Breach Response Guidelines for Research

Background

A breach is the unauthorized acquisition, access, use, or disclosure of data by unauthorized persons. When a potential breach has occurred or when notification is received from a sponsor, vendor, or collaborator that a breach has occurred, the PI has various reporting obligations.

The goal of this document is to help PIs and their staff understand their incident reporting obligations and provide guidelines for PIs and researchers to know what constitutes a breach, how to report a breach, their responsibilities, and the offices they should notify and work with to address a potential breach.

PIs and their staff should periodically review these guidelines to remain up to date on the latest requirements. Every Mass General Brigham (MGB) employee involved in a research project, e.g., study staff, must be trained on the breach response guidelines. The PI, or their designee, is responsible for ensuring their staff are so trained. All researchers, not just the PI, are responsible for maintaining the integrity of their project data.

Reporting a Breach

A breach must be reported to your institution's Privacy Office immediately upon its discovery. When reporting the breach to the institution's Privacy Office, include information about which states and/or countries may be affected by the breach. This will help facilitate the process and ensure that the incident response activities are properly scoped. If the project is supported by external funds, do not independently report the incident to the sponsor or collaborator prior to consulting the Privacy Office and Incident Response Team.

- Mass General Brigham (MGB) Institution Privacy Office
  - The Privacy Office must be contacted immediately when a potential breach has occurred. (Privacy Contacts by Institution)
  - An anonymous report of a breach may be reported in good faith to the Mass General Brigham Compliance HelpLine, by telephone or via the web.
- MGB - Institutional Review Board (IRB)
  - If the breach pertains to a research study that has been approved by the MGB IRB, the Principal Investigator (PI) must also notify the Mass General Brigham Institutional Review Board (IRB).
  - A breach of data confidentiality is considered non-compliance and must be reported through the "Other Events" form in Insight for the associated IRB protocol.

Incident Response

The Privacy Office will convene an Incident Response Team that includes other departments, as appropriate, e.g., OGC, MGB/Institution Research Compliance, MGB RISO, etc.

PIs, researchers, and their study staff are not authorized to speak with the media, patients, or others without Privacy Office permission. The Privacy Office, in conjunction with the departments involved in the breach investigation, will authorize instructions and guidance on speaking with the media, patients, or other third parties that may be affected by the breach.

When reporting the breach, the PI and their staff may receive instructions from the Privacy Office and the Incident Response Team to provide various documentation. For example, they may be asked to provide audits and logs

and/or inventories pertaining to hardware, software, network, and data. If the project is supported by external funds, the PI must provide the Privacy Office with copies of all current research agreements/contracts.

During an investigation, it is the responsibility of the PI and their staff to maintain the integrity of the data. They should not attempt to reboot systems or remediate on their own, as evidence may be lost. They must wait to hear from the Privacy Office and the Incident Response Team before providing any data or documentation that may pertain to the breach.

External Reporting Obligations

When there is a potential breach there are obligations in connection with sponsors, vendors, the IRB and other regulatory agencies.

The institutional Privacy Office and MGB Research Management, Research Compliance and IRB share responsibility for handling any external reporting to patients, sponsors, vendors and other third parties who are affected by a breach. Researchers are required to await further instructions from the Privacy Office, the Incident Response Team or the appropriate MGB office before initiating any external communications.

Data Breach Regulations Reporting Obligations

The Privacy Office will work with MGB and institutional Research Compliance and/or the Office of General Counsel (OGC) to determine with the PI whether a breach notification to a law enforcement, regulatory agency, federal sponsor, or other organization is necessary when affected individuals reside outside of Massachusetts or the United States and its territories.

When international data breach regulations are in scope, there may be a specific time window to report the breach to international authorities, when to send notifications to the individuals affected, and other requirements. As noted above, the PI must inform the Privacy Office, the Incident Response Team, and the MGB IRB which countries may be in scope.

Contractual Reporting Obligations with Sponsors and Collaborators

When a breach involves third parties such as sponsors and collaborators, the Privacy Office and other institutional departments will review the contracts and agreements that have been executed. If a notification is required, the Privacy Office and the appropriate institutional offices will ensure that proper notice have been effectuated.

Responsibilities of the Researchers

PIs, especially those who host externally facing databases, should develop an internal breach response procedure in the event of a potential breach. If their project has sponsor specific obligations and/or is subject to GDPR or other international privacy regulations, the research staff should also develop and maintain an incident reporting procedure which aligns with contractual and regulatory breach reporting obligations.

When reporting the breach, it is imperative to mention the state, federal, and international laws the research project may be subject to (e.g., HIPAA, GDPR, MA-93H, CCPA, etc.). If the breach includes a sponsor, vendor or other contractual agreements, please include this information so that the Privacy Office and the Incident Response Team can report the breach to the affected parties.

Contacts and References

Contacts for reporting a breach		
Department	**Contact**	**Site**
Privacy Office	Privacy Contacts by Institution	**Listed by institution**
Information Security Officer	Information Security Officers by Institution	**Listed by institution**
Anonymous Compliance HelpLine (MGB)	Mass General Brigham Compliance HelpLine	**Mass General Brigham**
Institutional Review Board	Mass General Brigham Institutional Review Board (IRB)	**Mass General Brigham**
Research Compliance Office	Mass General Brigham Research Compliance Office	**Mass General Brigham**
IS Service Desk	Mass General Brigham IS Service Desk by Institution	**Listed by Institution**

Policies

Privacy & Information Security Incident Investigation & Response PH-115a

ISPR-16a.4: Internal Reporting Procedures

EISP-16.4: Information Security and Privacy Incident Response Policy

EISP-7b.3: Policy for Sanctions Addressing Information Security and Privacy Violations

Noncompliance in Human-Subjects Research

Reporting Unanticipated Problems including Adverse Events

Additional Resources

Research Navigator

Mass General Brigham – Incident Reporting Fact Sheet

Partners Research Data Management Requirements

Anatomy of a Breach Presentation Slide Deck