# logosmallNIH caBIG | CCTS Security Requirements Project

## Topic: Questions for Legal Team

Date: August 8, 2008

The following questions will be used to filter and sort the use cases.

**Data Control**

*Patient Data Entered / Transferred*

* Is patient data controlled at entry?
* Is patient data controlled when transferred between applications?
* Is access to patient data controlled?
* Is patient data controlled in multi-site configuration?

*Study Data Entered/ Transferred*

* Is study data controlled at entry?
* Is study data controlled when transferred between applications?
* Is access to data controlled?
* Is study data controlled in multi-sit configuration?

**Administrative control**

*Rate-Specific Data Entered*

* Is role criteria controlled at entry?
* Is role criteria consistent between applications?
* Are users assigned to roles according to documented controls?
* Are role criteria consistent between sites in multi-site configuration?

*User Data Entered/ Authenticated*

* Are users authenticated at login?
* Is access to user/role assignments controlled?
* Are users controlled in multi-site configuration?

*Audit Log Data Captured*

*Authentication*

* What LOA (using the NIST pub 800-63 guidelines) is required for access to this data set based on HIPAA defined type of data and data steward determination? (authentication done at the cross application level and passes to data steward/application for determination to grant/withhold authorization)

*Authorization*

* What is the (HIPAA-defined) type of data:
	+ PHI
	+ LDS
	+ De-ID
	+ Non-human
* Who may access/transform the data (role based; data steward’s determination)
	+ HIPAA may constrain (minimum necessary)
	+ Donor/patient informed consent (HIPAA or Common Rule) may constrain
* Where will the data be sent/to whom (likely the who may access question but if mandated reporting, constraints may be obviated.
	+ HIPAA may constrain (minimum necessary)
	+ Donor/patient informed consent (HIPAA or Common Rule) may constrain
* What if any FDA regulatory constraints are there on authorization (will this be imposed by the steward or in the application?)