Table of Contents

1.0 Purpose

This SOP describes the Biopharmaceutical Development Program (BDP) procedure to ensure the protection of personally identifiable, sensitive, and confidential information resulting from NIH & NCI supported research or belonging to the federal government. This SOP enumerates the BDP policy, requirements, and procedures that relate to personnel and patient information that can potentially identify a person, to privacy rights, and to comply with associated Health Insurance Portability and Accountability Act of 1996 (HIPAA), Personally identifiable information (PII), and Protected Health Information (PHI) regulations.

2.0 Scope

This SOP applies to BDP employees that may access health related data or information that could potentially identify patients and other persons. This document covers what information is protected and how protected health information can be used and disclosed.

This SOP does not apply to de-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

3.0 Background

Protected Health Information & Personally Identifiable Information – The HIPAA/HITEC Privacy Rules protect all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual,
- the past, present, or future payment for the provision of health care to the individual,
- that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

Protection of patient identifiable health information is achieved by the removal of specified identifiers of the individual and ensuring that remaining information could not be used to directly or indirectly identify the individual.

Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number, etc.).

4.0 Policy

It is the policy of the BDP to comply with both the letter and spirit of federal, state, and local regulations. The BDP expects all employees to follow this SOP and ensure that protected health information (PHI) will be considered confidential and will be protected from inappropriate release to protect PHI for patients, government and non-government employees, and the public.

5.0 Authority and Responsibility

5.1 BDP Program and Technical Director

- Enforces compliance with this SOP.
- Takes corrective action if the BDP is found to be out of compliance

5.2 Director of Regulatory Compliance

- Takes corrective action if the BDP is found to be out of compliance
- Enforces compliances to this SOP in the event the BDP Director is unavailable.

5.3 Biopharmaceutical Quality Assurance (BQA) & Regulatory Affairs (RA) Management

- Prepares and conducts training and documents compliance with this procedure.
- Enforces compliances to this SOP in the event the BDP Director is unavailable.

5.4 BDP Supervisors and Managers

- Ensures that their employees that collect, use, or control access to personal information receive appropriate training and understand their responsibilities and obligations with respect to privacy and confidentiality.

5.5 BDP Employees who collect, use, or control access to personal information

- Ensures compliance with the requirements specified in this procedure.

5.6 BDP RA

- Provides a written response to Regulatory Agency inquiries and inspections.

6.0 Definitions & Abbreviations

6.1 **HIPAA – Health Insurance Portability and Accountability Act** (1996)

6.2 **HITECH – Health Information Technology for Economic and Clinical Health** (2009 & 2013)

6.3 **PII – Personally Identifiable Information is:**

6.3.1 Data that could potentially identify a specific individual.

6.3.2 Information that can be used to distinguish one person from another.

6.3.3 Information that can be used to defeat an anonymous state of data or documents/records, e.g., codes, passwords, information lists, etc. that can be used, when coupled with other available information, to directly or indirectly identify an individual.

6.3.4 Patient (Person) identification includes, but is not limited to, the following:

- Name
- Address
- Date of birth
- Facility admission or discharge dates
- Telephone numbers
- Driver’s license number
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate & license numbers
- Vehicle license plates
- Personal device serial numbers
- Web addresses (URL)
- Internet protocol (IP) address
- Biometric identifiers – finger & voice prints, retinal scans, etc.
- Photographic images

6.4 **PHI – Protected Health Information**

- Information that relates to the physical or mental health of an individual
- Information that identifies an individual or may be used to identify an individual
- Health related data maintained or transmitted in any form including verbal, written, or electronic.

6.5 **Covered Entities –** Those entities that must comply with HIPAA regulations. Covered entities include health care providers, including researchers, health plans/insurers, health care clearing houses (billing, etc., services). Business Associates, those that perform certain functions or activities that involve the use of PHI, are considered covered entities.

6.6 **Limited Data Set (LDS) –** An LDS lacks specific PII/PHI identifiers such as name, address, phone numbers, etc. An LDS may contain date of birth, date of death, city, state, or zip code.

6.7 **Privacy Rule –** A Federal law, part of HIPAA, that gives individuals rights concerning their health information. It sets rules and limits on who can access or receive health information.

6.8 **Security Rule –** A Federal law, part of HIPAA, that requires security for health information in electronic form.

6.9 **BDP** – Biopharmaceutical Development Program

6.10 **Security Incident –** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operation in an information system. An incident will become a breach if it involves the actual or suspected loss of PII/PHI.

6.11 **Breach –** The impermissible use or disclosure, under the Privacy Rule, that compromises the security or privacy of PII/PHI is presumed to be a breach unless it can be proven that there is a low probability of PII/PHI compromise as per a risk assessment/investigation.

7.0 Procedure

7.1 The handling of PII & PHI must comply with HIPAA/HITEC requirements. Refer to the references in section 8.0.

7.2 **Patient Identification**

7.2.1 Proper and clear patient identification is required and is important to prevent mix-ups and mis-identifications.

7.2.2 Patient identification such as apheresis cell donor identification that includes name and/or a unique code must clearly identify the donor.

7.2.3 Autologous products, that may only be administered back to the donor, must be clearly identified with donor/recipient identification to prevent mix-ups.

7.2.4 Allogeneic products must be clearly identified with the intended recipient identification.

7.3 Employee Identification

7.3.1 Employees that have a need to access PHI & PII and are properly authorized to access PHI & PII must be clearly identified. BDP employees must read ***SOP 21406 - Personnel Signature and Initial Verification System*** and complete Form 21406-01 Signature File and Electronic Signature Equivalency Statement to identify their signatures.

7.3.2 Employees must have on their person at all times approved identification such as PIV cards, Protective Services issued temporary cards, driver's license, etc.

7.3.3 Only employees that have passed at least a Public Trust Security Clearance and possess an official PIV card are allowed access to records and materials that include patient PHI.

7.3.4 BDP employees are not to leave PIV badges unattended.

7.4 Training and Qualifications of Employees

7.4.1 Only employees that have passed the NIH Privacy Awareness Course, Leidos, and/or BDP PII/PHI compliance and handling training are allowed access to records and materials that include patient PHI.

7.4.2 Training of BDP employees is conducted and documented in accordance with ***SOP 21600 - Training and Qualification of Personnel in a CGMP Environment.***

7.4.3 Employee HIPAA training may include:

- Classroom instruction
- Reading and understanding this SOP
- Passing a written test with at least 80% of the questions being answered correctly.

7.4.4 Employees must successfully pass training requirements every two years.

7.4.4.1 Successfully completing the NIH Privacy Awareness Course, Leidos, BDP, or other official HIPAA, HITEC, or related training satisfies this requirement.

7.4.4.2 Training must be properly documented.

7.5 Protecting Health Information (PII & PHI)

7.5.1 Ensure delivery of PII/PHI to intended recipient.

7.5.2 Observe “Minimum Necessary” rule when handling PII/PHI information at all times.

7.5.2.1 Minimum Necessary – Only that information that is needed for immediate use or disclosure

7.5.3 Use PII/PHI only for the purpose for which it was collected.

7.5.4 Use limited PII/PHI data sets (LDS) and de-identified PII/PHI when appropriate.

7.5.4.1 LDS lacks specific PII/PHI identifiers such as name, full address, phone numbers, etc. LDS may contain date of birth, date of death, city, state, or zip code.

7.5.4.2 De-identified PII/PHI – Whenever possible and appropriate, PII & PHI should be de-identified. There are no restrictions on the use or disclosure of de-identified health information. An individual’s identity must not be determinable, directly or indirectly, through de-identified health information. Remove all common and specific identifiers from the data/document.

7.5.5 Keep PII/PHI out of sight when visitors or unauthorized individuals are present.

7.5.6 Never leave documents containing PII/PHI at printers, copiers, and fax machines.

7.5.7 Secure all PII/PHI information (paper and electronic formats) when left unattended.

7.5.8 Log off or lock computer systems when leaving them unattended.

7.5.9 No PII/PHI data is to be stored on local hard drives or laptops.

7.5.10 Ensure PII/PHI data is stored ONLY on a network server that is regularly backed up.

7.5.11 Use the telephone to communicate discreetly. Verify the identity and authority of the person you are communicating with before disclosing any PII/PHI.

7.6 **PII & PHI Disposal**

7.6.1 Shred PII/PHI using only a cross-cut shredder or locked burn box

7.6.2 Contact IT for the pickup and disposal of flash drives, CD/DVDs and Computer Hardware; all items for disposal should remain in a locked environment until pickup.

7.6.3 Disposal and Handling of Biological and Laboratory Waste Labeled with PHI/PII.

7.6.3.1 Remove or completely deface the PII from the vial, bag or container and then handle as normal laboratory or infectious waste as appropriate.

7.6.3.2 Or alternatively, if the waste is infectious or potentially infectious, autoclave the material yourself and place it into a Biohazardous Waste box. Waste containing PII must be segregated from other waste streams and labelled to keep the content secured. Biohazardous Waste boxes containing PII will be moved to the medical waste storage room B1505.

NOTE: Do not place autoclave waste that contains PII in a white autoclave bucket for FME Service Staff to autoclave. This waste will be placed in a landfill for disposal, which may violate laboratory PII or CLIA guidelines.

7.6.3.3 Read and follow **EHS SOP; EHS-WM-2.1, *Biological Waste Handling and Disposal for the Advanced Technology Research Facility***.

7.7 Computer Related Security

7.7.1 Ensure that only authorized individuals can access electronic health information. Follow the three Security Rule safeguards:

7.7.1.1 Administrative Safeguards – BDP employees must maintain awareness of and comply with BDP, Leidos, NCI, NIH, and other policies, regulations, and procedures to protect PHI & PII. The requirements listed in this SOP must be followed.

7.7.1.2 Technical Safeguards – The BDP complies with FDA 21 CFR, Part 11, *Electronic Records; Electronic Signatures* regulations. Doing so ensures compliance with HIPAA Technical Safeguard requirements and includes:

- Access control using passwords and PIV cards
- The generation of an audit trail to record who has accessed computer systems and data
- User authentication including user name and password
- Encryption of PII, PHI, and other data when transmitted electronically
- Backing up data on a regular basis.

7.7.1.3 Physical Safeguards – Employees are responsible for ensuring that only authorized users may access facilities, laboratories, computers, and other equipment that contains PII & PHI. Computers must not be left unattended when PII or PHI information is displayed on the screen. Log off or power down computers when not in use. Secure USB memory devices, laptops, government issued cell phones, and related items when not in use, see below.

7.8 E-mail & Electronic Transfer of Files

7.8.1 Prior to sending PII/PHI electronically, ensure that the intended receiver of transmitted PII/PHI is authorized to receive the information.

7.8.2 E-mail and the electronic transfer of files containing PII/PHI must be encrypted.

7.8.2.1 Encrypt e-mail using the Secure MIME (S/MIME) standard.

When sending e-mails that may contain PHI or PII, Outlook users should open “New E-mail,” click on “File,” then “Properties,” click on “Security Settings,” and click the box “Encrypt message contents and attachments.”

7.8.2.2 Send data and files that contain PHI or PII using the Secure E-mail & File Transfer Service (SEFT).

7.8.3 The Secure E-mail and File Transfer User Guide for Employees and Contractors can be accessed at:

[redacted]

7.8.4 If e-mail is received with unencrypted PII/PHI. Respond back to the sender using text in Attachment 1, *Response to Email Received with Unencrypted PII/PHI*.

7.8.4.1 Notify BDP QA/RA Management whenever unencrypted e-mail with PII or PHI is received.

7.8.5 Two-Factor Authentication, e.g., PIV card and password, is required for Web Mail (mail.nih.gov)

7.8.6 Avoid clicking on suspicious links or unknown attachments within Emails – AVOID getting trapped in phishing attacks and scams. Report any incidents to IT personnel immediately!

7.9 Laptop and Desktop Computers

7.9.1 Only Government-owned encrypted Laptops are allowed for use.

7.9.2 Authorized Laptop Users must have Laptop checked during semi-annual check-ins; this ensures the laptop has updated security software.

7.9.3 Lock up Laptops when not in use.

7.10 External Media Devices

7.10.1 Use only encrypted CD/DVDS and USB flash drives when transferring or storing PII/PHI data; no personal flash drives are to be used.

7.10.2 All External Media/Devices containing PII/PHI must be stored in a locked environment when not in use.

7.11 Mobile Devices (Cell Phones and Related)

7.11.1 Be vigilant about not losing or misplacing your mobile device.

7.11.2 Don't store passwords or PII/PHI on your mobile device.

7.11.3 Use caution when connecting to a public wireless network due to the open transmission of unsecure Wi-Fi; your data and/or device could be compromised.

7.12 Remote Access

7.12.1 Only access NIH managed networks from NIH equipment and, when offsite, use NIH VPN.

7.12.2 Only use VPN on cellular networks (mobile hot spot, 3G, 4G, etc. services) to access the Internet while traveling. Do not use public wireless networks.

7.13 Privacy and Security Incident Procedures

7.13.1 Report potential privacy breaches or security incidents, including stolen or lost computers and other equipment that may contain PII/PHI, AS SOON AS DISCOVERED, to your Supervisor. If your Supervisor is unavailable, please immediately contact the BDP QA/RA Management.

7.13.2 If you have accidentally sent an unencrypted e-mail containing PII/PHI:

7.13.2.1 **Contain** the PII/PHI. Attempt to recall the e-mail. Immediately call or send a separate e-mail to the person you sent the unencrypted e-mail and ask them to delete the e-mail right away.

7.13.2.2 **Protect** the PII/PHI by deleting the e-mail from your "Sent" directory.

7.13.2.3 **Contact** IT and the BDP PII/PHI Compliance Team (see 7.13.6) for guidance.

7.13.2.4 **Inform** your supervisor.

7.13.2.5 **Document** what happened using the issue review system. See Section 7.13.5.

7.13.3 If you have received PII/PHI and aren't supposed to or you receive an unencrypted e-mail with PII/PHI:

7.13.3.1 **Contain** the PII/PHI. Do not respond to the e-mail or forward to anyone else.

7.13.3.2 **Protect** the PII/PHI. Permanently delete the e-mail as soon as possible.

7.13.3.3 **Contact** IT and the BDP PII/PHI Compliance Team (see 7.13.6) for guidance.

7.13.3.4 **Inform** the group that sent the PII/PHI using a separate e-mail that includes the statement in Attachment 1.

7.13.3.5 **Document** what happened using ***Issue Review of Quality Events*** (SOP 21919). If required as part of the investigation, initiate a deviation system.

7.13.4 Supervisors shall notify the BDP QA/RA Directors as soon as possible.

7.13.5 Inappropriate disclosure of BDP product patient information, a PHI/PII breach, is considered a deviation. If, as required as part of the Issue Review, initiate a Deviation in accordance with ***SOP 21301 - Deviations from Written Documents***.

7.13.6 Contact a member of the Compliance Team if you have questions.

BDP PII/PHI Compliance Team:

- Program and Technical Director
- Director of Regulatory Compliance
- Associate Director of Regulatory Affairs

8.0 References and Related Documents

SOP 21301 - *Deviations from Written Documents and Corrective and Preventative Actions*

SOP 21406 - *Personnel Signature and Initial Verification System*

SOP 21600 - *Training and Qualification of Personnel in a CGMP Environment*

45 CFR 160.103 Definitions

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

HIPAA – Health Insurance Portability and Accountability Act, 1996

HITECH – Health Information Technology for Economic and Clinical Health, 2009 & 2013

21 CFR, Part 11 Electronic Records; Electronic Signatures

§ 11.30 Controls for Open Systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

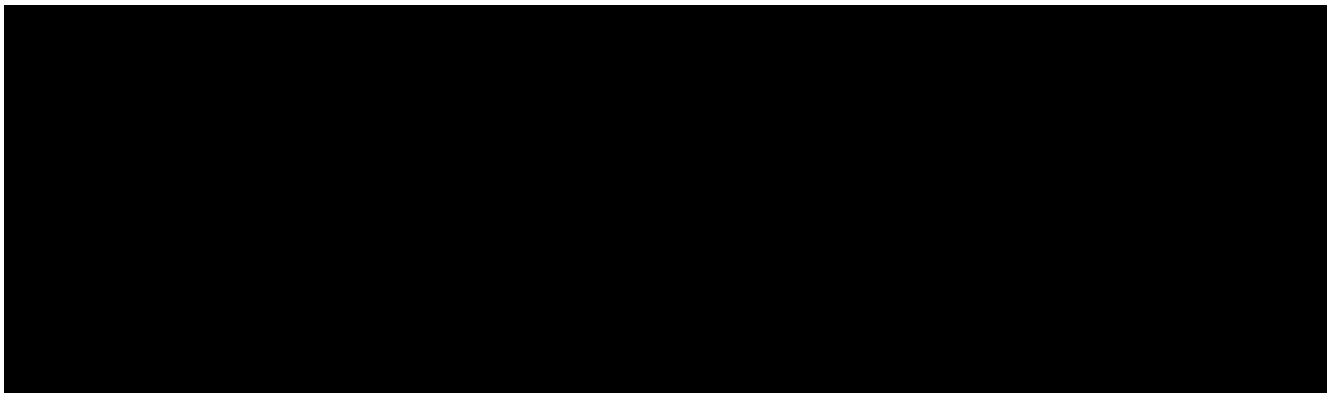
- Useful data security information can be accessed at:
  - NIAID SOP: https://www.niaid.nih.gov/research/data-security
  - HHS Security Awareness and Training Website: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html

9.0 Attachments

9.1 **Attachment 1** Standard Response to send when you have received unencrypted email that contains PHI

10.0 Change Summary

[redacted]



Attachment 1

STANDARD RESPONSE TO SEND WHEN YOU HAVE RECEIVED UNENCRYPTED EMAIL THAT CONTAINS PHI

Instructions for use: copy and paste the statement below into your email when responding to unencrypted email that contains PHI

The email you sent me contained (describe the PHI, without including names or other PHI) and was unencrypted. We are required by HIPAA/HITECH regulations to notify the sender to remember to send Protected Health Information (PHI) by encrypted email only. Thank you for your help in protecting the patient's privacy and in keeping us compliant with the regulations. NIH Policy MAS 09-3 states that all Personally Identifiable Information (PII) must be protected by encryption during transmission. PHI is part of PII. In addition to use of PKI encrypted email, the NIH maintains a Secure Email and File Transfer Service that all NIH employees have access to utilize. The link for this site is https://secureemail.nih.gov/bds/Main.do