STS Database Collection of Protected Health Information
FAQ for STS Database Participants

1) What is HIPAA?

HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996. The "Privacy Rule" is a regulation under HIPAA that restricts the use and disclosure of "Protected Health Information" (PHI) by "Covered Entities." PHI is any "individually identifiable health information" kept in electronic format.

"Individually identifiable health information" is information that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

A "Covered Entity" under HIPAA is divided into the following categories:

- Hospitals, physicians and other health care providers who transmit PHI electronically to process health care claims and billing. Providers may include community clinics, social service agencies, and practitioners in psychology, psychotherapy, and social work;
- Health insurers, HMOs, health plans; and
- Health care clearinghouses

STS Database Participants are HIPAA Covered Entities.

2) What is "The Common Rule"?

"The Common Rule" is the federal regulatory standard of ethics to which any government-funded research in the US is held. Among other things, the Common Rule governs Institutional Review Board (IRB) oversight of human subjects research at most academic medical centers and research institutions.

3) What are the HIPAA implications of sending PHI to the STS data warehouse at the Duke Clinical Research Institute (DCRI)?

Your participation in the STS Databases is primarily for "health care operations" purposes. Health care operations are defined by HIPAA to include quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines. The primary reason the STS Databases exist

is to provide you with feedback on your organization's case mix and performance relative to national and other select benchmarks. These quality improvement endeavors are considered part of health care operations under HIPAA.

For the purposes of health care operations, PHI can be disclosed by a Covered Entity to an entity that performs functions or services on behalf of the Covered Entity as long the Covered Entity has entered into a business associate agreement with the recipient of the data. The business associate agreement must contain provisions for the appropriate safeguarding of the PHI. The STS National Database Participation Agreement (including Appendix 1- Business Associate Contract and Data Use Agreement) you entered into with STS contains a business associate agreement that mandates the appropriate safeguarding of PHI in accordance with HIPAA regulations. STS is a business associate of each participant because it performs data aggregation services on behalf of the participants, both individually and collectively. The Privacy Rule specifically permits business associates to provide data aggregation services on behalf of covered entities that include data analyses relating to the health care operations of those entities. Although until January of 2008, STS data did not collect fully-identified PHI, STS leadership had the foresight in 2003 to enter into business associate agreements with participants that would permit the submission of such PHI to the National Databases in the future.

4) What are the Common Rule (IRB) requirements for sending PHI to the STS data warehouse at the DCRI?

As outlined in the response to FAQ #3, data you are collecting and submitting to the STS data warehouse at the DCRI are for the purposes of health care quality improvement. You are not submitting data to the STS data warehouse for the purposes of human subjects research. For this reason, the Common Rule is not applicable to the data collected by the Database. To the extent that the data submitted to the Databases results from research involving human subjects (such as clinical trials), the institutions or individuals submitting such data would likely need to comply with the Common Rule.

5) It is widely known that the STS Databases data are sometimes used for research. Doesn't that mean that IRB approval is needed at each participating organization?

Although it is true that some organizations may be conducting research using the STS Database data, research using STS data is secondary to the main purpose of the STS Database to support health care quality improvement efforts. Your organization's participation in the STS Database is for the purpose of receiving risk-adjusted feedback about your surgical performance and, therefore, your submission of PHI to the STS Database is covered by your business associate

agreement with STS. To the extent that STS Database data is used for some research purposes, DCRI, as the STS data warehouse and analysis center, has obtained approval from the Duke University Institutional Review Board for the collection and aggregation of PHI from Database participants for such purposes. The HIPAA rules clearly do not require each institution that submits data to a registry that may be used for research purposes to obtain separate approval from its own IRB. However, any uses of Database data for specific research projects will be required to obtain separate IRB approval.

6) What are the safeguards in place at the DCRI to handle identified data?

As of January 1, 2008, STS Database Participants will have a single method for submitting their data file to the DCRI – the Data Warehouse Submission Web Site (https://stsdatawarehouse.dcri.duke.edu). The vast majority of Database Participants are currently using this method of file submission. Data files submitted through the Data Warehouse Submission Web Site benefit from extensive technological safeguards that make this method of data submission superior to any other alternative methods of submission, including the use of e-mail attachments or sending data on disk via ground or air delivery.

The Data Warehouse Submission Web Site utilizes a Secure Sockets Layer (SSL) Web Server Certificate to protect data submissions. The Web Server Certificate provides data privacy and prevents data tampering by using 128-bit encryption to protect the information sent between your browser and our Web server. The128-bit encryption, the highest level available for Web Server Certificates, is available to everyone regardless of their geographic location, by using a special "step-up" certificate for those browsers that do not support the highest level of encryption due to US export laws. The Web Certificate also provides authentication so that you can trust that you are submitting your data to the STS Data Warehouse when connecting to the Web Site.

Once the data arrive at DCRI, they are stored on username and password protected computer servers. Only the necessary analytic staff members are granted access to data with identifying information, and access is granted and revoked only by written communication from the team project leader to the team database administrator. DCRI also employs a detailed Duke Medicine Information Security Operations Plan. Throughout all phases of the work at DCRI, the data used are the minimum necessary for the task at hand.

7) What is the safest method to submit data with identifiers to the warehouse?

The Data Warehouse Submission Web Site will be the **only** method to submit data files to the Data Warehouse at DCRI as of January 1, 2008. As detailed in

FAQ #6, above, this is the safest method for submitting data to the Data Warehouse.

8) Are there any circumstances in which research can be conducted using Database data without IRB approval?

While fully-identified PHI is required for tracking individuals through time and for linking to certain external datasets, that identifying information is not required to remain attached to the clinical data for the vast majority of the research analyses performed by DCRI with STS data. For this reason, DCRI has generally removed and will continue to remove certain patient identifying information to create what is defined by HIPAA as a "Limited Data Set." A Limited Data Set contains items like date of birth and ZIP code but does not include items that directly identify an individual, such as patient name or medical record number. HIPAA allows the disclosure of Limited Data Sets without individual authorization for research purposes as long as there is a data use agreement in effect between the disclosing Covered Entity and the recipient of the data. The Business Associate Agreement between Database participants and STS has data use provisions that satisfy the requirements for disclosure of Limited Data Sets.

Suggested information resources on HIPAA and the Common Rule:

1. http://privacyruleandresearch.nih.gov/ is the Web site with the HHS guidance on HIPAA and how it relates to research. The monograph, "Health Services Research and the HIPAA Privacy Rule," is the section that is most appropriate to the DCRI work with the STS data.
2. http://www.hhs.gov/ohrp/ is the main page for the Office for Human Research Protections (OHRP), the section at HHS that governs the operations of IRBs under the Common Rule.
3. http://www.hhs.gov/ohrp/humansubjects/guidance/cdebiol.htm is the Guidance from OHRP on the use of coded data in research, and when it can be declared "Not Human Subjects" in FAQ #8.