Agenda with time frames & presenters

2:30 Welcome and Introductions (BIRT and POCs)…………………Marci Roth

2:35 Goals of Meeting Marci Roth

2:40 Security Awareness and NEICE Safeguards…………………………Marci Roth

2:50 NEICE Security Incident and Breach Policy and Procedures….Anita Light

Purpose of Incident & Breach Policy and Reporting

Issues Addressed in the Revised Breach Policy and Reporting Procedures

Defining a NEICE Breach

3:00 Breach Incident Management…………………………………………………… Anita Light

Determining if a Breach Has Occurred

NEICE Breach Incident Reporting Process

3:15 Post Breach Activities……………………………………………………………… Anita Light

3:20 Questions/Recommendations/Action Plan………………………… Marci

Association of Administrators of the Interstate Compact on the Placement of Children

AAICPC

APHSA

American Public Human Services Association

NEICE All State Security Briefing

This meeting is for states’ Point of Contact in event of a breach to NEICE data.

November 17, 2021

NEICE

National Electronic Interstate Compact Enterprise

Today's Agenda

Welcome and Introductions

Goals of this Meeting

Security Awareness and NEICE Safeguards

NEICE Security Incident and Breach Policy and Procedures

- Purpose of Incident & Breach Policy and Reporting
- Issues Addressed in the Revised Policy and Reporting
- Defining a NEICE Breach

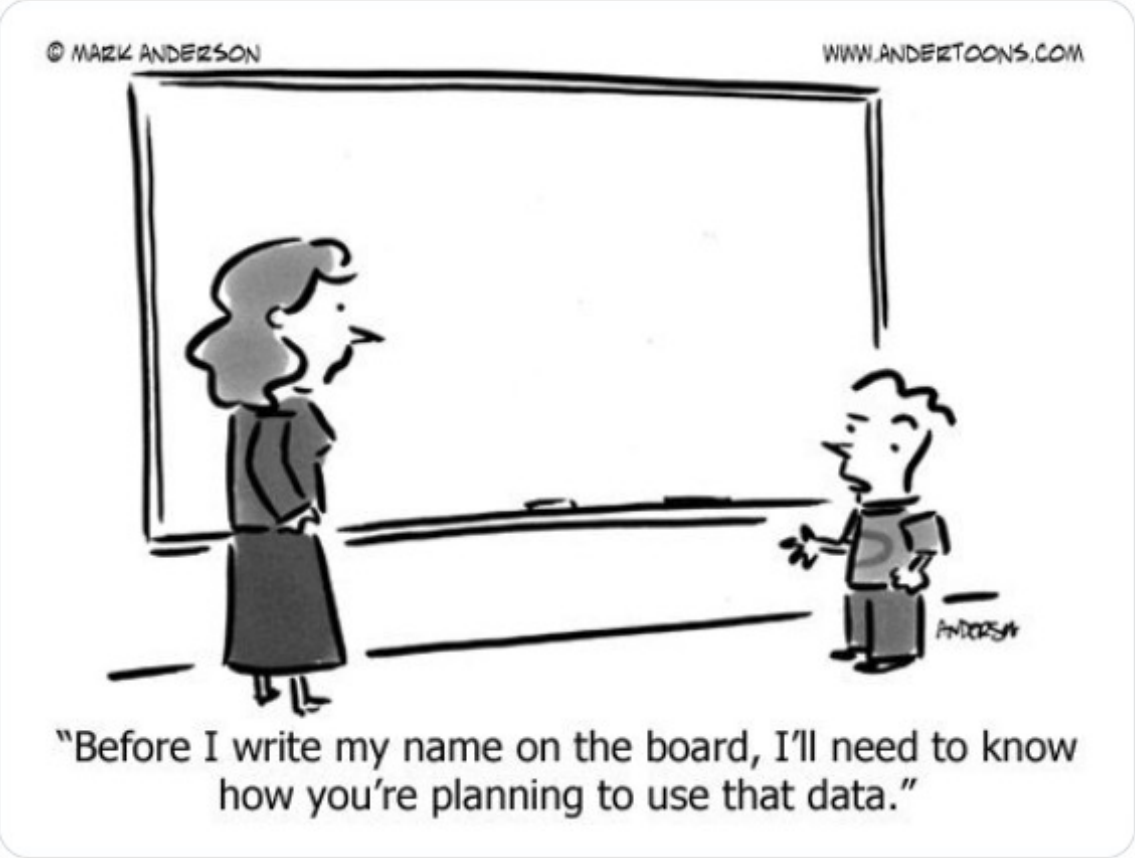
Breach Incident Management (Summary with decision tree)

- Determining if a Breach Has Occurred
- NEICE Breach Incident Reporting Process
- Post Breach Activities

Questions/Recommendations/Action Plan

Welcome and Introductions

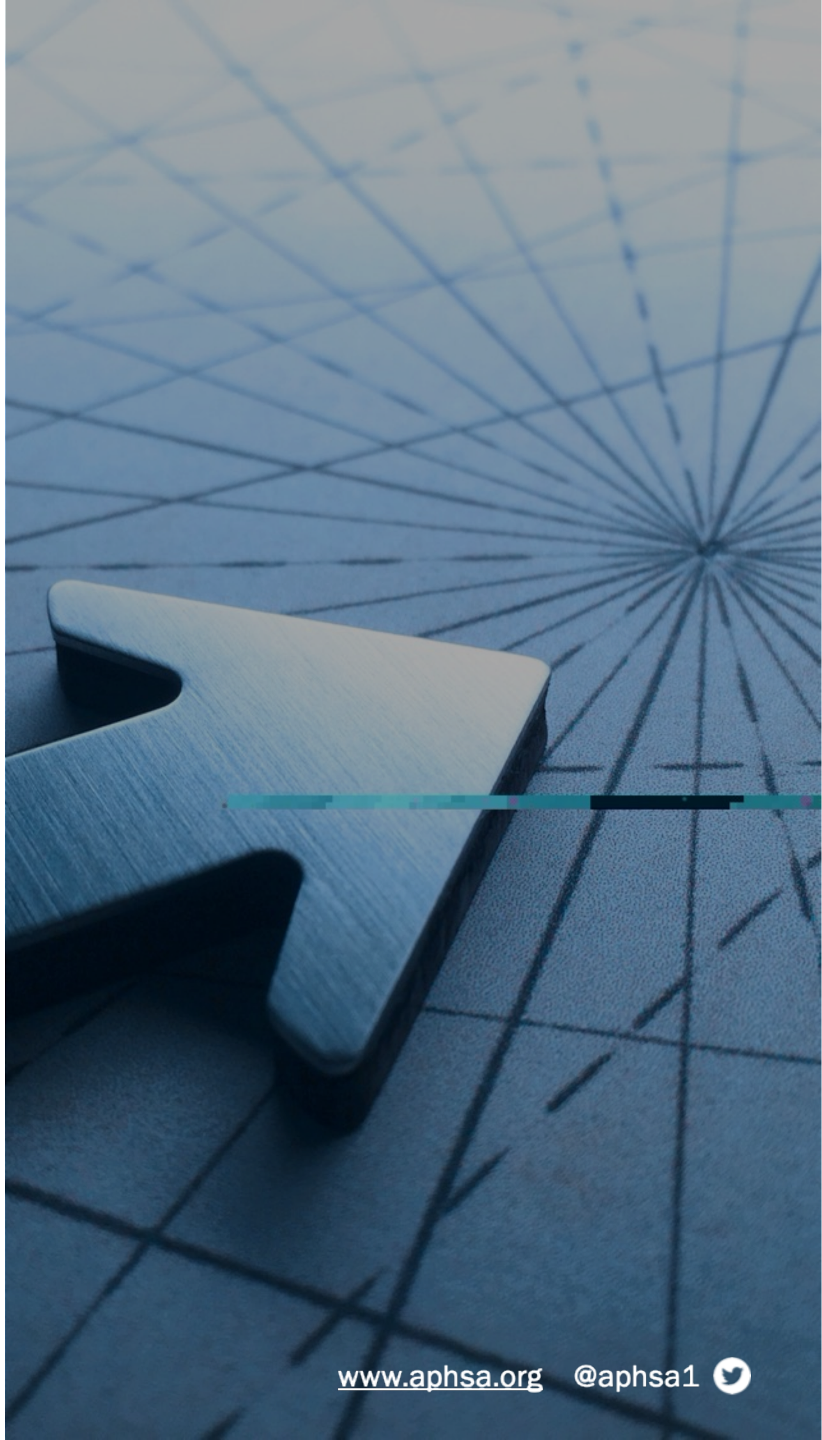
Please say hi in the chat box, with your name, state and role!



"Before I write my name on the board, I'll need to know how you're planning to use that data."

Goals of this meeting

1. Heighten security awareness for all NEICE partners
2. Learn about NEICE security safeguards
3. Become familiar with NEICE security breach policy, procedures & expectations
   - Understand what NEICE team will do in event of breach
   - Understand State responsibilities in the event of a breach



NEICE Security Awareness and Safeguards

"WELL, I *TOLD* YOU NOT TO OPEN THAT ATTACHMENT!"

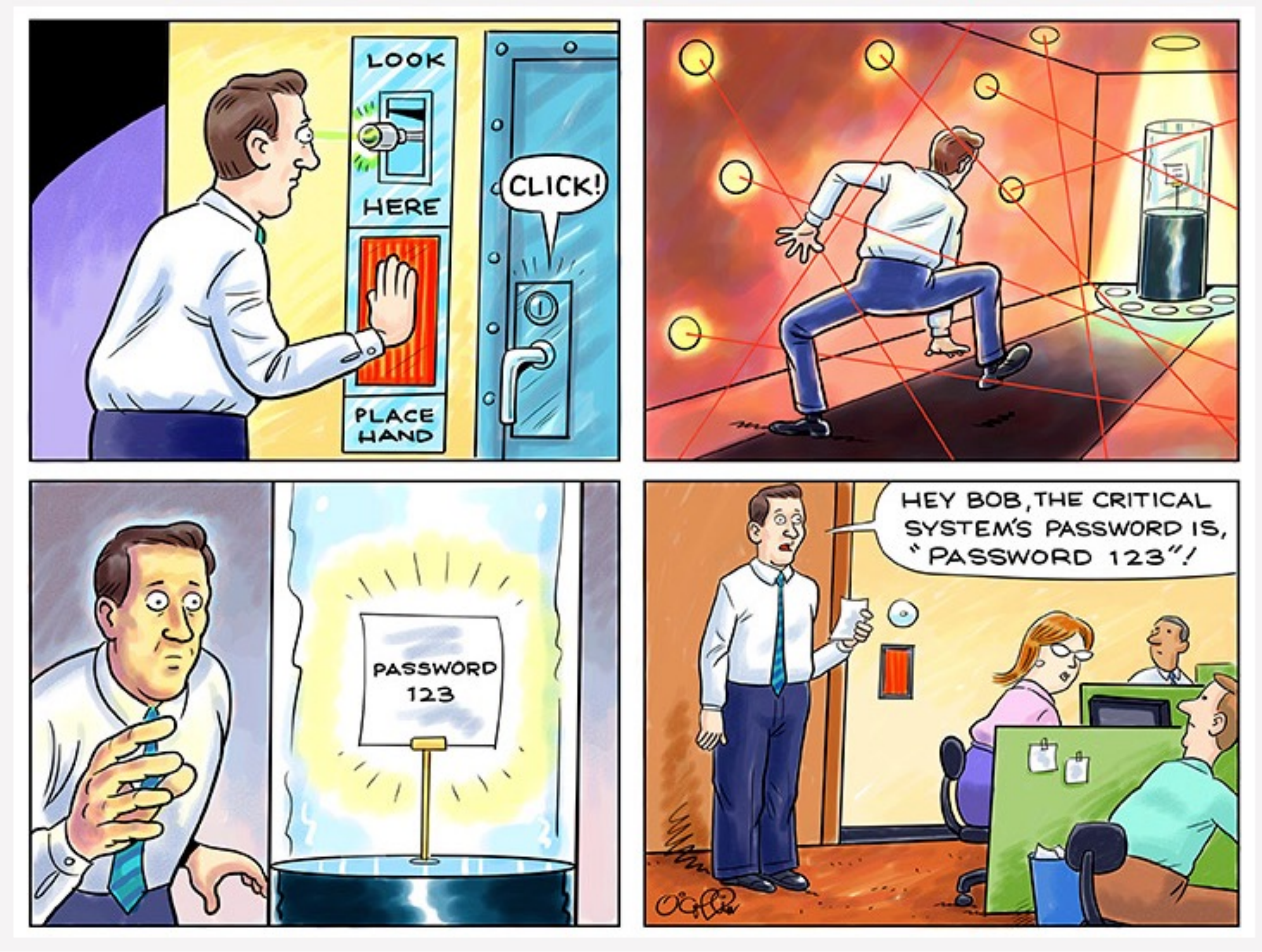
NEICE contains PII and PHI Data that must be protected

States use NEICE to exchange child and placement resource information with one another as part of the Interstate Compact on the Placement of Children (ICPC).

NEICE contains sensitive Personal Individual Information (PII) and Personal Health Information (PHI) on children and families.

State and federal laws require that anyone using a public data system to exchange PII or PHI data be aware of the security risks and follow public security requirements and protocols in order to safeguard the data.

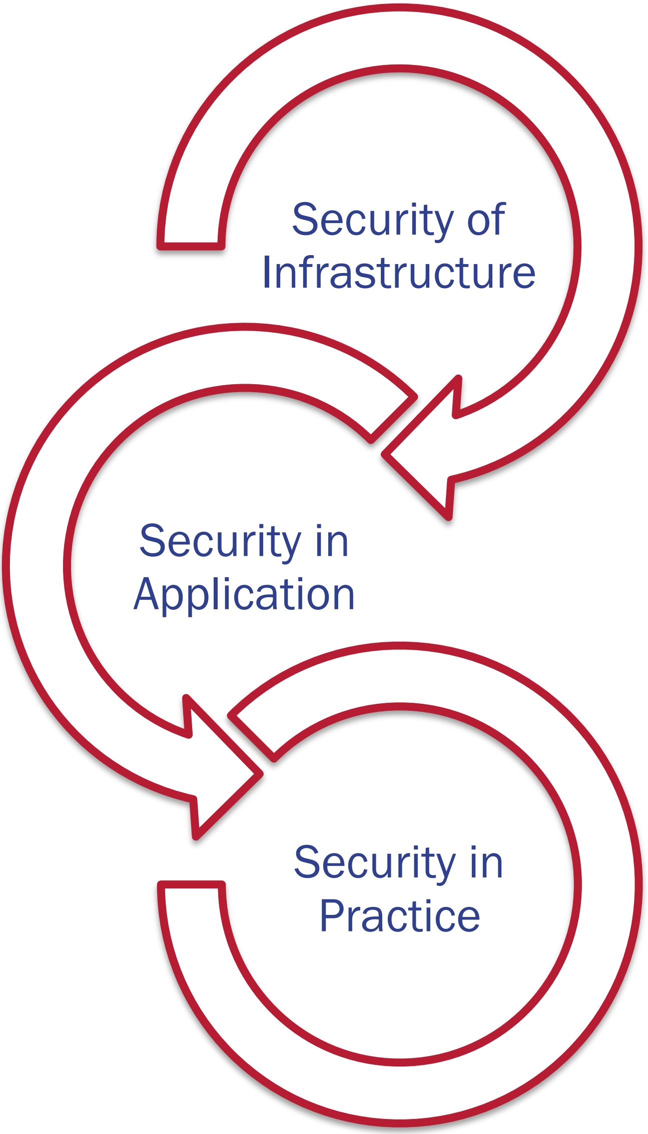
Security is everyone’s responsibility



There’s no silver bullet solution with cyber security, a layered defense is the only viable defense.”

James Scott, Institute for Critical Infrastructure Technology

NEICE Security Framework



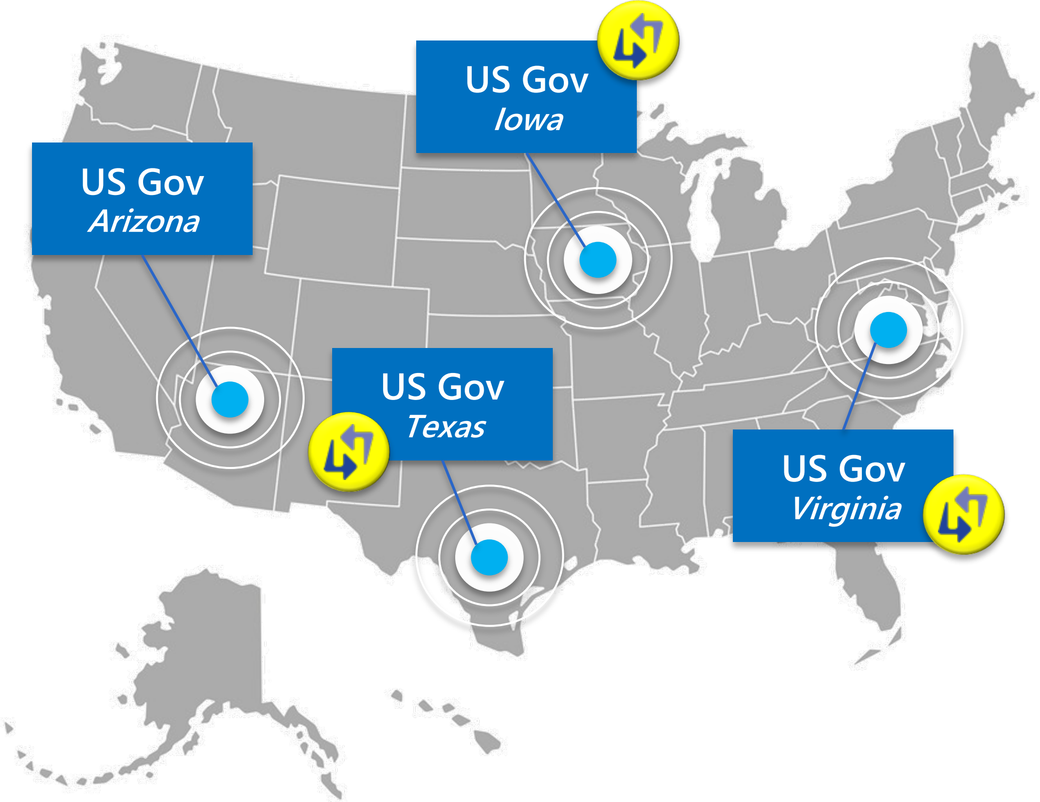
The overall security framework, policies regarding access to sensitive data, training of personnel etc., have been audited and found to be compliant

> *'…Results of the assessment show that all policies, practices, and processes meet the HIPAA HITECH … NIST cybersecurity framework aligned to the guidelines in NIST SP 800-30, Risk Management Guide for Information Technology Systems and Regulation 45 CFR Part 164") as of May 24, 2021.'*

Secure Infrastructure: Azure Government (Infrastructure and Compliance)

Security Starts with Physical Protection

- All NEICE infrastructure is hosted on Azure Government Cloud
- All Azure Government infrastructure is hosted in the United States
- Azure Government data centers are protected with state of the art physical security and 24x7 monitoring
- Microsoft performs monitoring & alerting on security events for the Azure platform
- Azure regularly conducts war game exercises and Live site penetration testing
- Microsoft's Assume Breach approach proactively identifies and addresses potential gaps



CJIS FedRAMP HIPAA COMPLIANCE

Secure Infrastructure: Tetrus (Security and Compliance)

Security and Compliance	• All Tetrus office doors are secured using smart card based access control • Tetrus conducts annual HIPAA audit for process compliance • All Tetrus employees are background check cleared and go through annual HIPAA training
Access to Azure Resources	• The access to all Azure resources is controlled using secure Role Based Active Directory logins • All NEICE Azure resources are accessed only from the Tetrus office physical network or Virtual Private Network with only one whitelisted Tetrus static IP address having access to resources • All access to NEICE data on Azure network are accessed through secure Virtual Machines hosted internally on Azure network

Application Security: Data Protection

Encryption for data in transit

- All communications and data in transit are protected using industry standard TLS/SSL encryption.
- All security certificates use a minimum of 1024 bit encryption
- Clearinghouse uses the Web Service Security standards and HTTPS for all communications

Securing data at rest

- All Databases are protected using the SQL Server Transparent Data Encryption to protect the data at rest
- All documents are encrypted and stored
- FIPS 140-2 approved algorithms are used for Encryption

Data segregation

- Data is segregated and logically isolated within the network using Network Security Groups
- Role based access control are in place to secure access to different logical segments and resource groups

Security in Practice: NEICE Application Protection

User Authentication	• NEICE enforces strong password rules to enforce password security • NEICE uses a modified multi factor security to secure user logins. NEICE would send a security code for users logging in from a device and remembers the device for future logins • NEICE would look for user activity and automatically prompt the users to enter an additional security code sent to their email addresses upon 30 days of inactivity
NEICE CMS Security Control and Monitoring	• NEICE CMS uses role-based profiles that limit user’s access to appropriate data elements and functionality • NEICE performs thorough audit logging on every user action that is performed in the NEICE CMS • NEICE audit logs includes the IP address from where the users are accessing the system and a monitoring routine monitors for any potentially malicious or suspicious user activity.

NEICE Security in Practice

Regular Monitoring of logs	• System logs are analyzed and outliers investigated by Tetrus employees • Examples: Unusual login / activity, w.r.t. time of day / day of week compared to what is normal for the given user • Monthly Vulnerability Scans and continuous Azure Security Monitoring
Security Awareness	• Tetrus employees are trained on safe handling of data • Only select tools are used when troubleshooting issues, where PII/PHI might need to be accessed • Yearly awareness training for all staff and phishing tests

Security in Practice: Security Starts and Ends with Users

To ensure users are aware of security and take utmost care, NEICE:

- Requires all users of the CMS/MCMS application to take an e-Learning training module before using NEICE and posts a job aid on its knowledge base. Each state is responsible for ensuring its users have taken the course.
- requires that all NEICE users agree to assume individual accountability and responsibility in maintaining the security of the NEICE and follow security best practices included in the training module and to their state's own policies and requirements.
- asks NEICE users to sign a user acceptance of the security rules policy annually and attest to follow security protocols each time they log into NEICE.
- provides annual security training for each state's lead NEICE ICPC Administrator/Deputy Administrator and IT staff for NEICE.

NEICE Security Breach Policy and Procedures

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."

Why are breach procedures so important?

Despite the many protections in NEICE, most Cybersecurity experts say, it’s not a matter of if you have a breach but when.

Having a breach plan for investigating, addressing and notifying parties in the case of a breach:

- Means the NEICE team can respond in a systematic, thoughtful and timely way to minimize impact.
- Ensures NEICE adheres to current federal standards for security of public data systems.
- Enables states to initiate their own procedures for investigating, addressing and notifying.

TREND MICRO

© Randy Glasbergen for Trend Micro

“On one hand, I’m grateful that we’ve never been targeted for a cyber-attack. On the other hand, I’m insulted that nobody thinks we’re worth the effort!”

Defining a NEICE 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.

NEICE
National Electronic Interstate Compact Enterprise

Declaring a NEICE Breach – Exception 1

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:

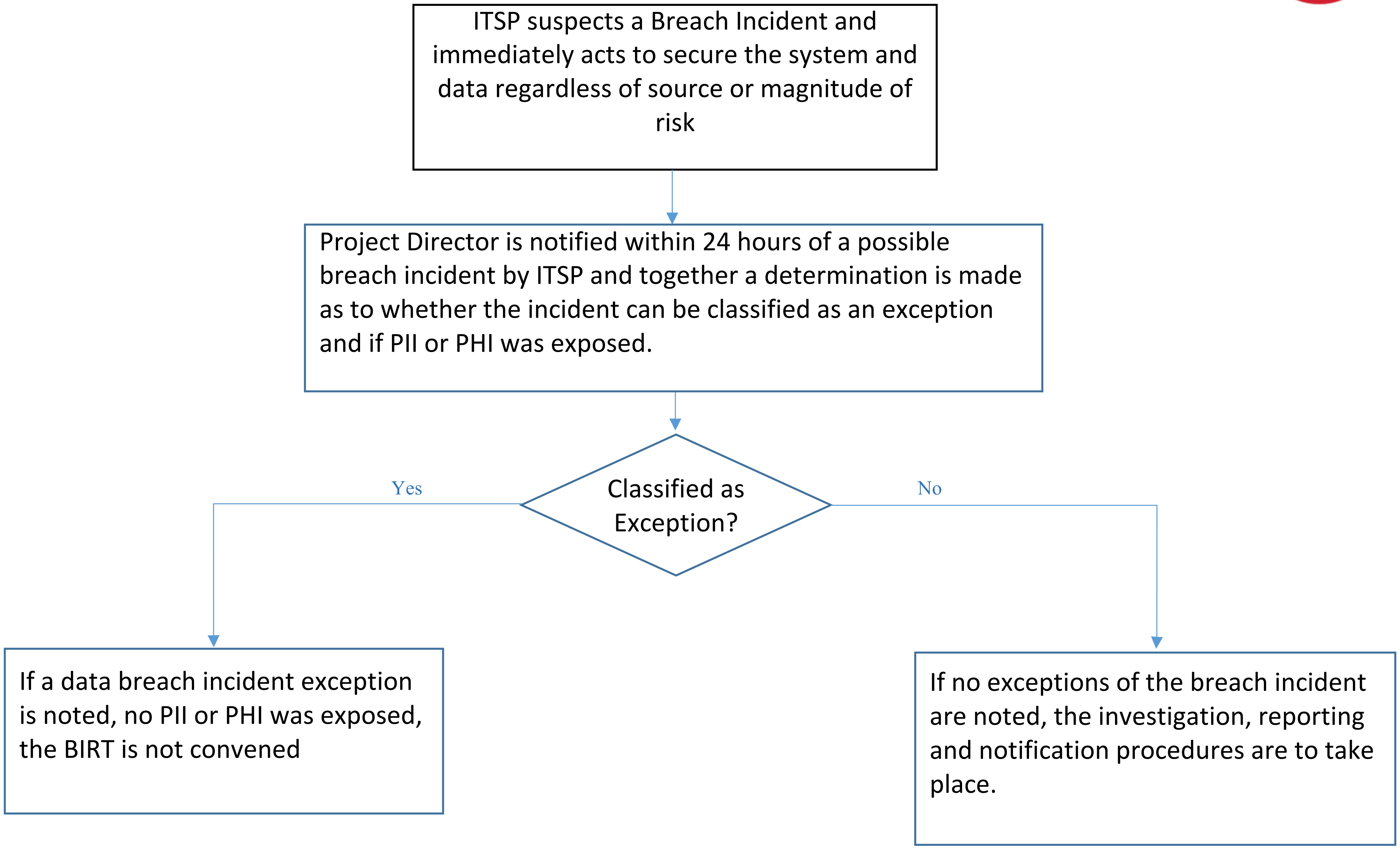
1. The first exception applies to the unintentional acquisition, access, or use of protected, confidential, or health information by a person acting under the authority of a Participant, if such acquisition, access, or use was made in good faith and within the scope of authority.

Declaring a NEICE Breach – Exceptions 2 and 3

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.

Phase 1- NEICE Breach Incident Response Decision Tree (Appendix B:1) Suspected Breach Incident – Exceptions Are Noted, No PHI or PII Data Exposed(Revised 11-1-21)



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

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.

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.

Breach Incident Management

"I'm no expert, but I think it's some kind of cyber attack!"

Determining whether a Breach has occurred

When the ITSP becomes aware of/detects a possible Breach Incident (either in a Participant jurisdiction or in the NEICE system), the ITSP

- immediately acts to secure the system and data mitigate the incident regardless of the source or magnitude of the incident.
- makes decision to shut system down if needed.

Within 24 hours of a suspected breach whether by the NEICE technical vendor or a Participant, the APHSA Project Director must be notified again and in writing and provided as much information as possible using the Breach Incident Reporting Form.

Determining actions needed WHEN a Breach has occurred

When it is determined that the incident requires further investigation, reporting and notification, the BIRT is immediately 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.

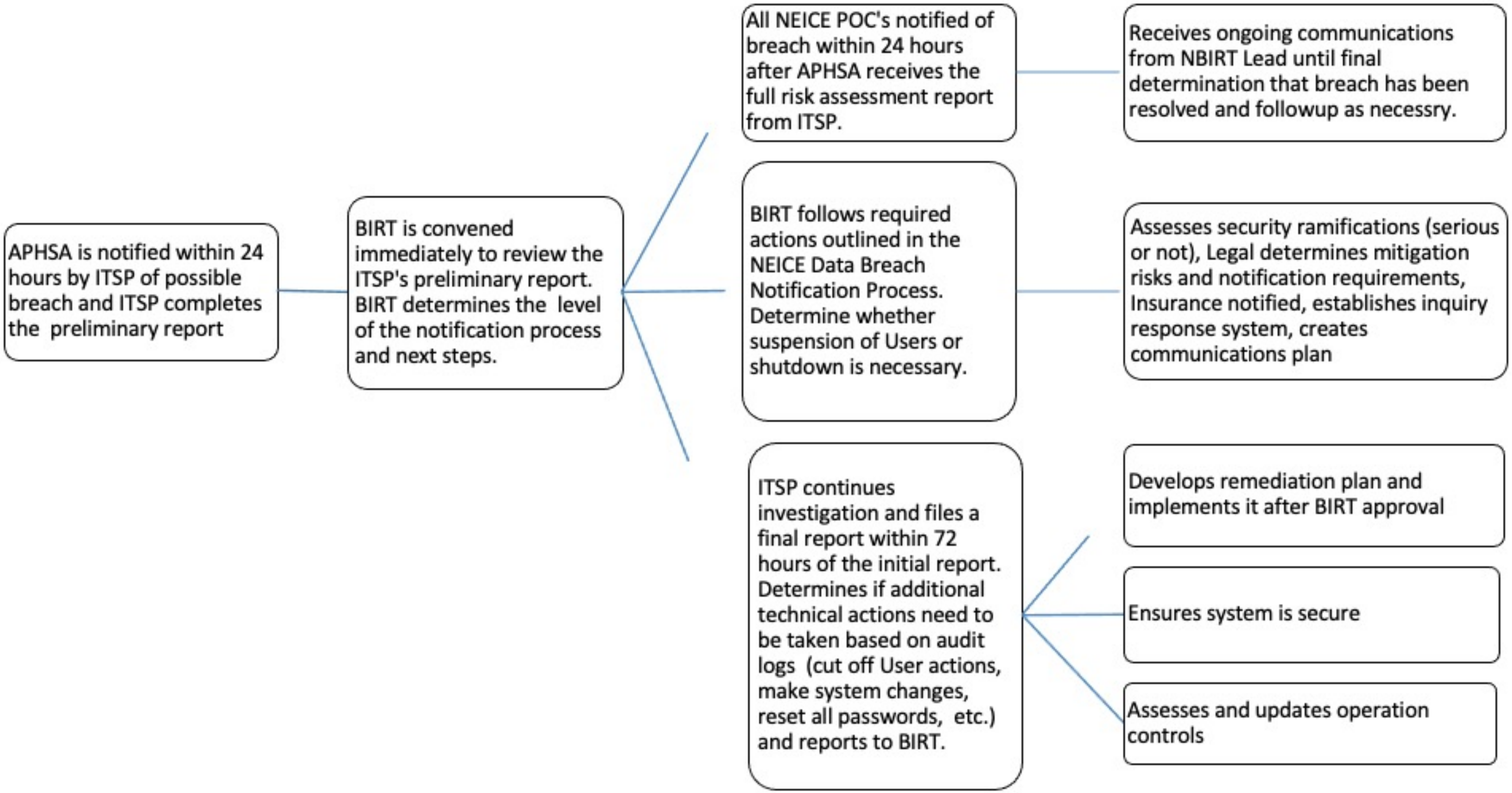
Within seventy-two hours of the initial report of a suspected Breach Incident, the ITSP will provide a full report to the APHSA NEICE Project Director using the form provided to the ITSP and Participants. This report will be reviewed by the BIRT to determine further action, shall not include any Confidential or Protected Data, and will be marked privileged and confidential.

Phase 2 - NEICE Breach Incident Response Decision Tree (Appendix B:2) Suspected Breach Incident – No Exceptions Noted (Revised 11-1-21)

Association of Administrators of the Interstate Compact on the Placement of Children

AAICPC

APHSA
American Public Human Services Association



APHSA is notified within 24 hours by ITSP of possible breach and ITSP completes the preliminary report

BIRT is convened immediately to review the ITSP's preliminary report. BIRT determines the level of the notification process and next steps.

All NEICE POC's notified of breach within 24 hours after APHSA receives the full risk assessment report from ITSP.

Receives ongoing communications from NBIRT Lead until final determination that breach has been resolved and followup as necessry.

BIRT follows required actions outlined in the NEICE Data Breach Notification Process. Determine whether suspension of Users or shutdown is necessary.

Assesses security ramifications (serious or not), Legal determines mitigation risks and notification requirements, Insurance notified, establishes inquiry response system, creates communications plan

ITSP continues investigation and files a final report within 72 hours of the initial report. Determines if additional technical actions need to be taken based on audit logs (cut off User actions, make system changes, reset all passwords, etc.) and reports to BIRT.

Develops remediation plan and implements it after BIRT approval

Ensures system is secure

Assesses and updates operation controls

NEICE Breach Incident Team (BIRT) Team Members

Ray Davidson rdavidson@aphsa.org APHSA COO
Max Daniel mdaniel@aphsa.org APHSA Data Analysis
Guy DeSilva gdesilva@aphsa.org APSA Director, Engagement Operations and Marketing
Duane Fontenot' dfontenot@dss.state.la.us APHSA Technical Consultant
Carla Fults CFults@aphsa.org APHSA Director, Interstate Affairs and Compact Operations
Jessica Garson Jessica.garson@aphsa APHSA Director of Communications
Raghu Govindaraj raghu@tetruscorp.com Tetrus NEICE Chief Architect
Donna Jarvis-Miller DJarvis-Miller@aphsa.org APHSA Director, Membership and Events
Anita Light anita.light@aphsa.org APHSA NEICE Senior Advisor
Susmita Linga susmita.linga@tetruscorp.com Tetris NEICE Developer
Tom Livoti tom.livoti@tetruscorp.com Tetrus Vice President of Customer Satisfaction
Bertha Levin bertha.Levin@aphsa.org APHSA Consultant
Marci McCoy-Roth, mroth@aphsa.org NEICE Director, APHSA
Heather Spencer, Heather.Spencer@jfs.ohio.gov, AAICPC President
Tim Reiniger tim@reinigerllc.com NEICE Attorney
Sharad Rao sharad.rao@tetruscorp.com Tetrus President
Antonette Russell arussell@aphsa.org APHSA HR Director
Sherray Whatley swhatley@aphsa.org APHSA Executive Coordinator

NEICE Breach Incident Reporting Process

The Breach Incident Report Team (BIRT) will :

- determine the severity of the Breach (for both internal or external).
- analyze and assess the immediate security ramification of the Breach.
- investigate cause and ensure immediate implementation of remediate strategies.
- work with legal counsel to analyze and assess the legal implication (page 6).
- determine next steps and develop plan (external and internal) for notification of the incident to NEICE Participants and other stakeholders (e.g., insurance carrier, law enforcement, HHS) and elements of the incident to be communicated in the plan. (For example, participants who had data impacted would be provided details about the data, participants who were impacted by system disruption would be provided higher level information regarding the system and how it has been secured.)

NEICE Breach Incident Communication Process

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 notification and following their protocols to notify clients if needed. Sample Communication in Appendix A.

APHSA will create a system for handling the inquiries and updating Participants when a breach occurs. System may include:

- Mode of communication with public (1-800 number and email address);
- Mode of communication with state NEICE partners (cell numbers needed to create a system similar to DC weather closings).
- Mode of communication with employees.

NEICE
National Electronic Interstate Compact Enterprise

State Points of Contact (POCs)

Alert to NEICE states (also referred to as Participants) in a timely way is critical in event of a breach.

- State Points of Contact (POCs) and Backups are a vital part of the process.
- Each state must have a POC and a back up.
- The state POC and/or Backup
  - ✓ will be responsible for alerting the Information Technology Service Provider (ITSP) of a Breach Incident in Participant’s state or jurisdiction and who will be alerted by APHSA in the event of a data breach by either another Participant or APHSA.
  - ✓ will be responsible for alerting the other state or jurisdiction personnel in Participant’s chain of Breach Notification protocols.
  - ✓ must update this information as changes occur by notifying mroth@aphsa.org.

NEICE Breach Incident Reporting Process

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, it may undergo a service level interruption or voluntary suspension in accordance with Appendix 5 of the MOU.

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.

NEICE Breach Incident Reporting Process

Determination of Breach Resolution: Once complete information about the Breach becomes available, APHSA shall assess whether the actions taken by the ITSP, 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.

NEICE Breach Incident Reporting Process

To summarize, 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:1 and Appendix B:2 – BIRT Decision Trees

Post Breach Actions

Post Breach Actions

1. Ensure system is secure.
   a. Conduct full analysis of Breach to determine root causes.
   b. Review applicable access controls and procedures (Both before and after breach) to ensure weaknesses have been resolved.
2. Implement remediation measures focused on credit monitoring.
3. Prepare for possible 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.)
4. Assess and update operation controls
   a. Assess operations to determine any need for revisions to data collection, retention, storage and processing policies and procedures.
   b. Assess need for additional employee training in data protection policies and processes

Post Breach Actions

c. Review contract provisions (standard and actual) with third parties that handle PI.

d. Review relevant website privacy notices and terms of services, update as needed.

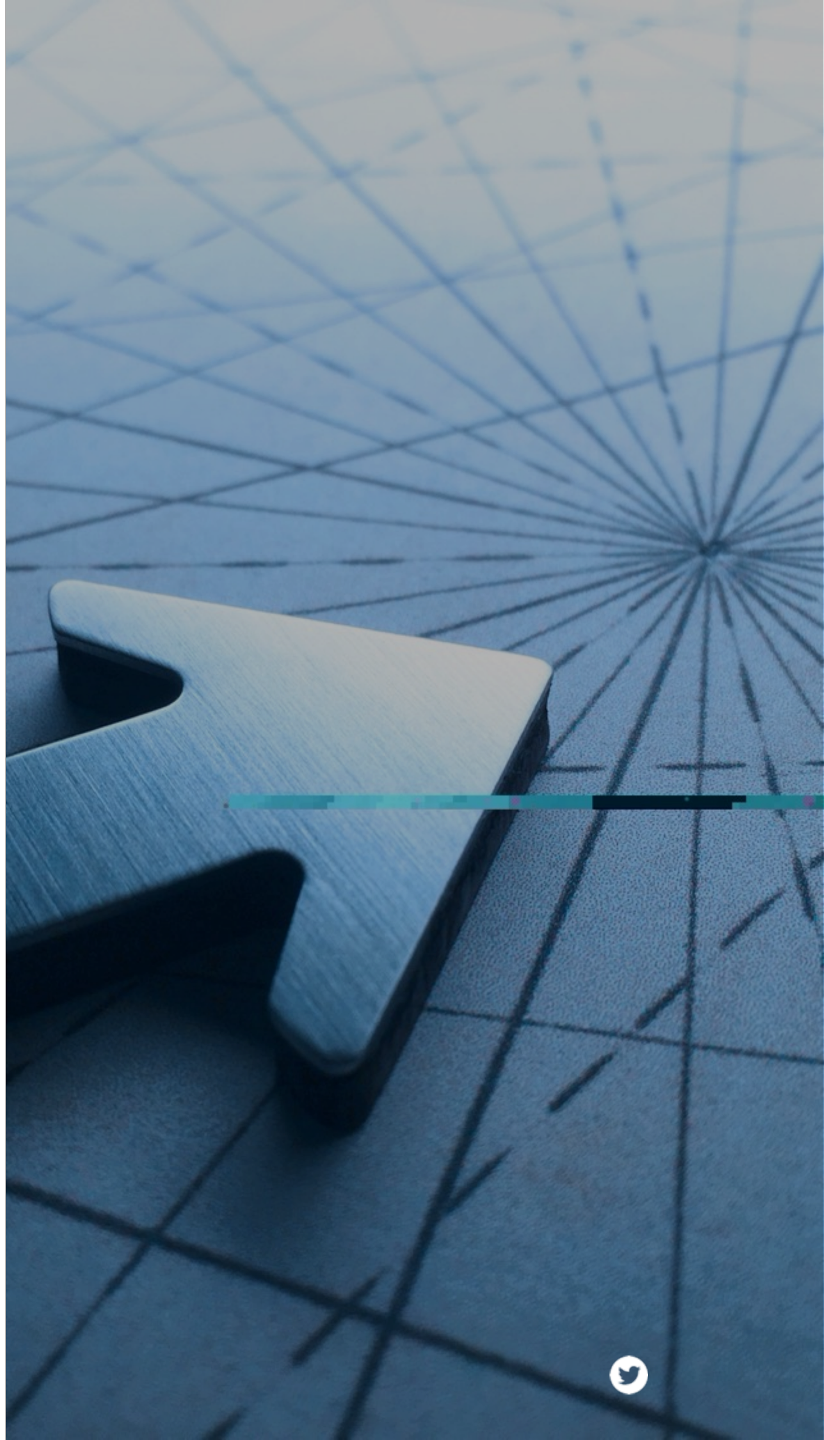
e. Review relevant agreements with partner states and vendors, determine whether form agreements need to be updated.

5. Assess the effectiveness of the Breach Response.

   a. 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.

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

Questions & Recommendations



Thank you!

NEICE
National Electronic Interstate Compact Enterprise