Data Classification Policy

I.   PURPOSE

The purpose of this data classification policy is to provide a system for protecting information that is critical to the organization. All workers who may come into contact with confidential information are expected to familiarize themselves with this data classification policy and to consistently use it.

II.   POLICY

The organizations data classification system has been designed to support the need to know so that information will be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, Company X unduly risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

Applicable Information: This data classification policy is applicable to all information in the Company X s possession. For example, medical records on patients, confidential information from suppliers, business partners and others must be protected with this data classification policy. No distinctions between the word data , information , knowledge, and wisdom are made for purposes of this policy.

Consistent Protection: Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, workers will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

CLASSIFICATION LABELS

Public: This classification applies to information that is available to the general public and intended for distribution outside the organizations. This information may be freely disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

For Internal Use Only: This classification applies to all other information that does not clearly fit into the other classifications. The unauthorized disclosure, modification or destruction of this information is not expected to seriously or adversely impact the

organization, its patients, its employees, or its business partners. Examples include the company telephone directory, new employee training materials, and internal policy manuals.

Confidential: This classification applies to information that is intended for use within the organization. Its unauthorized disclosure could adversely impact the organization, its patients, its employees and its business partners. Information that some people would consider private is included in this classification. Examples include medical information (except that which is restricted confidential), patient medical charts, appointment schedules, patient account records, department financial data, purchasing information, vendor contracts.

Restricted Confidential: This classification applies to the most sensitive medical and business information that is intended strictly for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization, its patients, its employees and its business partners. For example, statutorily protected medical information such as, mental health treatment, HIV testing, sexually transmitted diseases, abortion, and alcoholism or substance abuse treatment data. Other examples are merger and acquisition documents, corporate level strategic plans, and litigation strategy memos.

DATA CLASSIFICATION MATRIX

Refer to *Appendix A: Classification Matrix* for the handling and security requirements for information based on its classification.