UNIVERSITY HOSPITAL
Newark, New Jersey

Sensitive Electronic Information (SEI) Handling User Responsibility Acceptance

CONFIDENTIAL

User First & Last Name: (Print)

UH EMR System & User Name: (Print)

DATE:

Authorized By: (Print)

The Sensitive Electronic Information (SEI) Handling User Responsibility Acceptance form is required for any user who, as part of their job duties, either create or export SEI on or to a system other than a designated University Hospital Electronic Medical Record server. The user identified herein is authorized to create or export such information only in fulfillment of their job duties as part of an authorized department procedure that is compliant with all requirements of this acknowledgement form, all other University Hospital policies, and Federal and State Regulations. The authorized user will be held accountable for any misuse that results from the creation or exportation of this information and so must ensure the appropriate level of security is used. User may permit access of the information to only those knowledgeable in the appropriate handling of SEI, who acknowledge and accept their responsibility and are authorized by University Hospital only after completion and submission of this form.

The authorized user acknowledges the risk and responsibility they have to use and store this information in an appropriate and secure manner. The authorized user acknowledges and accepts their role as Data Steward for the information they create or export and, as the Data Steward, their accountability for any improper handling, use, or storage of the information which results in or contributes to an information privacy or security breach. User must ensure anyone they permit access to this information is aware and knowledgeable and accepts the responsibility and accountability for the proper handling of the information as specified below.

User acknowledges that SEI Information created or information exported from a designated EMR server is classified as “Restricted” by University Hospital and must be protected in accordance with all UH Information Privacy & Security requirements. Restricted information includes patient information, pictures or images. Use of this information must be compliant with University Hospital policies such as but not limited to University Hospital Information and System Classification Policy, Media Protection Policy, Personal Mobile Device Security Policy and University Hospital Acceptable Use of Information Technology Policy. User agrees to these requirements for the use of “Restricted” information and;

1. The user must ensure device security where “Restricted” information is stored so the information is protected accordance to the information classification. Restricted information must reside only on systems located in secure locations such as a Data Center with restricted and monitored access. Restricted information is not to be saved or stored on the local C: drive or any designated drive that is local to a workstation, laptop computer, mobile device or camera. An exception by University Hospital Management is required for instances where it is necessary to

store “Restricted” information on local storage media. For authorized exceptions, the user must utilize a risk mitigation control such as a documented physical security procedure and/or a technical control such as encryption to secure the information. Local storage or storage outside a secure Data Center must employ either encryption or a documented and authorized department physical security procedure as part of an official workflow. The workflow with the exception provided by UH Management is subject to audit and must be documented and saved by the department.

2. Prior to any exception authorization or implementation of any official workflow a risk assessment must be performed that includes a use of encryption consideration to determine if encryption is required for sufficient protection.
3. The department procedure must include reporting of any loss, theft or suspected breach of “Restricted” information to The University Hospital Chief Compliance and Privacy Officer for risk determination for compliance with breach reporting and notification requirements.

These requirements are necessary for SEI acceptable terms of use required by University Hospital. The user agrees to adhere to these requirements and is authorized to create, export and use this information by their acknowledgement of their role and responsibilities as a Data Steward of this information. The authorized user is subject to all HIPAA privacy and security requirements for the use of patient information. Any violations of these requirements may result in access revocation of University Hospital information systems and other sanctions up to and including suspension and/or termination of Hospital privileges or employment.

As an authorized user of University Hospital information systems I acknowledge my responsibility to safeguard the information I create or export from University Hospital systems in fulfillment of my job duties and agree to the terms of use as described on this form.

Signature of Requester:

Date of signature:

FOR HST USE ONLY:
Date received @ HST: ____/____/____ HST Management Authorization:
____ Date: ____/____/_____
HST EMR Analyst: _____________________________ Date: ____/____/_____
Date Activated: ____/____/_____