



ANNUAL NATIONAL ELECTRONIC INTERSTATE COMPACT ENTERPRISE SECURITY OVERVIEW: Everyone has a role to play

All-State NEICE Security Training Meeting

April 25, 2024



NEICE
National Electronic Interstate
Compact Enterprise

1

Today's Agenda

- Welcome
- Goals of this Meeting
- NEICE Security
- NEICE Security Incident and Breach Policy and Procedures
- Breach Incident Management
- Questions



NEICE
National Electronic Interstate
Compact Enterprise

2

Welcome and Introductions

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



3

Goals of this meeting

1. Learn about NEICE security safeguards
2. 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



4



5

NEICE contains PII and PHI Data that must be protected



- States use NEICE to exchange child and placement resource information
- 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

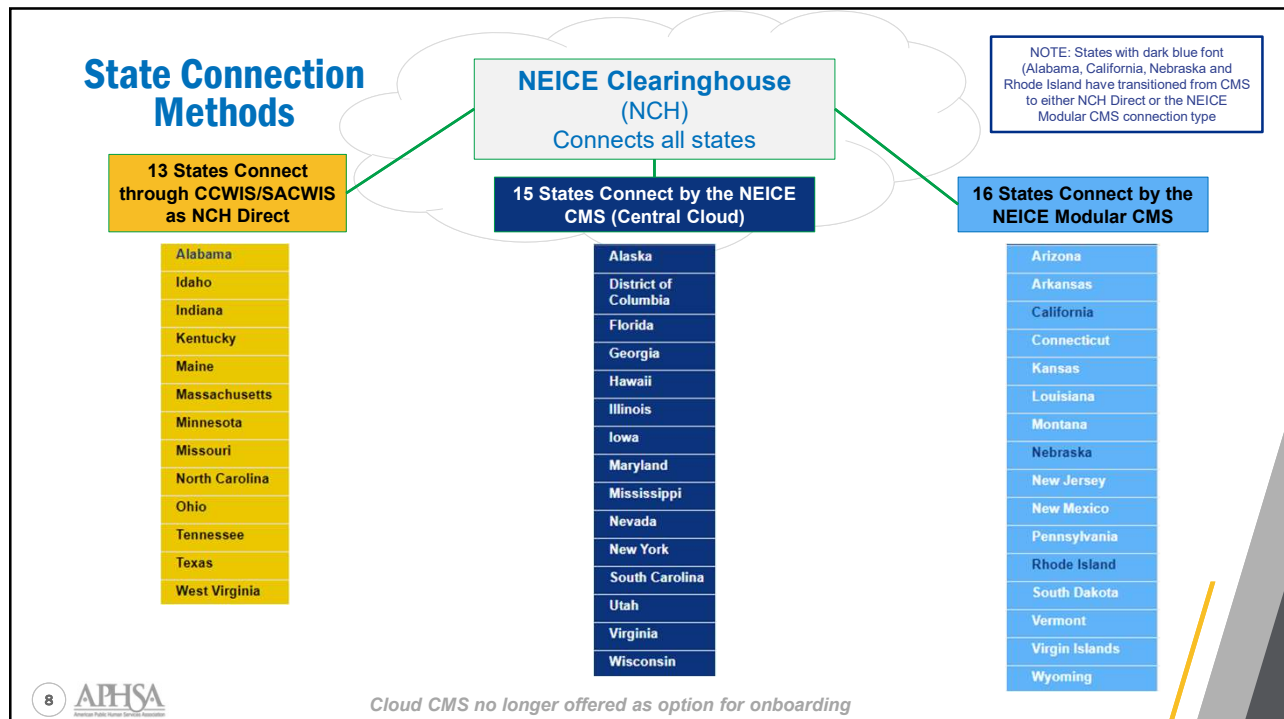


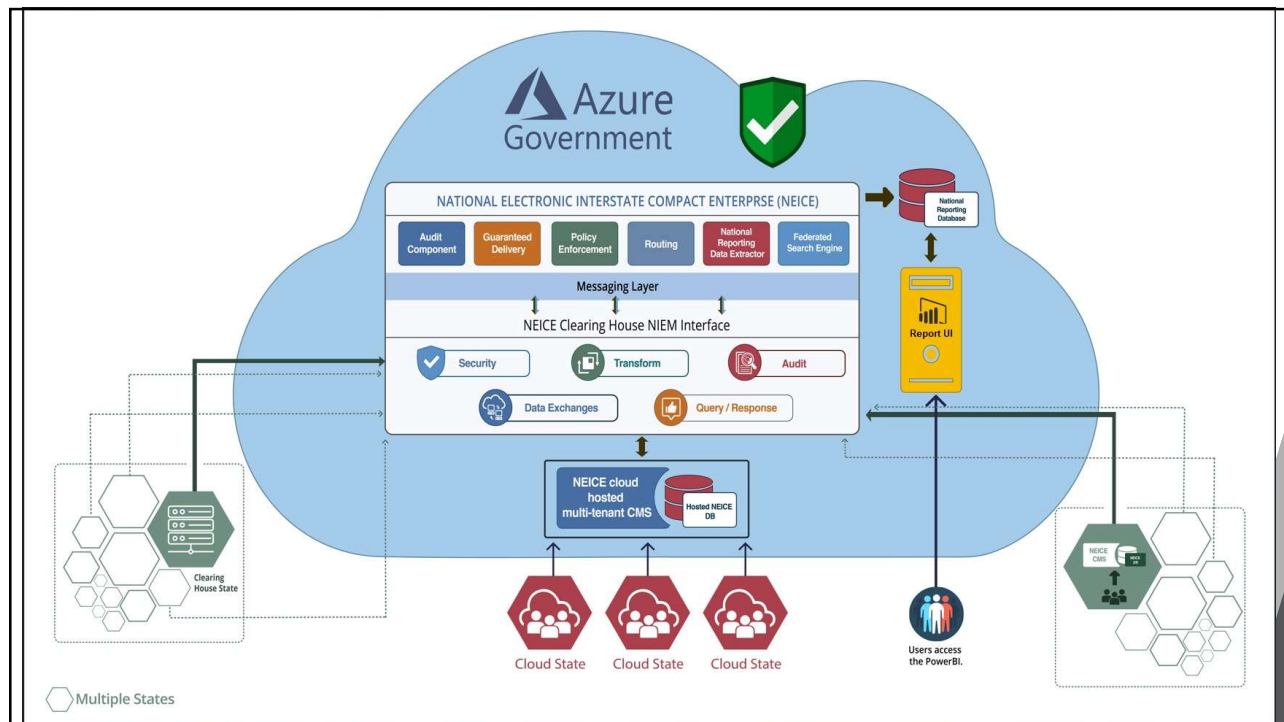
6

NEICE Versions

Three ways to connect

- Case Management System (CMS) (No longer available)
- Modular Case Management System (MCMS)
- National Clearinghouse Direct (NCH)





9

NEICE Security Policies

- ⚙ Meet NISTSP800-30, Risk Management Guide for IT Systems and Regulation 45 CFR Part 164
- ⚙ FedRamp, HIPAA, CJIS compliant
- ⚙ Currently Reviewing NIST 2.0 Guidelines

10

Physical Security

- ⚙ **Two Data Centers:** Virginia & Arizona
- ⚙ **Production Servers:** Geo-fenced, restricting access to the Americas
- ⚙ **Azure Government Cloud:** Data centers are FedRamp compliant and meet HIPAA standards



11

Physical Security

Azure

- 🔲 **Azure Government** uses state of the art physical security
- 🟩 **Azure Defender** monitors threats and provides alerts



12

Network Security



- Data encrypted in transit using FIPS 140-2
- NEICE uses whitelisting IP addresses
- All communication uses HTTPS

Data

Data is encrypted in transit and at rest

PII and PHI are double encrypted - SQL storage encryption



Data Handling

- ⚙ CMS version stores all data in MS Azure Cloud
- ⚙ Backups – nightly rolled to weekly rolled to monthly rolled to annually
- ⚙ NCH stores **only meta data** transmitted to and from a NCH or MCMS state
- ⚙ Data is segregated and logically isolated within the network using network security groups

Staff and System Security Checks

- 🟩 APHSA and AAICPC staff only have access to meta data for reporting purposes
- 🟩 Clearinghouse only stores meta data
- 🟩 Annual HIPAA audits
- 🟩 APHSA had regular security audits this year
- 🟩 SOC II Audit completed this year



Contractor Staff Security

Tetrus Corporation

- ⚙ Contractor staff undergo background checks
- ⚙ Contractor staff must use office network or VPN with multifactor authentication – only two static IP addresses have access to resources
- ⚙ Select tools are used when troubleshooting issues where PII/PHI data may be accessed
- ⚙ Contractor has annual HIPPA audits
- ⚙ Contractor had a SOC II Audit completed this year
- ⚙ Contractor staff trained on safe handling of data

User/Participant Security

CMS and MCMS Versions

- ⚙ Acceptable Use Policy for users
- ⚙ Strong password rules
- ⚙ Multi-factor authentication available
- ⚙ Five levels of role-based security
- ⚙ Audit trails for every case – monitoring who opens, views or alters a case (CMS Version)



Security: User Access

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 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. (outlined in the MOU)
- Asks NEICE users to sign a User Acceptable Use Policy document prior to gaining access to the system and annually thereafter (outlined in Appendix 3 and includes the responsibilities and expected behavior of all authorized Users).
- Provides annual security training for each state's lead NEICE ICPC Administrator/Deputy Administrator and IT staff for NEICE.



19


Security: State Obligations/Responsibilities


1. Check to ensure all state users have taken the eLearning Security training
2. Make sure to update the NEICE Project team of changes to NEICE Security Point of Contact
3. If a state or jurisdiction experiences a breach, notify the NEICE Project team within 24 hours.



20

Handling a Potential Data Breach Incident



21 

21

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.

22

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.



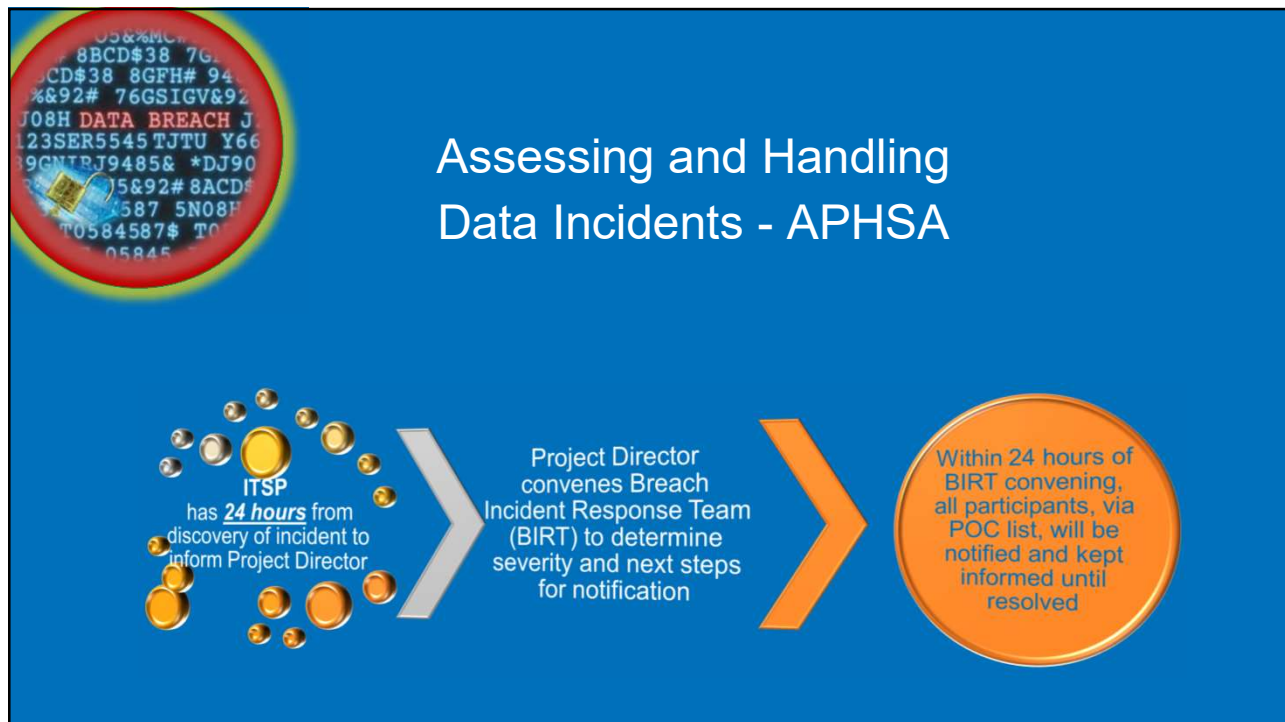
23

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.



24



25

How the BIRT Works



26

Post Breach



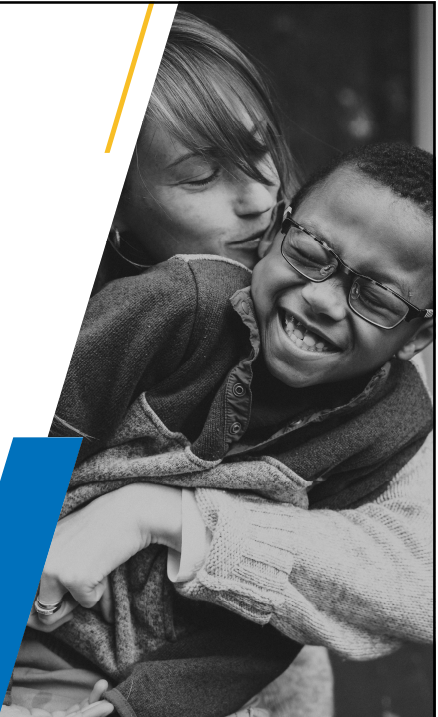
- Ensure system is secure
- Assess effectiveness of breach response



27



Questions



28