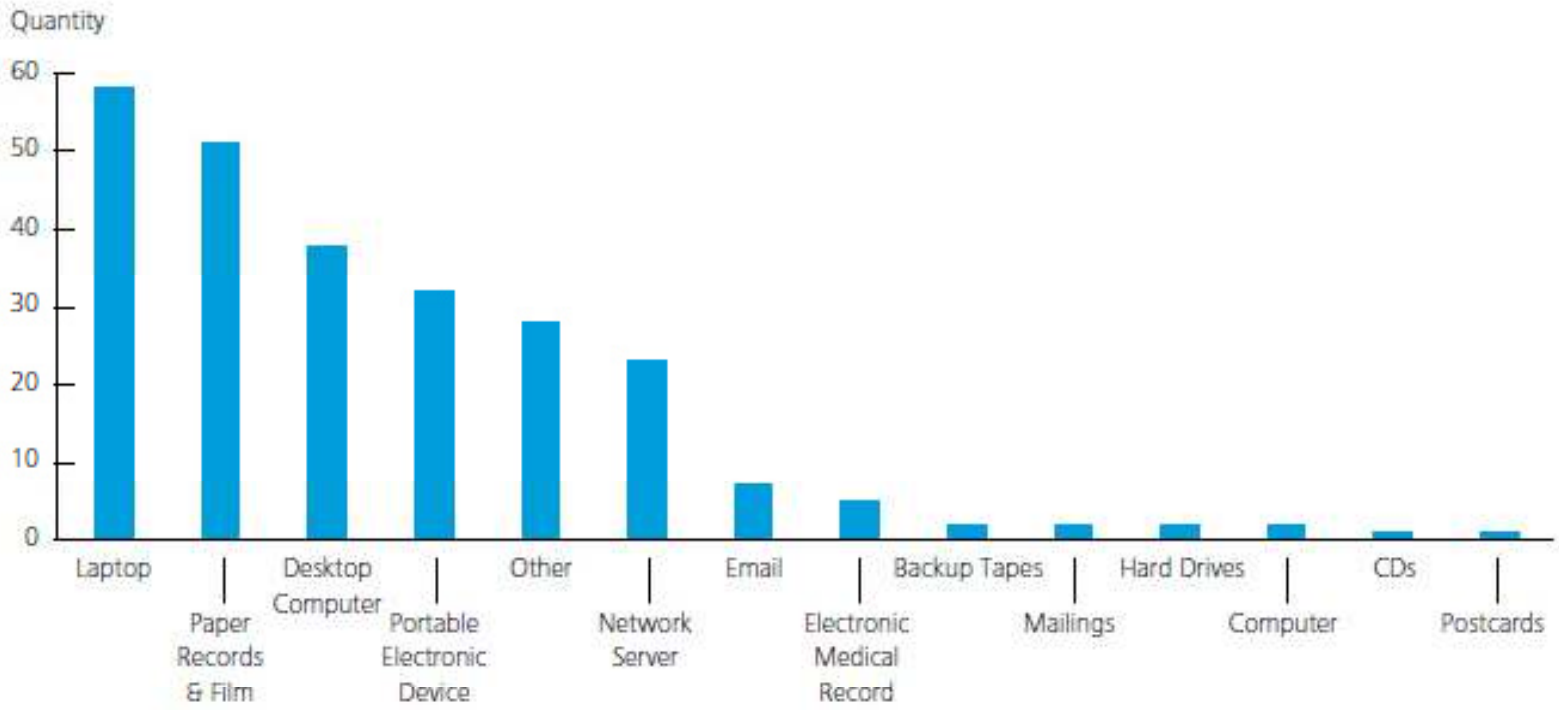
"an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

HIPAA Violations

Type of Breach & Number of Instances



Location of Breached Information



Based on data published by HHS as of December 27, 2010

Enforcement

- Most federal laws do not provide a private cause of action
- Whether state law permits a private cause of action depends on *state* law
- Government enforcement of HIPAA has increased
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html

Proposed Changes to Common Rule

According to HHS

1. Human research landscape has “changed dramatically” since early 1980s (in volume, in human services and social science research, and in multi-site studies)

2. Need to enhance protection of subjects and make regulatory structure more efficient

Proposed Changes

- Filed July 26, 2011
- Comments extended until October 26, 2011
- More information here: http://www.hhs.gov/ohrp/humansubjects/anprm2011page.html

Proposed Changes

- “Calibrate the level of review to the level of risk”
- Use single IRB for domestic multi-site studies
- Update informed consent processes
- Mandatory data security and information protection standards for all studies
- Systematic data collection on problems and adverse events
- Extend regulatory coverage to all studies conducted by institutions receiving Common Rule agency funding
- Provide uniform guidance on federal regulations

Level of Risk and Level of Review

- There is “little evidence that most IRB review of social and behavioral research does much to protect subjects from psychological or informational risks…
- Over-regulating social and behavioral research in general may…distract attention from…studies that do pose threats to the welfare of subjects”
- Most risk is one of three categories: physical, psychological, **and informational**

Informational Risks

- Informational risks derive from inappropriate use or disclosure of information…which might jeopardize current or future employment, or cause emotional or social harm
- Informational risks are correlated with the nature of the information and the degree of identifiability
- Most disclosures “occur due to inadequate data security”

What Would Change?

- Creation of an “excused” category of research
- Subject to new informational security requirements
- Research using data or records collected for purposes other than research could include data not in existence at time study commenced
- Researchers could maintain identifiers

New Data Protections

- HHS considering “mandating data security and information protection that would apply to all research that collected, stored, analyzed, or otherwise reused identifiable or potentially identifiable information”
- Protections would be “scaled appropriately to the level of identifiability of the data”
- HIPAA standards for identifiable and deidentifiable information are not aligned with Common Rule

HIPAA and Common Rule Alignment

- Considering amendment of Common Rule to adopt HIPAA definitions of
  - Identifiable information
  - Limited data set
  - De-identified information

For Data Security

- Research using identifiable data or limited data sets could be required to meet security standards modeled on HIPAA security rule
- Researchers could see the identifiers as long as do not record them in a permanent research file
- More aggressive audits of data security
  - **Informational studies would fall into "excused" category**

Proposed Changes in Rulemaking for the Family Educational Rights and Privacy Act (FERPA):

Implications for Integrated Data Systems

Overview

- FERPA is Changing
- Timeline of changes
- Rationale and Context:
  Why has it been so hard to include education data and what's different now?
- Review of proposed changes relevant to IDS:
  - Educational data **can be shared and integrated**
  - Data can be shared with other agencies
  - Data can be stored in data warehouses

Timeline

- Notice of Proposed Rulemaking
  Filed 4/7/2011
- Period for Public Comment
  Passed 5/23/2011
- When will the changes be finalized?
  - Anticipated by the end of the year

Barriers to Education Data in IDS

Past restrictive interpretation of FERPA:

Disclosures of **personally identifiable information** prohibited to ***anyone not under an educational authority's direct control***

(Hanson Memorandum, 2003; FERPA Preamble, 2008)

Personally Identifiable Information

a) The student's name.
b) The name of the student's parent or other family members.
c) The address of the student or student's family.
d) A personal identifier, such as a social security number, student number, or a biometric record: a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, i.e., fingerprints, handwriting, etc.
e) A list of personal characteristics.
f) Other information that would make a student's identity easily traceable.

What's Changed?

Congress emphasizes more effective use of educational data in the service of:

- Innovation and Improvements
- Accountability and Transparency
- Maintaining privacy safeguards

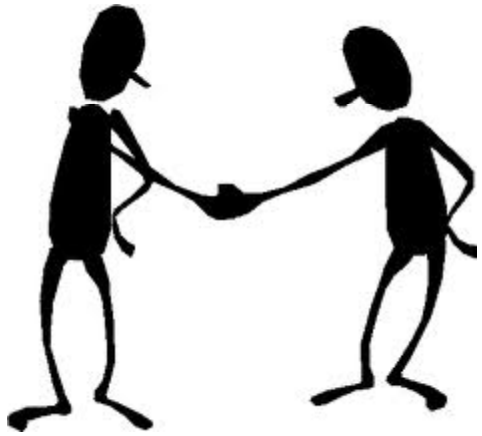
Department of Education's Response

New guidance and clarifications "…to ensure…FERPA continues to **protect the privacy of education records**…while **allowing for the effective use of data**" (emphasis added)

Overview of Clarifications Relevant to IDS

State or local educational authorities can share personally identifiable information with entities that they designate

- In data warehouses; To other agencies for integration
- For audit, evaluation, or enforcement
- For research



Who can PII be shared with?

- In original FERPA doc

FERPA does not define "authorized representatives"

FERPA permits educational agencies to disclose PII without consent to "authorized representatives" of the educational authorities…

Sharing with an ‘authorized representative’

- Proposed regulation provides clarification:

  1) “…an ‘authorized representative’ would mean any entity or individual designed by a State or local educational authority or agency…”

  2) The State, local authority, or agency is responsible “to use reasonable methods” to ensure the authorized representative complies with FERPA

  3) If the protected infromation is improperly disclosed by the authorized representative, it cannot receive protected data from the authority or agency for 5 years

  4) A written agreement is required

4) A written agreement is required.

The agreement should:

- Designate the authorized representative
- Specify the information to be disclosed and for what purpose
- Require the return or destruction of personally identifiable information when no longer needed
- Specify when the information must be returned or destroyed
- Establish policies and procedures to protect the information from further disclosure and unauthorized use

Innovation through Integration

Other types of data can be linked with education data:

- Allows data disclosure to outside entities for integration
- Allows linking with data from other agencies to study education effectiveness (e.g., workforce data)
- "Educational programs" defined broadly:
  e.g., early childhood & postsecondary; job training
- Allows disclosure of PII to State data warehouses to better ensure practices consistent with FERPA protections

Implications for IDS

1) Integrated data can be used to increase innovation, accountability, and transparency
   - Linking with other agencies' data and more types of educational programs
   - Contributing to data warehouses for integration

Implications for IDS

2) Clear guidance on who can share, how to share, and policies to protect privacy:

- States and local authorities can share data with outside groups and agencies
- Defined requirements for written agreements
- Defined penalties for inappropriate disclosures

For more information:

- Notice of Proposed Rulemaking:
  http://www.federalregister.gov/articles/2011/04/08/2011-8205/family-educational-rights-and-privacy

- FERPA page at Department of Education:
  http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

- Contact at Dept. of Education:
  FERPA@ed.gov