DATA CLASSIFICATION AND MANAGEMENT POLICY

I. Intent

This policy establishes uniform data classification and management standards for purposes of informing expectations for the security of Personal, Private and Sensitive Information (PPSI) set forth in other Questar III policies. PPSI is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, students or third parties. Such information could include one of more of the following: Social Security number, driver's license number or non-driver ID, account number, credit card number, or authentication credentials that permit access to an individual's financial or otherwise protected information.

II. Data Classification

Data classification, in the context of information security, is the categorization of PPSI data based upon the impact to the organization should that data (electronic or physical) be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data and therefore drives the development of all other policies and operational procedures.

Data owned, used, created, or maintained by Questar III is classified into the following four general categories:

Data Classification	Level of Risk	Description	Examples
Restricted	*High*	Data whose loss or unauthorized access could adversely affect Questar III, a partner or the public. Data that is "private information" as defined by the Internet Security and Privacy Act (State Technology Law, section 208). The greatest level of security controls should be applied to Restricted data.	• Social Security number • Driver's License number • Financial and banking information • Electronic Protected Health Information • Data otherwise protected by state or federal privacy regulations or confidentiality agreements • Student records protected by FERPA
Protected	*Medium*	Data with a diminished level of importance but that should nevertheless be protected from general access. A reasonable level of security controls should be applied to Moderate Risk data.	• Questar III intellectual property • Questar III proprietary data • Human Resources data (excluding "restricted data," above)
Confidential	*Low*	All other non-public data not included in the Restricted or Protected classes.	Non-public data, which could include non-personally identifiable statistical data.

Public	*None*	All public data.	General access data, such as that made publically available on the Questar III web site or which could be accessed in accordance with the Questar III Records Policy.

Data is typically stored electronically (e.g., databases, files, tables, etc.) or physically (e.g., hardcopy reports, memos, etc.).

III. Classification Inventory

Activities involving the classification, inventorying and risk assessment of data shall be overseen by Questar III's Information Security Officer.

ADOPTED: 07/10/14

References:
State Technology Law, section 208
Protecting Intellectual Property Policy 2-104
Student Records Policy 3-106
Records Policy 2-102
Acceptable Use Policy 7-208
Information Security, Breach, and Notification Policy 7-211
Erasure and Disposal of Electronic Media Policy 7-212