

SOP#: AOCR-16

Version #: 1.1

Approved Date: 12/2020

NCI Clinical Director Signature:

Submission of Privacy Incidents and Breaches

Next Review Date: 09/2022

Review Interval Period: Biennial



William L. Dahut, M.D. 12/28/2020

## POLICY

All potential or actual privacy incidents and breaches that resulted from an NCI staff/contractor action must be reported to the Incident Response Team (IRT) within one hour of incident being discovered. If a CC or other Institute staff/contractor caused the privacy incident involving an NCI patient, then that staff/contractor is responsible for reporting the incident to the IRT. The NCI staff/contractor staff may be responsible for reporting to the IRB if applicable.

## PURPOSE

To identify the actions necessary to report a potential or actual privacy incident or breach. Please see Appendix A for types of information that may constitute a privacy incident or breach. If information is sent to an unintended recipient or sent outside of the NIH email system in an unsecure fashion, this could be a privacy incident or breach and must be reported. Please see Appendix B for some examples of privacy incidents.

## RESOURCE

- NIH Privacy Program [website](#)  
Includes on bottom left side:
  - Privacy Program FAQs
  - Privacy Incidents and Breach Response
  - IC Privacy Coordinators
- NIH Office of Intramural Research Policies & Guidance [website](#)  
Policy 107 - *Privacy and Confidentiality*

## PROCEDURES

### STEP 1: Report Potential Privacy Incident

- Within 1 hour of discovering the privacy incident, send an email describing the incident to [IRT@nih.gov](mailto:IRT@nih.gov) and "NCI CBIIT" and cc "Craig Hayn" (NCI Information Security Officer) and "NCI CCR QA." DO NOT include any Personally Identifiable Information (PII) in this email. The CCR QA mailbox includes all ORN team leads.

- If the incident involves email sent to an unintended recipient or sent unencrypted to an outside email, please ask the recipient of the email to fully delete the email from all of their email folders and to send you an email confirming that all copies of the emails were deleted. Make sure to delete the email from your sent folder and deleted/trash folder also.
- NCI CBIIT team will enter the incident into the Incident Response Team (IRT) Portal to create an incident report.
- The NCI Privacy Coordinator, Suzanne Milliard, will be automatically sent the incident report for review.

### **STEP 2: Review of Incident Report**

- The NCI Privacy Coordinator, Suzanne Milliard, will review the report and determine next steps to take.
- Suzanne will contact the Clinical Center Privacy Coordinator, Susan Martin, if the incident involves a Clinical Center patient.
- Suzanne will contact the person who reported the incident directly to obtain more information as needed.
- Suzanne will need to know the names of the staff involved in the privacy incident.
- Follow-up with the NCI Privacy Coordinator may include steps for remediation and privacy training for staff.
- After all remediation steps are communicated, the incident will be resolved in the IRT portal and a final report is sent to the appropriate individuals.

### **STEP 3: Report Incident to IRB via a Reportable Event Form (REF)**

- The team is responsible to report the privacy incident to the IRB via REF within 7 days of becoming aware of the privacy incident.
- A REF must be submitted for each protocol involved in the privacy incident.
  - For "Name the Event," select "Breach of PII"
  - For "How would you classify the event," select "Non-compliance, Other"
- The IRB will need a copy of the final incident report when it is available. If the REF was submitted prior to the final incident report, the IRB may stipulate that the report is needed. Submit once the report is available.
- Send the following to your PSO manager for the regulatory file: REF, IRB determination and incident report.

## Appendix A

### DEFINITIONS

**Health Information**: Any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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

**Individually Identifiable Health Information**: 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.

**Personally Identifiable Information (PII)**: Information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

**Protected Health Information (PHI)**: "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. "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, or
- the past, present, or future payment for the provision of health care to the individual;

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

## **Appendix B**

### **Examples of Privacy Incidents that are required to be reported:**

- Sending a Welcome letter or other communication containing patient information to the incorrect patient
- Losing/misplacing paper copies of records that contain patient information
- Sending a spreadsheet with research data to an outside collaborator without removing PII
- A laptop or portable storage device containing PII is lost or stolen, regardless if the device is encrypted or password protected
- Government issued cell phone is lost or stolen
- Sending an unencrypted email outside of NIH that contains PII