Data Security

Roger A. Boothroyd, Ph.D.

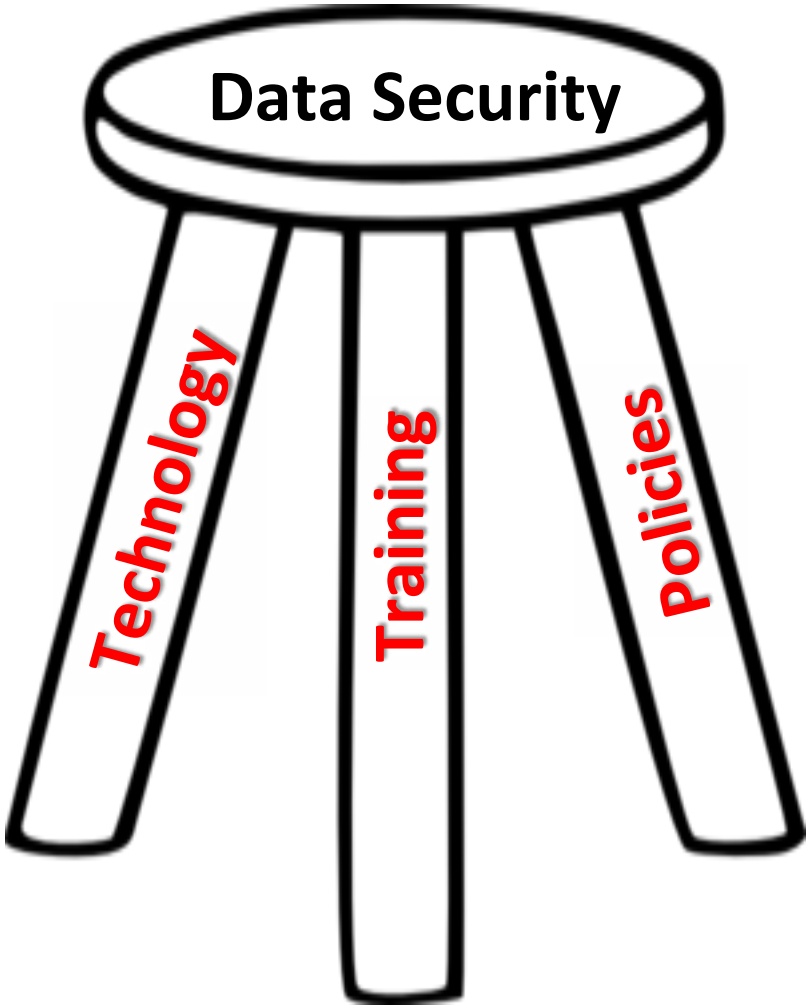
Paul G. Stiles, Ph.D., J.D.

Four Principles of Ethical Data Use*

- Four guiding principles that data owners/ custodians need to consider are:
  1. ***Data security***
  2. Confidentiality of information
  3. Permission to use data for research
  4. Appropriate/ethical use of data

*Stiles, P. G., Boothroyd, R. A., Robst, J., & Ray, J.V. (2011). Ethically using administrative data in research: Medicaid administrators current practices and best practices recommendations. *Administration & Society*, *43*, 171-192.

The Three-Legged Stool of Data Security



Training (expertise)

- Major weakness in security is the human element – a well-trained staff is essential.

- People with access to or who can grant access to sensitive data must
  - **understand the risks** involved with disclosure
  - **have the expertise** to secure the data

- Regular, mandatory training is needed to ensure all staff receive
  - **foundational security education** on data privacy and security
  - more advanced **professional development/training** in use and maintenance of sensitive data

- Organizations maintaining and/or sharing sensitive data should establish an information security **awareness program**

Policies (processes)

- Well-crafted policies and procedures with detailed processes that address
  - data procurement and use
  - data security and access
  - security incident and disaster recovery procedures
  - recording and monitoring of system activity
  - policy enforcement and training

- Sample security guidelines models and policies are available online (*e.g., S*ANS Institute, 2011; Litwak, 2011)

Technology (tools)

- Technological security is what we typically think of first.
- Technological safeguards are insufficient if they are the only line of defense.
- The owner/custodian must decide where on the continuum of technological options it falls in order to determine whether enough safeguards are in place.
- If disclosure would be disastrous for the organization (*e.g.,* highly sensitive data) or it is risk-averse, data should be stored on a physically secured, password protected, system, isolated and disconnected from any networks and external links such as the Internet.

- Less secure but strong option is to maintain a secured server behind a firewall filtering and activity logging.
- Two-factor authentication is also advisable.

Security Fails

References

- Stiles, P. G., & Boothroyd, R. A. (2011). *Ethical use of administrative data for research purposes*. Commissioned Paper by the MacArthur Foundation funded Workgroup on Intelligence for Social Policy, University of Pennsylvania.

- Stiles, P. G., Boothroyd, R. A., Robst, J., & Ray, J.V. (2011). Ethically using administrative data in research: Medicaid administrators current practices and best practices recommendations. *Administration & Society*, *43*, 171-192.

- Stiles, P. G. & Petrila, J. (2011). Research and confidentiality: Legal issues and risk management strategies. *Psychology, Public Policy & Law*, *17*, 333-356.