IRB GUIDANCE: INFORMATION SECURITY

TABLE OF CONTENTS:

Introduction **2**

Downstate Information Security Officer **2**

Contacts **3**

Suspected Breach **3**

Information Security Requirements **3**

Physical Safeguards **3**

Technical Safeguards **4**

General 4

Downstate E-Mail 5

Storage and Data Back-up 5

Virtual, Internet & Telehealth Platforms 5

Remote Consent **6**

Electronic Consent; Electronic Signatures **6**

Administrative Safeguards **7**

General 7

Protocol Specific Safeguards 8

Agreements 8

DUA Or BAA related to Data Security 8

Social Media 9

Research Subject to GDPR 9

Research Subject To Other International Regulations 10

California Privacy Rights and Enforcement Act (CPRA)/ California Consumer Privacy Act (CCPA) 11

References 11

Authors 11

Review and Approval History 11

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 (E-PHI), SUNY Downstate Health Science University (SDHSU) Protected Data (PD), SDHSU Sensitive Data (SD), or SDHSU General Business Data (GBD). For the purposes of this guidance, these data are collectively referred to as “Sensitive Data” in the text below.

E-PHI is any electronic PHI, which is healthcare information associated with a HIPAA identifier. HIPAA identifiers are outlined in Policy HIPAA-6, De-Identification of Information

SDHSU Protected Data, SDHSU Sensitive Data, or SDHSU General Business Data are defined in Policy HIS-22, Cloud Data Security Protocol (DHSU Intranet Link).

This guidance applies to investigators and others approved by the Downstate IRB, including any affected Business Associate with access to the above data.

DOWNSTATE INFORMATION SECURITY OFFICER

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

CONTACTS

For information on data security as it relates to SUNY Downstate specific policies, please contact the Information Security Officer, Igor Gorelik at igor.gorelik@downstate.edu.

For questions related to EU GDPR requirements, contact Alexandra Bliss, Director or Compliance, Office of Compliance & Audit Services at Alexandra.Bliss@downstate.edu.

For questions for the Downstate Privacy Officer, contact Shoshana Milstein, Vice President, Compliance and Audit Services at shoshana.milstein@downstate.edu

For any contractual agreements related to research data security, contact Sponsored Programs Administration.

For SUNY RF policies, related to RF business applications, see: Acceptable Use and Security of RF Data and Information Technology or contact: Gerard Drahos, Vice President Chief Information Officer, Corporate Information Security Officer; Gerard.Drahos@rfsuny.org; Phone: (518) 434-7205.

For reporting suspected breach involving the RF business system, contact the Downstate RF Operations Manager, Dr. David Christini, PhD, at David.christini@downstate.edu

For more general information or questions, please contact the Downstate IRB at IRB@downstate.edu.

SUSPECTED BREACH

In the event of a suspected breach, immediately contact the Downstate IRB, Downstate Information Security Officer, and Downstate Privacy Officer, and report the event to the IRB in writing in accordance with Policy IRB-01.

In addition to notifying the above individuals and IRB for a suspected breach involving an RF business management system, notify the Downstate RF Operations Manager who will then notify the RF Information Security Officer.

INFORMATION SECURITY REQUIREMENTS

Safeguards can be physical, technical, or administrative 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.

TECHNICAL SAFEGUARDS

GENERAL

- When transmitting Sensitive Data over an electronic network, utilize technical security controls (such as encryption) to guard against unauthorized access.
- Research projects that contain Sensitive Data must reside in a centralized secure location (i.e., network file share, server database, secure system approved by the Downstate Information Security Officer).
- OneDrive is the only cloud drive approved for use at Downstate; however, it cannot be used for EPHI or PD. For more information see Policy HIS-22.
- Downstate hosts REDCap on a Downstate server with a web interface. It can be used to store EPHI. For more information, see: http://guides.downstate.edu/redcap
- Sensitive Data must not be stored on a local computer hard drive, non-encrypted laptop, or non-encrypted mobile device. All mobile devices intended for Downstate business/research use of E-PHI must be provided to IT for enrollment into the Mobile Device Management (MDM) platform. For more information see Policy HIS-22
- Messages sent within Downstate’s network (from one Downstate.edu account to another) are automatically secured. Emails containing Sensitive Data that are sent outside of Downstate’s network (including forwarding or replying to external emails) MUST be encrypted. **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.
- Downstate and Non-Downstate 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 Sensitive Data, 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.
- To ensure data security when in transit, data entry or file transfers containing Sensitive Data may be sent to an external site via a HTTPS secured website, encrypted e-mail, or via a Secure File Transfer Protocol (SFTP), Virtual Private Networks (VPN), or via other methods approved by the Downstate Information Security Officer.
- Do not use USB drives or other removable storage devices for long-term storage of Sensitive Data.

DOWNSTATE E-MAIL

All Downstate business must be conducted using a downstate.edu e-mail address.

All members of the Downstate workforce MUST use their Downstate e-mail address when communicating with the Downstate IRB and when setting up accounts to use IRB systems (e.g., such as IRBNet, Huron Click, Downstate MyResearch, etc.).

Note: This does not apply to temporary members of the Downstate workforce and others who are not provided with a Downstate e-mail address.

STORAGE AND DATA BACK-UP

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

Back-Up the research data to a Downstate approved server or other alternative secure location. If the data is Sensitive Data, use the technical safeguards noted above.

VIRTUAL, INTERNET & TELEHEALTH PLATFORMS

When approved by the Downstate IRB, the following platforms may be used for interviews, focus groups or obtaining informed consent/HIPAA authorizations, remote communications, data collection, and data storage that involve PHI:

- Applications through software available through the Downstate HELP Desk:
    - Microsoft Teams (BAA in place with Downstate)
    - Doxy.Me
    - REDCap hosted by Downstate.
        - *Note: The REDCap system used at Downstate is HIPAA compliant; however, there is no documentation in place for 21 CFR Part 11 certification (therefore e-consent cannot be used for FDA regulated clinical investigations).*

- Applications used in collaboration with external sites:
    - When PHI is shared from Downstate in an Electronic Data Capture (EDC) system, the EDC must be HIPAA compliant.
    - When PHI is included in REDCap or software platforms hosted at other sites, written documentation about the system must be approved by the Downstate Information Security Officer to demonstrate that it is fully compliant with privacy and security guidelines defined by HIPAA and the Federal Information Security Management Act (FISMA). It is highly recommended that sites use MS SQL server version 2016 or newer to support strong encryption. The REDCap database should also be encrypted.
        - When REDCap hosted at an external site is used to obtain e-signatures for informed consent for FDA regulated clinical trials, REDCap must be compliant with HIPAA and 21 CFR Part 11 (electronic records regulations).
- When applicable the platform must be approved by Information Security and compliant as follows:
    - 21 CFR Part 11 compliant for FDA regulated clinical investigations,
    - ISO certified when required, and/or
    - Compliant for foreign regulations as applicable to the research.

WARNING: DO NOT use Zoom, One Drive, MS Forms, Qualtrics, or Google Forms for research activities involving PHI, as there are no BAAs in place with Downstate for these platforms.

REMOTE CONSENT

With IRB approval, research participants may participate in studies in which they do not have to meet directly with the investigator. In general, informed consent and authorization may be initiated and obtained through the following methods as recruitment policy allows (i.e., telephone contact, email, letter, fax).

Fax transmissions from Downstate should use the approved HIPAA Facsimile Cover Page.

When a consent document contains PHI, electronic communications containing PHI for research purposes must be encrypted to Downstate standards.

ELECTRONIC CONSENT; ELECTRONIC SIGNATURES

With IRB approval, an investigator may obtain electronic consent and obtain electronic signatures, when the IRB waives documentation of informed consent or when all applicable regulatory requirements for an electronic signature are met. For more information on regulatory requirements refer to:

- FDA Regulations (21 CFR part 11): Electronic Records; Electronic Signatures
- United States Code Title 15- Electronic Signatures in Global and National Commerce Act, Subchapter I- Electronic Records and Signatures in Commerce (Esign Law), October 1, 2000
- New York State Technology Law Article 1- Electronic Signatures & Records Act (ESRA), September 28, 1999 and amended August 6, 2002
- 9 NYCRR Part 540- ESRA Amended Regulations, May 7, 2003
- NYS Office for Technology- ESRA Guidelines, May 26, 2004
- National Archives & Records Administration- Records Management Guidelines for Agencies Implementing Electronic Signature Technologies, October 18, 2000
- NYS Archives & Records Administration- Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment, published 1998
- 10 NYCRR Part 405.10- Medical Records, February 25, 1998
- 42 CFR Section 482.24- CMS Conditions of Participation for Hospitals, Medical Record Services
- Joint Commission Hospital Accreditation Standards- IM.2.20

ADMINISTRATIVE SAFEGUARDS

GENERAL

- Principal Investigators are responsible for enforcing Downstate and RF policies related to data security.
- Principal Investigators are responsible for ensuring that all study personnel have received appropriate training in accordance with Downstate Policies.
- 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 re-use the same passwords across different media.
- 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, Compliance Line, IRB, etc.).
- General reports or concerns related to privacy or mis-use of data should be reported to the IRB Office, the HIPAA Privacy Officer or to the Downstate Compliance Line at 1-877-349-SUNY or by making a report on the "Compliance Line" on the bottom of Downstate's webpage or https://www.compliance-helpline.com/downstate.jsp

- 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).
- Investigators must follow Policy HIS-12, Mobile Device Usage, when using mobile devices in a research project.

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 security measures used for data retention.
- Do not release or disclose data other than what is required to perform the research as approved by the IRB.
- The user of a mobile device that has been approved for use in research must provide reasonable safeguards and manage the location of the device to prevent unauthorized access. All Bring Your Own Devices (BYOD) should be approved and enrolled in the MDM platform to ensure the appropriate level of security controls over data and have ability to selectively lock or wipe Downstate data only, without affective the user's personal data.

AGREEMENTS

When applicable to the research, appropriate agreements must be established prior to conducting the research. These may include any of the following:

- Data Agreements
- Data Use Agreements (DUA) for research involving limited data sets
- Business Associate Agreements (BAA)
- Material Transfer Agreements (MTA)
- Confidentiality agreements
- Confidentiality and Non-Disclosure Agreements (CDA/NDAs)

Note: For more information on agreements, please see **Step 5** on the Downstate IRB Electronic Submission webpage.

DUA OR BAA RELATED TO DATA SECURITY

When a limited data set is released outside the institution where the research takes place or obtained from an external source, a Data Use Agreement (DUA) is generally required; however, the Privacy Officer or IRB may consider the approval of a HIPAA authorization or waiver to release the data.

A Business Associate Agreement (BAA) is required when providing a vendor (e.g., transcription service, data center, etc.) with PHI information for the purposes of the research.

A DUA or BAA for unfunded studies must be reviewed and approved by Downstate General Counsel and the Downstate Hospital Privacy Officer, before being presented to the individual with Downstate signatory authority.

A DUA or BAA for funded studies must be reviewed and approved by Sponsored Programs Administration (SPA) and are signed by SPA.

All original signed and dated DUA and BAA forms must be retained in the investigator's research files, secure but readily retrievable.

When a human research project is approved by the IRB as "Exempt" and involves PHI, a HIPAA Waiver, a HIPAA Authorization, a Data Use Agreement (DUA), or a Business Associate Agreement (BAA) is usually still required.

For more information and for Downstate templates, please see see **Step 5** on the Downstate IRB Electronic Submission webpage.

Note: If informed consent is obtained from a research participant when a limited data set is released outside the institution where the research takes place, a HIPAA authorization should be obtained, indicating the disclosure. A "limited data set" is a data set that is stripped of certain direct identifiers that are specified in the Privacy Rule.

SOCIAL MEDIA

Social media platforms may be considered for recruitment of potential research participants if approved by the Downstate IRB.

The Downstate IRB will consult with the Office of Communications and Marketing; the Office of Compliance and Audit Services, and General Counsel, for input as applicable when approving a social media ad. It is permissible to use the files without an IRB approval stamp when stamping is not possible.

RESEARCH SUBJECT TO GDPR

At the present time, Downstate cannot conduct research that is subject to compliance with the EU General Data Protection Regulation (GDPR).

- GDPR covers all of the European Union Member States, which includes: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.
- On January 1, 2021, the United Kingdom's UK GDPR rules became effective. The UK GDPR absorbs the privacy compliance requirements of the EEA's GDPR and combines them with

the requirements of the UK's Data Protection Act. The United Kingdom includes: Channel Isles, England, Northern Ireland, Scotland, and Wales.
- GDPR also includes European Economic Area Countries, such as Iceland, Lichtenstein, and Norway.

Examples for when GDPR applies to the research include the following:

- Downstate (or a site approved by the Downstate IRB) collects and/or processes Personal Data (as defined by GDPR) from people physically located in the above countries (including collection via Internet research) at the time of data collection, even if they are not citizens.
- Downstate (or a site approved by the Downstate IRB) is the primary research site of a multi-site study that includes recruitment of individuals from the above locations or direct data exchange with any research site or entity in any of the above locations.
- The lead investigator is from Downstate (or a site approved by the Downstate IRB) for a multi-site study that includes recruitment of individuals from the above locations or exchange of Personal Data (as defined by GDPR) with any research site or entity in the above locations.

The GDPR requirements are much different than US regulations. Even when Downstate is not considered engaged in human research as determined by US regulations, Downstate is prohibited from participation in research or data exchange with the above countries which are subject to GDPR, at this time.

RESEARCH SUBJECT TO OTHER INTERNATIONAL REGULATIONS

The Downstate IRB will consider the review of human research that must comply with other international privacy or data protection or human research regulations in consultation with the Privacy Officer, Information Security Office, General Counsel, and Sponsored Programs Administrations, as applicable, to confirm the research complies with SUNY/RF and foreign regulations. In general, these projects must also be reviewed by the local IRB/IEC (or equivalent) of the international site, when the study includes outreach and recruitment of individuals located at the international site or when data is obtained from the international site. The Downstate PI may be required to obtain the current English version of the applicable regulations from the local site or sponsor in order to make this determination, if they are not readily available to the IRB.

When collaborating with international sites that are not subject to GDPR, please request an IRB Determination Letter to indicate Downstate IRB approval is not required for the following situations:

- When Downstate is “not engaged” in human research (i.e., releasing a de-identified data set from Downstate and not interacting or intervening with research participants).
- When the Downstate workforce serves in a consultant or investigator capacity on a project when activities do not constitute human research.

CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT (CPRA)/ CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

In general, the California Privacy Rights and Enforcement Act (CPRA)/ California Consumer Privacy Act (CCPA) regulations do not apply to non-profit organizations or government agencies; however, when applicable to a multi-site study, these requirements should be reviewed by the external site to ensure compliance, when the California regulations apply.

REFERENCES

- California Consumer Privacy Act (CCPA) regulations
- California Privacy Rights and Enforcement Act (CPRA)
- Complete Guide to GDPR Compliance
- Cookieyes, Guide to the UK GDPR
- Do You Know Which Countries are Included in GDPR Compliance?
- European Union General Data Protection Regulation (EU GDPR)
- Office of Civil Rights Notification of Enforcement Discretion for Telehealth
- SUNY Downstate Information Services Policies and Procedures (Downstate Intranet link)
- SUNY RF Acceptable Use and Security of RF Data and Information Technology
- UK Data Protection Act 2018

AUTHORS

Alexandra Bliss, Compliance Coordinator, Office of Compliance & Audit Services
Ethan Denny, Contract Manager, Research Administration
Igor Gorelik, Information Security Officer,
Kevin L. Nellis, Executive Director Human Research Protections and Quality Assurance

REVIEW AND APPROVAL HISTORY

Original Issue Date: 12.27.2016

Supersedes: 12.27.2016, 12.28.2016, 1.23.2019, 09.05.2019, 9.26.2019, 01.20.2021, 10.22.2021, 11.04.2021

Revision Date: 03.24.2024

Date Reviewed & Approved	**Revision Required**		**Responsible Staff Name and Title**	
	Yes	No		

12.27.2016		X	Kevin Nellis, Executive Director Human Research Protections and Quality Assurance	
12.28.2016	X		Kevin Nellis, Executive Director Human Research Protections and Quality Assurance	
01.23.2019	X		Kevin Nellis, Executive Director Human Research Protections and Quality Assurance David Loewy, PhD SUNY Downstate Information Security Officer	Guidance updated with input from Dr. David Lowey.
09.05.2019	X		Kevin Nellis, Executive Director Human Research Protections and Quality Assurance Lin Wang, PhD, PMO, Interim SUNY Downstate Information Security Officer	Guidance updated with input from Lin Wang, PhD, PMO. GDPR section updated.
9.26.2019	X		Kevin Nellis, Executive Director Human Research Protections and Quality Assurance Lin Wang, PhD, PMO, Interim SUNY Downstate Information Security Officer	Updated technical specifications for encrypted e-mails and use of REDCap
01.20.2021	X		Kevin Nellis, Executive Director Human Research Protections and Quality Assurance Igor Gorelik, Information Security Officer Alexandra Bliss, Compliance Coordinator	Updated or added information for new Information Security Officer, revised IT policies, references to RF policies, CA regulations, agreements, social media, virtual and internet platforms, remote consent, DUA, BAA, reporting suspected breach. Reorganized based on categories of safeguards. Changed the term Electronic Personal Information to Electronic Confidential Information to

				be in alignment with IT and OCAS policies.
01.21.2021	X		Kevin Nellis, Executive Director Human Research Protections and Quality Assurance	Minor edits and formatting changes made.
10.22.2021	X		Igor Gorelik, Information Security Officer Shoshana Milstein, Senior Vice President, Compliance and Audit & Privacy Officer Kevin Nellis, Executive Director Human Research Protections and Quality Assurance	Updated information on social media and foreign regulations.
11.04.2021	X		Kevin Nellis, Executive Director Human Research Protections and Quality Assurance	Updated information on social media and foreign regulations with additional input from OCAS, SPA, Information Security Officer, Privacy Officer, General Counsel and feedback from various investigators.
03.24.2023	X		Kevin Nellis, MS Executive Director Human Research Protections and Quality Assurance Clinton D. Brown, MD, FASN, FAHA, FNLA Chair, Downstate IRB & Privacy Board	Updated information to rescind COVID-19 risk mitigation strategies with input from the IRB, OCAS, SPA, Information Security Officer, Privacy Officer.