# Lost/Stolen/Compromised Devices Form

## Instructions

In the event of a lost, stolen or compromised device, by law the University must gather details about any regulated and/or confidential information that might have been put at risk.

This form collects contact, device, incident and data information that may be needed for a possible investigation. For this reason, please complete all sections, including the Attestation one if the device had not been encrypted. Once completed, please scan and email the form to ISG@brown.edu.

If the device was encrypted, please inform your departmental computing coordinator (DCC) or central IT support to send ISG evidence of encryption (such as a screenshot showing that the device is encrypted) in addition to completing this form.

For background please see the "Policy on the Handling of Brown Restricted Information" and its supporting documents at http://brown.edu/go-computing-policies. To learn more about computing security incident response, please visit the web pages of Brown's Information Security Group at http://brown.edu/go/isg.

## Contact Information

| | | | |
|---|---|---|---|
| **Name** | | **Date** | |
| **Phone** | | **Location** | |
| **Email** | | **Dept** | |

## Device Information

| | | | |
|---|---|---|---|
| **Type:** (e.g. laptop, desktop, tablet, phone, ext. HD | | **Make / Model** | |
| | | **Serial #** | |
| **Is the device Brown-owned?** | ☐ YES ☐ NO | **Was the device encrypted?** | ☐ YES ☐ NO |

## Incident Information

| | | | |
|---|---|---|---|
| **Briefly describe what happened:** | | | |
| **Where was the device lost or stolen?** | | **Date of Incident:** | |
| **If stolen, was a police report filed?** | ☐ YES ☐ NO | **Police Report # (if applicable):** | |

# Data Classification

## Personally Identifiable Information (PII)

**Personally Identifiable Information** defined for this Rhode Island requirement (RI Statute Section 11-49.2-5) is an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Account credentials and passwords
- Account number, credit or debit card number
- Driver's license number or Rhode Island Identification Card number
- Social security number

**PII is often found in:**

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

## Brown Restricted Information (BRI)

**Brown Restricted Information (BRI)** (as defined in Section 2.0 of Brown's Policy on the Handling of BRI) is any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

**BRI includes but is not limited to:**

- Addresses
- Credit card numbers
- Dates of birth
- Driver's license numbers
- Medical records
- Passport information
- Social security numbers

## Electronic Protected Health Information (ePHI)

**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.

**ePHI is often found in:**

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

*Note: Be sure to check for old documents and databases that may still have SSNs.*

## Please mark all the Brown University data elements stored on your device(s)

- ☐ Names
- ☐ Phone Numbers
- ☐ List/database of Brown email addresses
- ☐ Account credentials (user names and passwords)
- ☐ Account, credit or debit card numbers
- ☐ Biometric IDs, finger or voiceprints
- ☐ Other unique IDs, characteristics or codes
- ☐ Driver's License or RI ID numbers
- ☐ Certificate License numbers
- ☐ Device ID or Serial numbers
- ☐ Employee confidential information (payroll, benefits, loans, evaluations and other personal information)
- ☐ Applicant / admission information
- ☐ Alumni information
- ☐ Parent / Family information
- ☐ Intellectual Property
- ☐ Medical records (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis)
- ☐ Anything that might embarrass the University
- ☐ Dates of birth
- ☐ Fax Numbers
- ☐ Street Address, City, State & Zipcode
- ☐ Social Security numbers
- ☐ Passport information
- ☐ Full-face photos or comparable images
- ☐ Brown tax / banking data
- ☐ Vehicle (VIN) #
- ☐ Medical Record numbers
- ☐ Web URL or IP addresses
- ☐ Student information (names, grades, application details)
- ☐ Financial aid data
- ☐ Donor information
- ☐ Grant information
- ☐ Animal Research (photos, data, researcher info / protocols)
- ☐ Health Insurance information (policy number or subscriber identification #, any unique identifier, or application and claims history information, including any appeals records)
- ☐ Any other sensitive or confidential information

## Data Relationships

| Was any of the data Brown-related? | ☐ **YES** | ☐ **NO** |
|---|---|---|

## Attestation: No PII, BRI or ePHI
## Complete only if device is not encrypted

☐ **The device contains no restricted information**

I attest that no Personally Identifiable Information, Brown Restricted Information or Electronic Protected Health Information or 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 Brown Restricted Information on the device(s) lost or stolen.

Signature* _____ Date/Time _____

* Physical signature is required. Please print the last page and physically sign the Attestation section. Email ISG the .pdf scan of the signed attestation page along with the completed form, or fax the signature page to (401) 863-9596.