Confidentiality Statement

I Understand That:

- I am responsible and held accountable for keeping electronic and hardcopy data, information, and information assets classified as High-Risk or Moderate-Risk (i.e. “confidential”) in strict confidence. Examples of confidential information includes, but are not limited to, protected health information (PHI), medical records systems and records, personal identifiable information (PII), e-mail, telephone calls, voice mail records, payroll, financial systems, payment card information (PCI), computer applications, computer source-code, and other data, information, and information asset classified as High-Risk or Moderate-Risk.

- I am not permitted to access, view, and alter (change) confidential information unless I have received authorization as required to complete my job responsibilities, and that I will access, view, and alter (change) only the confidential information records needed to perform those job duties.

- I am not permitted to alter my own confidential medical and/or any associated information, and to alter my confidential medical or any associated information, I will contact my physician and/or the Health Information Management (medical records) Department.

- HIV, mental health, and drug or alcohol counseling records are classified as High-Risk information and are therefore considered confidential, and that I may be subject to legal sanctions in addition to disciplinary actions if I improperly disclose (release) or permit the disclosure of information contained in these records. I understand that such improper disclosure by me of confidential HIV patient information is a criminal misdemeanor under New York State law, which could result in a fine or jail sentence or both. I understand if I improperly disclose or permit the disclosure of information relative to a patient’s treatment for drug or alcohol abuse, I may be subject to criminal penalties including payment of a fine ranging from $500 to $5,000 or more, as stipulated in the laws and regulations then in effect.

- I am responsible and will be held accountable for securing my authentication and access authorization mechanisms including passwords for all information systems. This means I will protect my means for accessing confidential systems, applications, data, information, and information assets so that others will not have access via my authentication and authorization mechanism including my passwords.

- I am responsible for knowing and abiding by published University information security policies and other related policies. This includes, but is not limited to, the Data Security Classification policy and policies related to proper confidential electronic and hardcopy data handling, protection, disposal, and retention.

- It is my responsibility to notify my supervisor, the Information Security Office, the Compliance Office, or Legal Counsel if I become aware of any unauthorized access and/or disclosure of confidential information.

- I will seek clarification from my supervisor, the Information Security Office, the Compliance Office, or Legal Counsel on any of the above whenever I have questions or concerns.

I understand unauthorized access and/or disclosure of confidential information will result in disciplinary action, up to and including termination of my employment and may also result in criminal penalties under Federal, New York State, and/or Local law.

Signature
Date

Print Name
Date

Last Revised April 2021