MOREHOUSE SCHOOL OF MEDICINE

Office of Compliance and Corporate Integrity

Lost/Stolen Computer – Electronic/Mobile Device Report

Date of Report:	**Time:**

Name: _____

Title: _____

Location/Dept.: _____

Phone: _____

Email: _____

Type: **[Laptop, Mobile Hard Drive, Phone, PDA, USB-Thumb Drive, etc.]** _____
Make/Model/SN#: _____
Device owned by MSM? No **, If not, who owns it?** _____
Was Device Encrypted? No

Briefly describe what happened: _____
_____
_____
_____
_____

If stolen, was a police report filed? No **(if yes, please provide name and contact information of law enforcement agency)** _____

Personal Information & Protected Health Information (PHI)

Electronic Protected Health Information (ePHI) is any electronic information that is created or received by a health care provider that relates to the past, present, or future physical or mental health of an individual, and identifies the individual. Research data that originally was collected for patient treatment is usually ePHI.

Personal Information is an individual's first name or first initial and last name, in combination with any one or more of the following:

*social security number
*driver's license number or government-issued identification card number
*account number #, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
*medical information, health insurance

ePHI is often found in:

Medical instrumentation controllers
Clinical devices and workstations that run clinical applications Scheduling and billing systems
Clinical and research databases Image analysis workstations
Departmental file servers Research group servers
Clinical and research workstations Physician laptops and PDAs

PI is often found in:

Financial and personnel databases and spreadsheets Billing databases and documents
Student records
Recommendation letters for students Radiation Safety documents
NSF grant applications

Be sure to check for old documents and databases that may still have SSNs

Please mark all the data elements stored on your device(s):

- ☐ Name
- ☐ Email
- ☐ Phone Number
- ☐ Street Address, City, State & Zip Code
- ☐ Dates (Birth, Death, Treatment, etc.)
- ☐ Biometric IDs, finger or voice prints
- ☐ Confidential MSM Information
- ☐ Medical Information (PHI, diagnosis, history, treatment)
- ☐ Mental Health related data
- ☐ Student Information (Names, grades, etc.)
- ☐ Health Insurance Information
- ☐ Account #, Credit/Debit Card Information
- ☐ Other unique ID, characteristic or code
- ☐ Social Security Number
- ☐ Driver's License or School ID #
- ☐ Med Record Number
- ☐ Device ID or Ser. Number
- ☐ Full-Face photos or comparable images
- ☐ Intellectual Property
- ☐ Animal Research Data
- ☐ Human Subject Research Data
- ☐ Any other sensitive or confidential information
- ☐ Other (please specify)

Attestation: No PHI, PI, or Confidential Information

☐ **The device contains no PHI, PI or Confidential Information**

I attest that no Personal Information or Protected Health Information is on the device(s) lost or stolen. I further attest that I understand the consequences of my statement that no such information is on these devices and that I might be held accountable for any misstatements or misrepresentations regarding Personal Information, Protected Health Information or Confidential Information on the device(s) lost or stolen.

Signature _____ Date/Time _____

Physical signature is required for attestation

If you checked <u>ANY</u> boxes above, do not sign this attestation

Did you report this lost/stolen device(s) on the Compliance Hotline? ☐ Yes ☐ No

If yes, date/time?

Did you report this lost/stolen device(s) to MSM IT? ☐ Yes ☐ No

If yes, date/time?

Did you report this lost/stolen device(s) to Legal Department? ☐ Yes ☐ No

If yes, date/time?

Did you report this lost/stolen device(s) to your supervisor/manager? ☐ Yes ☐ No

If yes, date/time?

Report Intake Party

Name: _____
Department: _____
Phone: _____
Email: _____