**Text

Description automatically generated**A picture containing diagram

Description automatically generatedA picture containing text, clipart

Description automatically generated

**NEICE Data Breach Report Form**

This form is to be completed by the NEICE Participant, the NEICE Information Technology Service Provider (ITSP), or APHSA if there is a suspected or actual breach of the NEICE System. Depending on the severity of the incident you may complete partial or all of this form as described here:

1. For a suspected breach, complete questions 1-11 and submit to the NEICE Project Director.
2. After a full investigation/risk assessment, update and complete questions 1-15 and submit to the NEICE Project Director.

**Reporting Entity Where Suspected Breach Occurred (Check appropriate entity):**

* + NEICE State/Country/District Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  + NEICE Technical Provider: Tetrus Corporation
  + APHSA

**Name of Individual Submitting form: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Agency: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cell: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date Report Form Submitted:** \_\_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_\_\_ (Month / Day / Year)

1. Describe the Breach in 1-2 sentences to include date of incident and date of discovery, time, duration of incident, and location of the breach.
2. Indicate 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 involve in the incident.
   * HIGH (external breach)
   * MEDIUM (state report of internal access)
   * LOW (internal misdirected data within NEICE system)
3. Describe the type of Breach Incident (theft, loss, improper disposal, unauthorized access, unauthorized disclosure, mis-sent, hacking/IT incident, unknown, or other).
4. List of the Participants likely impacted by the Breach Incident. (Typically state names)
5. Describe the roles of the people involved in the Breach Incident (e.g., employees, Users, service providers, unauthorized persons, etc.).
6. Type of system involved in the Breach Incident. (NEICE Clearinghouse, specific NEICE MCMS application, Cloud-based CMS, other (be specific))
   * NEICE Clearinghouse Direct Application
   * NEICE Clearinghouse Direct (State Participant level)
   * NEICE MCMS Application
   * NEICE MCMS Application (State Participant level)
   * NEICE CMS Cloud-based Application
   * NEICE CMS Cloud-based Application (State Participant level)
   * Other (please be specific) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
7. Types of Data involved in the Breach (PHI or PII to include demographic, financial, clinical, or other).
8. Number of Users or records impacted/estimated to be impacted by the Breach.
9. Is there reasonable basis to believe Data involved in incident can be used to identify an individual?
   * Yes
   * No
   * Unknown
10. What actions have been taken by the Participant or the ITSP to investigate and mitigate the Breach?
11. What is the current status of the Breach (under investigation, resolved, other)? Mark all that apply.
    * Under Investigation
    * Initial Steps Taken to Protect Data and System
    * Corrective Action taken
    * Resolved
    * Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
12. What corrective action has been taken and what are the steps planned to be taken to prevent a similar Breach?
13. Provide a description of corrective actions affected children and adults should take to protect themselves in relation to the types of Data impermissibly used or disclosed.
14. Provide a statement whether the impermissible use or disclosure constitutes a Breach of Unsecured Protected Health Information.
15. Provide a statement as to whether a law enforcement official has advised, either verbally or in writing, APHSA 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.

**Submitted By:**

Name:

Signature: