

Data Stewardship and Security Task Force  
Summary of Meeting  
August 24, 2006

Present: R. Barclay, L. Gaetano, M. Lochner, S. Koger, S. Swartzentruber, and B. Stahl

- Reviewed the types of data protected by legislation. Mary Ann explained that there is a hierarchy of confidential data with HIPPA data being the most confidential.
  - *Mary Ann and Lisa agreed to develop a single list of all relevant data that is considered confidential under any law.*
- Ray distributed a summary of the security classifications of data used by different institutions. The group agreed that the grid format used by Stanford University seemed to be the most useful.
- The members agreed that three tiers of security classification were adequate.
- The draft outline of a Data Stewardship and Security Policy was reviewed. The group made the following decisions:
  - The policy addresses access and disclosure
  - The policy addresses all institutional data, not just that housed on IT-managed systems
  - The default assumption should be that the data is classified as “Internal” – requiring permission before it can be accessed or disclosed
  - Need to indicate in the policy that contractual obligations may affect the security classification of data.
  - Need to incorporate the formation of an ongoing Data Stewardship and Security committee to oversee the implementation of the policy, ensure procedures are up to date and assist offices with risk assessments, etc.
- The Task Force agreed that the various roles of data handlers (administrator, processor, user, etc.) need to be incorporated into the procedure document and should be generally referred to in the policy.
- The Task Force agreed that putting together the *Procedures for Data Handling* document will be the most time-consuming.
  - *The Task Force members are to recommend the organization of the procedures document at least two weeks before the next meeting (Sept. 14<sup>th</sup>). We will assign responsibilities for developing each of the procedures section.*

