3.3: Guide to Data Privacy and Confidentiality

Protecting sensitive information about children and families is a crucial part of any data system. Two questions to address when considering data privacy are—

- What data must be protected?
- What needs to be done to ensure data is kept private and secure?

This guide provides a brief introduction to data privacy and confidentiality and will help your team understand what data must to be protected, what are the required regulations, and how to work with system vendors to ensure data privacy.

What data must be protected?

Personally Identifiable Information

The information that must be private/protected is called Personally Identifiable Information (PII). This information can be used to identify, contact, or locate a person. PII includes anything that identifies, such as name, address, phone number, or email address. Federal Government issued identification data such as Social Security numbers are particularly sensitive. PII also includes records such as medical, educational, financial, or employment.

The Federal Government describes three "impact levels" of PII: *low, medium,* and *high*. These levels are related to the amount of harm that could come from an individual's private information being accessed. For example, an individual's credit card information could likely cause more harm than an email address.

How can data be compromised?

Human Error

The single, main reason for compromised data is human error. A simple mistakes, such as writing login information on paper, leaves valuable data unsecured. Users also make blunders such as publishing private data to unsecured public sites or sending such data through less secure technologies like email. Leaving a system unattended while logged into a secure system also exposes data.

Security Breach

Security breaches happen for a variety of reasons. Hackers sometimes break through firewalls to access systems or use malicious software to access secure systems. Human error also often contributes to security breaches. Users can be tricked into giving login information to people pretending to be authorized. This is called "social engineering" and is a common cause of many high profile "hacks." Likewise, users unknowingly click on email links to malicious software that enable access to their systems. This is called "phishing."

How can data be protected?

Regulations

Laws exist to ensure privacy at federal, state, and local levels. Many tribes have data privacy regulations. Some international treaties even cover privacy. Data systems have to comply with all regulations.

HIPAA (Health Insurance Portability and Accountability Act) is a federal law enacted to protect the privacy of a patient's health information.

FERPA (Family Educational Rights and Privacy Act) is a federal law protecting the privacy of student education records.

FISMA (Federal Information Security Management Act) is a federal law requiring federal agencies to develop a plan to ensure private information is secure. If your agency/program reports data to a federal agency, this law guides the security of the data.

IRBs (Institutional Review Boards) often have a role in regulating data privacy protections in cases where your agency/program is engaged in research. For more information on IRBs and their role in the protection of data privacy as well as strategies for adhering to data privacy requirements in research, see the Tribal Evaluation Institute's Data Collection Toolkit Module 3.[1]

Privacy Agreements and Security

Data system providers should define their detailed privacy policies, either as part of a standard user agreement or in a separate privacy agreement. The agreement should specify who can access the data and how the provider protects and stores it.

Access. Most data providers allow limited access to agency data by their administrative users and technicians for support and maintenance purposes. Ideally the privacy agreement details exactly who can access the data, when, and under what circumstances. These systems have an audit trail feature allowing the provider to document all access made to data.

Security. Data security in modern systems uses encryption. Encryption is a method of encoding data, so it can be read only by authorized users who possess a key to unlock it. Transport encryption protects data when sent between computers or across the internet. File/storage encryption protects the data stored on the server.

[1] http://www.tribaleval.org/performance-measurement/data-collection-toolkit/