****

**Appendix 4 - NEICE Data Breach Notification Process**

**(Revised November 1, 2021)**

1. **OVERVIEW of PROCESS**
2. **Initiation Activities**

Each NEICE Participant will provide the name of a single point of contact (POC) as well as a back-up POC to APHSA when the Memorandum of Understanding is signed. This POC will be responsible for alerting the Information Technology Service Provider (ITSP) of a Breach Incident in the Participant’s state or jurisdiction and is the person who would be alerted by APHSA in the event of a data breach by either another Participant or APHSA. This POC will be responsible for alerting the other state or jurisdiction personnel in Participant’s chain of Breach Notification protocols. The Participants will be asked to update this information as changes occur or at a minimum, annually.

1. **Defining whether there has been a Breach**

In the context of the NEICE MOU, a Breach shall mean all known incidents that threaten the security of the Participant’s data or databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Participant’s information technology systems with the potential to cause major disruption to normal ICPC activities. Such Breach may include an incident in which sensitive or confidential or otherwise protected information, including Public Health Information (PHI) and Personally Identifying Information (PII), is accessed and/or disclosed, stolen, or taken from a system without the prior knowledge or authorization of the system’s owner. APHSA’s Breach Incident Response Team (BIRT) will review and determine, after investigation, whether a Breach has occurred and the magnitude of the Breach. In addition, because APHSA is a Business Associate (BA) of a number of NEICE Participants, the NEICE BIRT will also review and determine, after investigation, whether a HIPAA-specific Breach of the NEICE has taken place.

There are three exceptions to declaring a Breach, according to the HIPAA Breach Notification Rule 45 CFR§§164.400.414 and adapted for use by the NEICE project. These exceptions mean that if one or more of these situations was noted, a Breach does not need to be declared:

1. The first exception applies to the **unintentional** acquisition, access, or use of protected, confidential, or health information by a person acting under the authority of a Participant, if such acquisition, access, or use was made in good faith and within the scope of authority.
2. The second exception applies to the **inadvertent** disclosure of protected, confidential, or health information by a NEICE-related authorized person to another authorized person within a Participant state, and the information has not or cannot be further used or disclosed in a manner not permitted by the NEICE or ICPC.
3. The third exception applies if the Participant has a **good faith belief** that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

Immediately upon identifying a suspected Breach Incident, the ITSP will act to secure the system and data and mitigate the incident regardless of the source or magnitude of the incident.

When the Project Director is informed of a possible Breach Incident by the ITSP, a determination will be made whether the incident falls into one of these exceptions and whether the initial investigation indicates protected information has been exposed and the magnitude of that exposure. The BIRT will not need to be convened and a formal Breach Incident Notification Process will not need to take place if an exception is noted or if the information exposed does not rise up to meet definition of PII or PHI data exposure. If it is determined that a breach incident has taken place the following investigation, reporting and notification process will go into effect.

1. **Initial Notice of Data Breach Incident**

When the ITSP becomes aware of/detects a possible Breach Incident, the ITSP will notify the APHSA Project Director within **24 hours**. This notification will include, as much as possible, the following information, using the Breach Incident Reporting Form, specifically:

* A brief description of the Breach Incident to include date of incident, date of discovery, time, duration of incident, and location of incident. Additionally, the ITSP will provide a preliminary risk assessment that identifies a high (e.g., external breach), medium (e.g., state report of internal access), or low (e.g., internal misdirected data within the system) risk of impact based on the number of individuals/records involved in the incident
* Describe the type of Breach Incident (theft, loss, improper disposal, unauthorized access, unauthorized disclosure, mis-sent, hacking/IT incident, Unknown, Other)
* A list of the Participants likely impacted by the Breach Incident
* Description of the roles of the people who may have improperly sent, used, accessed, or disclosed PHI/PII (e.g., employees, Users, service providers, unauthorized persons, etc.) and a description of the roles of those persons who may have viewed (or accidentally) obtained PHI/PII
* A description of the system (MCMS, NCH, CMS), and types (PHI or PII to include demographic, financial, clinical, or other types) of Data involved in the Breach Incident
* Indicate whether the data involved in the incident provide a reasonable basis to believe it can be used to identify an individual
* Actions taken by the Participant or the ITSP to investigate and mitigate the Breach Incident
* Status of the Breach Incident (under investigation, resolved, or other)
* Contact information of the ITSP individual providing the report (name, email, contact number, and any additional entities or person(s) the incident was reported to

Upon receipt of the initial report of a suspected breach by the NEICE Project Director, the BIRT will be convened to determine next steps for notification of the incident to NEICE Participants and other stakeholders (e.g., insurance carrier, law enforcement, HHS) as well as elements of the incident to be communicated.

1. **Follow Up to Initial Report of Breach Incident**

Within **seventy-two hours** of the initial report of a suspected Breach Incident, the ITSP will provide a full report (See Section 5 –Notification Content) to the APHSA NEICE Project Director. This report will be reviewed by the BIRT to determine further action.

If a Breach has not actually occurred, communication of this will be sent to those required to be notified.

If the ITSP’s report indicates that a Breach has actually occurred, the Breach Incident Response Team (BIRT) will determine the severity of the Breach (whether it was internal or external) and which steps as outlined in Section IV should be activated. The ITSP report will address all elements outlined in #5 - Notification Content. Once the ITSP has provided the final report to APHSA, all Participants impacted by the Breach will be notified by APHSA within twenty-four hours and kept up to date on all activity until Breach is completely resolved. Notifications of ongoing investigation, mitigation, and corrective actions will continue all the way from suspected incident report to the lessons learned as outlined in an incident response debrief. (See Appendix B – BIRT Decision Tree)

1. **Notification Content**

The notification content within 72 hours of the suspected incident (Form Provided to the ITSP and Participants) from either the Participant or the ITSP shall include the following information:

* A brief description of the Breach Incident to include date of incident, date of discovery, time, duration of incident, and location of incident. Additionally, the ITSP will provide a preliminary risk assessment that identifies a high (e.g., external breach), medium (e.g., state report of internal access), or low (e.g., internal misdirected data within the system) risk of impact based on the number of individuals/records involved in the incident. Included in this description, the ITSP will indicate how many of these cases involved in the incident exposed PHI or PII
* Describe the type of Breach Incident (theft, loss, improper disposal, unauthorized access, unauthorized disclosure, mis-sent, hacking/IT incident, Unknown, Other)
* Description of the roles of the people who may have improperly sent, used, accessed, or disclosed PHI/PII (e.g., employees, Users, service providers, unauthorized persons, etc.) and a description of the roles of those persons who may have viewed (or accidentally) obtained PHI/PII
* A description of the system (MCMS, NCH, CMS), and types (PHI or PII to include demographic, financial, clinical, or other types) of Data involved in the Breach Incident
* Indicate whether the data involved in the incident provide a reasonable basis to believe it can be used to identify an individual?
* Location of the information disclosed in the incident (e.g., laptop, desktop computer, network server, email, other portable electronic device, electronic medical record, paper data, blackberry, cell phone, hard drive (external), hard drive (internal), CD/DVD, PDA, Tape/DLT/DASD, USB, other
* Safeguards in place prior to the Breach Incident (e.g., firewalls, packet filtering (router based), secure browser sessions, strong authentication, encrypted wireless, physical security, logical access control, anti-virus software, intrusion detection, and biometrics
* Indicate what malicious code or malware involved in the incident (e.g., worm, virus, trojan, buffer overflow, denial service, other
* Indicate training provided to staff involved in HIPAA Privacy and Security within the past year
* Actions taken by the Participant or the ITSP to investigate and mitigate the Breach Incident
* Status of the Breach Incident (under investigation, resolved, or other)
* Contact information of the ITSP individual providing the report (name, email, contact number, and any additional entities or person(s) the incident was reported to
* Corrective action taken and steps planned to be taken to prevent a similar Breach (e.g., security and/or privacy safeguards, mitigation strategies, sanctions, improved policies, and procedures, other)
* A statement whether the impermissible use or disclosure constitutes a Breach of Unsecured Protected Health Information
* Describe data recovery strategies, indicating what APHSA systems were involved, if any; if data was encrypted per NIST standards; if data was recovered and if so, where it is at time of report; and if not, explain; and indicate any further potential misuse of data involved in the incident
* A statement as to whether a law enforcement official has advised APHSA, either verbally or in writing, that he or she has determined that notification or notice to affected individuals or posting required under section 13402 of the HITECH Act or their own state legislation would impede a criminal investigation or cause damage to national security and, if so, include contact information for this official.

The Notification shall not include any Confidential or Protected Data. The Participant or the ITSP agrees to supplement the information contained in the Notification as it becomes available.

If, on the basis of the information available to the Participants or the ITSP, the Participant or APHSA believes it should temporarily cease data transmittals with all other Participants, the system may undergo a service level interruption or voluntary suspension in accordance with Appendix 5 of the MOU.

1. **Disposition of Breach Alerts and Notifications**

APHSA shall facilitate a discussion with appropriate parties upon notification of the Breach for the purpose of reviewing the following:

* The impact of the Breach on the privacy, security, confidentiality, and integrity of the data transmittals to include PHI and PII in the NEICE
* Whether APHSA needs any additional information to assess the impact and subsequent decision-making related to the Breach
* Whether APHSA needs to take further action to suspend a Participant involved in the Breach or potential Breach; and
* Whether APHSA needs to take any further action to mitigate the impact of the Breach.
1. **Voluntary Suspension or Termination by the Participant**

If, on the basis of the Breach notification, a Participant desires to cease data transmittals with the Participant involved with the Breach, such Participant should notify APHSA of such a request for cessation. APHSA will facilitate a discussion between both Participants to include the ITSP to determine the best approach to resolve the request. Should cessation occur, APHSA shall notify all Participants of each cessation and will keep a log of all such cessations.

1. **Determination of Breach Resolution**

Once complete information about the Breach becomes available, APHSA shall assess whether the actions taken by the ITSP and/or Participant(s) involved with the Breach are sufficient to mitigate the Breach and prevent a similar Breach from occurring in the future. Once APHSA is satisfied that all appropriate measures have been taken, APHSA will deem the Breach resolved.

APHSA will communicate this decision to all Participants in the NEICE as well as all lessons learned about the root cause of the Breach to prevent a recurrence of the event in the future.