****

**NEICE Data Breach Notification Process (Detailed)**

**(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.

## Breach Incident Management

When a Breach Incident has been identified, whether by the NEICE technical vendor or a Participant, the following plan will be implemented:

1. The Breach Incident Response Team (BIRT) will meet (at time of suspected notification as well as throughout the investigation by ITSP) to determine whether the Breach Incident involved any personal information or PHI. All members of the BIRT must be made aware of the incident.
2. Within twenty-four hours of the BIRT determining that a Breach has taken place, all Participants will be notified by APHSA and kept up to date on all activity until the Breach is resolved. APHSA will use the NEICE Point of Contact (POC), and each state is responsible for ensuring someone on their staff reads notifications. Sample Communications in Appendix A.
3. All available data related to the Breach will be collected and presented to the BIRT **at the direction of counsel** so that remediation steps and legal responsibilities can be assessed, and to provide necessary information to law enforcement investigations resulting from a Breach. The report (contents detailed in #4 below) will be marked: **“Privileged and Confidential: Attorney-Client Privileged Communication. This document was prepared at the direction of counsel for the purpose of obtaining legal advice.”**

When a data Breach occurs, a risk assessment must be conducted by the ITSP and provided to the BIRT that includes the following information. The risk assessment report should include, but is not limited to the following information:

* 1. Data, time, duration, and location of breach.
	2. How the Breach was discovered, by whom, and any known details surrounding the breach (e.g., identification of the unauthorized person accessing the data, method of intrusion, entry or exit points, paths taken, compromised systems, whether data was deleted vs modified vs viewed, whether any physical assets are missing.)
	3. Details about the compromised data, including a list of affected individuals, and type (employee, vendor, child, agency, etc.), data fields (including all fields of personal information maintained), number of records affected, whether any data was encrypted (if so, which fields), and what individual the data relates to.
	4. If the data that was breached contained unencrypted information, specifically, name, plus SSN, driver’s license/state ID, credit card/bank account info with PIN/PW the BIRT must be notified immediately.
1. The BIRT must analyze and assess the immediate security ramifications of the Breach, specifically:
	1. Evaluate and understand the cause of the incident.
	2. Identify who the affected persons are and what personal information has been compromised.
	3. Determine extent to which the risk to the personal information has been mitigated.
	4. Determine what is likely to happen to the data that was compromised.
	5. Determine whether other systems are under threat or of immediate or future danger.
	6. Analysis may also involve issues that require the assistance of specialized consultants. If necessary, contact previously identified third party Information Technology consultants to assist in capturing relevant information and performing forensic analysis.
2. Legal Counsel must analyze and assess the legal implications of the breach, including:
	1. Litigation risk: Review customer, supplier, and any other relevant company agreements, including website privacy policies to see whether the company owes notification or other obligations to any third party with respect to the data breached.
	2. Statutory notification requirements.
		1. Identify legal jurisdictions involved: states, counties involved in a Breach by determining location of children, adult resources, employees and/or systems affected by the Breach.
		2. Identify statutes triggered: Determine whether compromised Personal Information triggers data notification laws. Generally, notification could be required where the compromised data is unencrypted and includes affected person’s first and last names, plus one of the following: SSN, driver’s license number, state identification number, credit card number, or bank account with password. (If more than 500 individuals’ health information was compromised, The Secretary of HHS must be notified).
		3. Jurisdiction: Determine whether, if acting as a service provider to another business, whether notification obligations to such other businesses have been triggered and if so whether that stratifies all notification obligations.
		4. Jurisdiction: Determine whether applicable state or federal law requires additional consumer notification.
		5. Law Enforcement Notification Requirement: Determine whether law enforcement or other agencies *must* be notified by law, e.g., states such as Connecticut, Indiana, New Hampshire, New York, New Jersey, North Carolina, and Hawaii.
		6. Notify Credit Agencies: Determine whether credit reporting agencies *must* be notified by law relative to the affected persons in the Breach.
	3. Insurance coverage. Review company’s insurance coverage to determine whether the Breach Incident is covered by law.
	4. Indemnification by and/or responsibility of third parties if they are the cause of the breach. Analyze and determine whether any third parties have obligations to the company based on their actions or inactions giving rise to the Breach.
	5. Law enforcement investigation of the company (outlined below)
	6. Liability of individual employees. Analyze whether any employee(s) violated company policies or laws and are responsible for the Breach.
3. Contact Law Enforcement if necessary (and US HHS if HIPAA was violated.)
	1. Analysis of the compromised data will suggest which legal jurisdictions may be relevant as potential parties for notification in the event of a Breach. If necessary, contact the appropriate local and/or federal law enforcement agencies to enable immediate deployment of investigative capabilities.
	2. Assign one member of BIRT to be liaison with law enforcement.
	3. Law enforcement agencies may require delay in notification to affected persons or release of public information if doing so would hamper law enforcement investigations.
	4. Local or federal law enforcement authorities may conduct an investigation of company’s security systems and response to the Breach as part of their investigation. Consult legal counsel BEFORE notifying law enforcement.
	5. Even if no state notification or individual notification is required, may need to file police report of incident (e.g., stolen laptop, burglary).
4. Contact insurance carrier. Review insurance coverage relevant to Breach and notify the carrier in accordance with policy requirements. Consult with legal counsel prior to notification of insurer.
5. Organize Incident Notification System and Inquiry Response System.
The NEICE BIRT may need to be convened outside normal work hours and a system for telephone and texting needs to be set up so that the BIRT can be notified and convened in a timely way.

In addition, there may be a high number of inquiries related to the breach. As a result, APHSA should create a system for handling the inquiries when a breach occurs in coordination with the insurance company, which should cover the expense. System may include:
	1. Mode of communication with public (1-800 number and email address);
	2. Mode of communication with state NEICE partners.
	3. Mode of communication with employees.
	4. Training staff or outsourcing to a call center to monitor inquiries to the breach.
	5. Documentation of inquiry responses, preparation of script, preparation of website Frequently Asked Questions (FAQs).
6. Investigation Remediation Strategies.
	1. APHSA will offer remediation services to affected persons following a Breach in the form of credit monitoring services as provided in the cyber insurance coverage.

1. Develop a notification plan for affected persons in conjunction with the Participant State. (See Appendix A)
	1. Develop list of who should be notified. In case of children, determine who needs to be notified. Minimize false positives.
	2. Tetrus will prepare a report in the event of a breach.
	3. Should go to the legal guardian (which in most cases is the state) or to the adoptive parents.
	4. Determine how the state will be notified (letter).
	5. Notice should include:
		1. Description of what happened
		2. Type of protected data involved
		3. Actions to protect data from further unauthorized access
		4. What the Participant State will do to assist affected persons
		5. What affected persons can do to assist themselves
		6. Contact information for APHSA’s inquiry response system (1 800 toll free number); and
		7. Contact information for local and federal government information.
	6. Create a sample notification letter to affected persons.
	7. Some states require special notification.
2. Develop a communication plan
	1. Implement internal communication plan. May require phone updates rather than email, if email system was compromised. Reissue policy statement to staff about external communication with media, third parties or via social media.
	2. Create Communication Strategy:
		1. Law Enforcement Notification – May require delay in notification of media or affected persons.
		2. Affected Person Notification (as outlined in Appendix A)
		3. Credit Agency Notification (if necessary relative to the affected person) (notify them before notifying large number of affected persons.)
		4. Media and Web Statement/Press Release (draft and post)
	3. Preparation of Support Systems
		1. Ensure company inquiry system is in place.
		2. Remediation strategies have been activated.
	4. Execute strategy
		1. Central communications person handles execution of this plan and documents activities.
	5. Handle follow up contacts/returned notifications
		1. Collect returned mailings
		2. Maintain database of returned mailings including date of return by individual
		3. Run returned mailings through National Change of Address vendor.
		4. Re-mail if new address is obtained.
		5. If returned again, use third party data vendor (Acxiom, or others)
		6. Track all further returned mails and enter into database.
3. **Post Breach Actions**
4. Ensure system is secure.
	1. Conduct full analysis of Breach to determine root causes.
	2. Review applicable access controls and procedures (Both before and after breach) to ensure weaknesses have been resolved.
5. Implement remediation measures focused on credit monitoring.
6. Prepare for litigation. (May include civil lawsuits by affected persons; investigation of company and specific employees by law enforcement; indemnification by third parties in event that third parties are at fault.)
7. Assess and update operation controls
	1. Assess operations to determine any need for revisions to data collection, retention, storage and processing policies and procedures.
	2. Assess need for additional employee training in data protection policies and processes.
	3. Review contract provisions (standard and actual) with third parties that handle PI.
	4. Review relevant website privacy notices and terms of services, update as needed.
	5. Review relevant agreements with partner states and vendors, determine whether form agreements need to be updated.
8. Assess the effectiveness of the Breach Response.
	1. Review steps taken by Data Owners and BIRT during course of response to the Breach and implement changes to the plans to improve effectiveness in preventing and responding to data Breaches.

Record the date and time that the BIRT meeting was held.

**APPENDIX A – Sample Communications for Breach Notification to Affected Persons/Entity**

Show through ENVELOPE:

Important Security and Protection Notification. Please read this entire letter.

Dear [Insert name]: I am contacting you regarding a data security incident that has occurred at the National Electronic Interstate Compact Enterprise – an online data exchange to help with moving children across state lines for adoption or foster care, operated on behalf of the Association of Administrators for the Interstate Compact on the Placement of Children by the American Public Human Services Association. This incident involved your [describe the type of personal information (of your client) that may be potentially exposed due to the Breach Incident (i.e., Social Security number, etc.)].

As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us. [Insert Company Name] takes this incident seriously and is committed to assuring the security of your data.

To help protect your identity, we are offering a complimentary one-year membership of CREDIT MONITORING SERVICE HERE. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft.

***DESCRIBE HOW TO ACTIVATE.***

***[Insert a detailed explanation about the circumstances surrounding the Breach Incident (e.g., this information was contained on a computer that was stolen from our offices.), what investigative steps have been taken, if you are aware of any fraudulent use of the information, explain the steps your company has taken to ensure that this issue won’t happen again, e.g., better secure our computers and facilities and include any and all other relevant facts]***

We sincerely apologize for this incident, regret any inconvenience it may cause you, and encourage you to take advantage of the product outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at [insert company phone number].

Sincerely,

[Signed by appropriate executive - president, CEO or VP HR]

**Appendix B:1 – NEICE Breach Incident Response Decision Tree**

**(Revised 11-1-21)**

**Suspected Breach Incident – Exceptions Are Noted, No PHI or PII Data Exposed**

ITSP suspects a Breach Incident and immediately acts to secure the system and data regardless of source or magnitude of risk

Classified as Exception?

If a data breach incident exception is noted, no PII or PHI was exposed, the BIRT is not convened

If no exceptions of the breach incident are noted, the investigation, reporting and notification procedures are to take place.

Yes

Project Director is notified within 24 hours of a possible breach incident by ITSP and together a determination is made as to whether the incident can be classified as an exception and if PII or PHI was exposed.

No

**Appendix B:2 - NEICE Breach Incident Response Decision Tree**

**(Revised 11-1-21)**

**Suspected Breach Incident – No Exceptions Noted**