IRB Guidance: DATA SECURITY

For more information please refer to IRB Policy & Guidance or contact the IRB at 718-613-8480 or IRB@downstate.edu

For information on data security as it relates to SUNY Downstate specific policies, please contact the Interim SUNY Downstate Information Security Officer, Lin Wang, PhD, PMO at (718) 270-4621 or LWang@downstate.edu

For informed consent disclosures related to EU GDPR requirements, contact Alexandra Bliss, Compliance Coordinator, Office of Compliance & Audit Services at (718) 270-2095 or Alexandra.Bliss@downstate.edu

For any contractual agreements related to research data security, contact Ethan Denny, Contract Manager, Research Administration at (718) 613-8551 or Ethan.Denny@downstate.edu

TABLE OF CONTENTS:

Introduction........................................................................................................................................................................... 2

Information Security Requirements................................................................................................................................. 2

Physical Safeguards............................................................................................................................................................. 2

Protocol Specific Safeguards............................................................................................................................................ 3

Technical Safeguards .......................................................................................................................................................... 3

Employee Controls............................................................................................................................................................. 4

Storage and Data Back-up.................................................................................................................................................... 5

Information Security Officer............................................................................................................................................. 5

European Union General Data Protection Regulation (EU GDPR) ................................................................................... 5

References ............................................................................................................................................................................. 5

Authors .................................................................................................................................................................................. 6
INTRODUCTION

Investigators must follow the standards outlined in the Downstate and RF policies, when using Downstate or RF resources or data.

All Research must meet the institutional requirements for electronic data and information security, including any data security plans involving the use, storage or transmission of Electronic Protected Health Information (EPHI), Electronic Personal Identifiable Information (EPII), or Electronic Sensitive Information (ESI).

This guidance applies to investigators and others approved by the Downstate Medical Center IRB, including any affected Business Associate with access to EPHI, EPII, ESI or confidential information.

INFORMATION SECURITY REQUIREMENTS

Safeguards can be physical, technical, or via employee controls and are described below.

The IRB, Privacy Officer, or Information Security Officer may consider or require additional safeguards.

PHYSICAL SAFEGUARDS

- Physical security measures must be in place. As applicable, these may include controlled access, locks, fire suppression, alarms, etc.
- Do not leave sensitive documents in plain view on your desk, computer, or on fax machines or copiers.
- Use simulated data for training purposes.
- Discard confidential and secure information in accordance with Downstate policy (e.g., Shred-It program, computer/electronic waste procedures, etc.). Do not discard any confidential and secure information in a waste receptacle or recycling bin.
- Enable a password protection/screen lock and establish automatic security timeout or auto lock after no more than 15 minutes of inactivity.
- When available, enable the application or feature to remotely trace, wipe or clear lost or stolen devices.
- Mobile devices must not be “jail broken” or “rooted” by the user.

**PROTOCOL SPECIFIC SAFEGUARDS**

- Within the study protocol or other IRB application materials, include a description of the methods to destroy data at the end of its life cycle, or data retention and disposition policies.
- Do not release or disclose data other than what is required to perform the research as approved by the IRB.
- Implement Confidentiality Agreements, Data Use Agreements, Business Associate Agreements, when needed or required.
- The user of a mobile device that is used for research must provide reasonable safeguards and manage the location of the device to prevent unauthorized access.

**TECHNICAL SAFEGUARDS**

- When transmitting EPHI, EPII, or ESI over an electronic network, include technical security measures to guard against unauthorized access.
- Research projects that contain EPHI, EPII, or ESI must reside in a centralized secure location (i.e. network file share, DMC SharePoint site or server database, secure system approved by the DMC Information Security Officer).
- OneDrive is the only cloud drive approved to use in Downstate.
- Downstate hosts REDCap on a Downstate server with a web interface. It can be used to store PHI. For more information, see: [http://guides.downstate.edu/redcap](http://guides.downstate.edu/redcap)
- EPHI, EPII, or ESI must not be stored on a local computer hard drive, non-encrypted laptop, or non-encrypted mobile device.
- Use a “Downsate.Edu” e-mail address when sending non-encrypted EPHI to another “Downsate.Edu” e-mail address.
- All Downstate business must be conducted using a downstate.edu e-mail address.
- Use a “Downsate.Edu” e-mail address to send EPHI, EPII, or ESI via encrypted emails to an external recipient. This applies to either forwarding or replying to an email.
  - The simplest way to encrypt an email message using the Downstate MS Outlook program is to enter “Confidential” without quote anywhere in the message subject.
- Encrypt any mobile device connected to a Downstate network. Call extension 4357 (HELP) for additional information.
- A secure FTP process approved by DMC Information Technology may be used to transmit EPHI, EPII, or ESI.
DMC and Non-DMC owned mobile devices (e.g., laptops, notebook, tablets, cell phones, smart phones, USB connected thumb drives, portable storage device, etc.) may be used for research; however, they cannot contain EPHI, EPII, or ESI, unless encrypted with a validated Federal Information Processing Standard (FIPS 140-2) or other encryption algorithms or protocols approved by Downstate policy (see HIS-13).

Any data repository, data warehouse, file server and/or database that stores research data must comply with Downstate policies.

OneDrive is the only DMC sanctioned cloud storage within the university.

To ensure data security when in transit, data entry or file transfers containing (EPHI), (PHI) and (PII) may be sent to an external site via a HTTPS secured website, encrypted e-mail, or via a secure file transfer, Secure File Transfer (SFTP), Virtual Private Networks (VPN), or via other methods approved by the DMC Information Security Officer.

Do not use USB drives or other removable storage devices for long-term storage or confidential or EPHI, EPII, or ESI data.

**EMPLOYEE CONTROLS**

- Principal Investigators are responsible for enforcing Downstate and RF policies related to data security.
- Passwords must comply with HIS-04, Password Policy.
- Do not share user credentials (i.e. logon and/or password) with anyone, including supervisors, immediate colleagues, or administrative support staff.
- Do not use someone else's logon and/or password.
- Change temporary passwords assigned by an administrator.
- When study personnel are no longer part of the Research team, the PI should remove their access to any identifiable research study data.
- Unauthorized access, manipulation, or disclosure of confidential data may constitute a security breach and may be grounds for disciplinary action up to and including termination of employment by the Department or School or an external institution.
- Report suspected violations to the appropriate person (e.g., Supervisor, Manager, Information Security Officer, Privacy Officer, IRB, etc.).
- Downstate and the RF will not tolerate retaliation toward or harassment of employees who in good faith report a suspected or knowing violation of policy.
- Investigators must immediately report lost or stolen mobile devices to the SUNY Downstate Data Safety Office by contacting the HELP desk (X4357) or the Downstate Medical Center Compliance Line at 1-877-349-SUNY or by making a report on the “Compliance Line” on the bottom of DMC’s webpage or [https://www.compliance-helpline.com/downstate.jsp](https://www.compliance-helpline.com/downstate.jsp)
- Investigators must follow Policy HIS-12, Mobile Device Usage, when using mobile devices in a research project.
STORAGE AND DATA BACK-UP

Take all reasonable precautions to mitigate the risk of loss, which may include storing work related data on a network drive to ensure appropriate back up.

Back-Up the research data to a server or other alternative secure location. If the data is sensitive or includes PHI, use the technical safeguards noted above.

INFORMATION SECURITY OFFICER

The Information Security Officer provides guidance to the IRB, reviews information security incidents. (S)he makes determinations of information security breach and reporting requirements to the HHS Office of Civil Rights. (S)he assists the IRB’s review of non-compliance, when applicable and is permitted to be appointed as an IRB Member.

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (EU GDPR)

If the European Union (EU) General Data Protection Regulation (GDPR) is applicable to a study, please work with the sponsor, Privacy Officer, or the Office of Compliance and Audit Services (OCAS) to include the appropriate GDPR disclosures within this consent or an addendum. The IRB will work with OCAS to confirm all required disclosures are included. Examples for when GDPR applies to the research include the following:

1) The study includes outreach and recruitment of individuals who are located in the European Economic Area (EEA), which is 28 EU member states and three additional countries (Liechtenstein, Iceland, and Norway),
2) Downstate or a site approved by the Downstate IRB is the site for a study involving the EEA and has the role of primary research site and/or lead investigator, or
3) Downstate or a site approved by the Downstate IRB collects and/or processes Personal Data (as defined by GDPR) in the EEA in connection with the study (including incidental collection of personal data on a mobile app while a research participant is travelling in the EEA).

REFERENCES

- European Union General Data Protection Regulation (EU GDPR)
- SUNY Downstate Medical Center Information Services Policies and Procedures

SUNY Downstate Medical Center IRB Guidance: Data Security
09.26.2019
Page 5
SUNY Downstate Medical Center HIS-13: Encryption and Decryption Policy
SUNY RF Acceptable Use and Security of RF Data and Information Technology

AUTHORS

Alexandra Bliss, Compliance Coordinator, Office of Compliance & Audit Services
Ethan Denny, Contract Manager, Research Administration
Dilip Nath, Interim VP & CIO
Kevin L. Nellis, MS, CIP, Executive Director Human Research Protections and Quality Assurance
Lin Wang, PhD, PMO, Interim SUNY Downstate Information Security Officer

REVIEW AND APPROVAL HISTORY

Original Issue Date: 12.27.2016
Supersedes: 12.27.2016, 12.28.2016, 1.23.2019, 09.05.2019
Revision Date: 9.26.2019

<table>
<thead>
<tr>
<th>Date Reviewed &amp; Approved</th>
<th>Revision Required</th>
<th>Responsible Staff Name and Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>12.27.2016</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>12.28.2016</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>01.23.2019</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Guidance updated with input from Dr. David Loewy.
<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>09.05.2019</td>
<td>X</td>
<td>Kevin Nellis, Executive Director Human Research Protections and Quality Assurance Lin Wang, PhD, PMO, Interim SUNY Downstate Information Security Officer</td>
<td>Guidance updated with input from Lin Wang, PhD, PMO. GDPR section updated.</td>
</tr>
</tbody>
</table>