Privacy Incident Management - Reference Sheet
Scenario Examples

Scenario Examples	Privacy Incident	Security Incident	Policy Violation	Breach Risk Assessment (NIH level)	Breach Response Plan (HHS level)	General Notes
1 - Email with PII sent unencrypted to correct person within NIH - **"A user sent an unencrypted email containing PII to the intended recipient within NIH."**	Yes	No	Yes	No	No	- must report via the NIH IRT Portal - ensure all emails have been deleted - review *NIH Sensitive Information and Encryption Resource Card*
2 - Email with PII sent unencrypted to correct person outside NIH - **"A user sent an unencrypted email with an attached file that contained PII to an intended recipient, their vendor."**	Yes	No	Yes	No	No	- must report via the NIH IRT Portal - ensure all emails have been deleted - review *NIH Sensitive Information and Encryption Resource Card*
3 - Email with PII sent encrypted to wrong person within NIH - **"A user sent an encrypted email containing PII which includes first and last names, DOB, home addresses, and phone numbers to the incorrect person within NIH."**	Yes	Yes	Yes	Yes	Depends on facts (# of recipients and type of PII)	- must report via the NIH IRT Portal - ensure all emails have been deleted - review *NIH Sensitive Information and Encryption Resource Card*
4 - Email with PII sent encrypted to wrong person outside NIH - **"A user sent an encrypted email containing SSNs, first and last names, and DOBs to an unintended individual outisde of NIH."**	Yes	Yes	Yes	Yes	Yes	- must report via the NIH IRT Portal - ensure all emails have been deleted - complete investigation process by NIH PIRT/TMIR/HHS PIRT included - may require credit monitoring
5 - Record/file containing PII accessed by a hacker from an internal NIH system or application (intrusion) - **"A record/file containing PII was accessed by a hacker from an internal NIH system."**	Yes	Yes	Yes	Yes	Depends on facts (# of recipients and type of PII)	- must report via the NIH IRT Portal - complete investigation process by NIH PIRT/TMIR/HHS PIRT included - may require credit monitoring

Privacy Incident Management - Reference Sheet
Scenario Examples

Scenario Examples	Privacy Incident	Security Incident	Policy Violation	Breach Risk Assessment (NIH level)	Breach Response Plan (HHS level)	General Notes
6 - Inadvertently uploading PII to an NIH system where users with different admin roles can access all records - **"A user inadvertently uploaded files containing PII to a system within a specific IC at NIH in which users with multiple admin roles with access to this program can view the uploaded PII, but they do not have a need-to-know."**	Yes	No	Yes	No	No	- must report via the NIH IRT Portal - NIH IC should consider reviewing all admin privilege roles - user should re-take necessary training
7 - Inadvertently uploading PII to an external system where users with different admin roles can access all records - **"A user inadvertently uploaded files containing PII to an external system in which users with multiple admin roles with access to this program can view the uploaded PII that is considered Government information, but they do not have a need-to-know (e.g., NIH personnel, vendors, other external collaborators such as principal investigators at Universities)."**	Yes	No	Yes	No	No	- must report via the NIH IRT Portal - NIH IC, vendor, and/or external collaborator should consider reviewing all admin privilege roles

Definitions:

Personally Indentifiable Information (PII) - OMB Circular A-130

Sensitive Information (SI) - NIST.SP.800-150

Incident - OMB M-17-12

Breach - OMB M-17-12