NC HealthConnex
Powering Health Care Outcomes

NORTH CAROLINA HEALTH INFORMATION EXCHANGE AUTHORITY

NC HealthConnex Teletown Hall: Data Privacy and Security

July 17, 2024

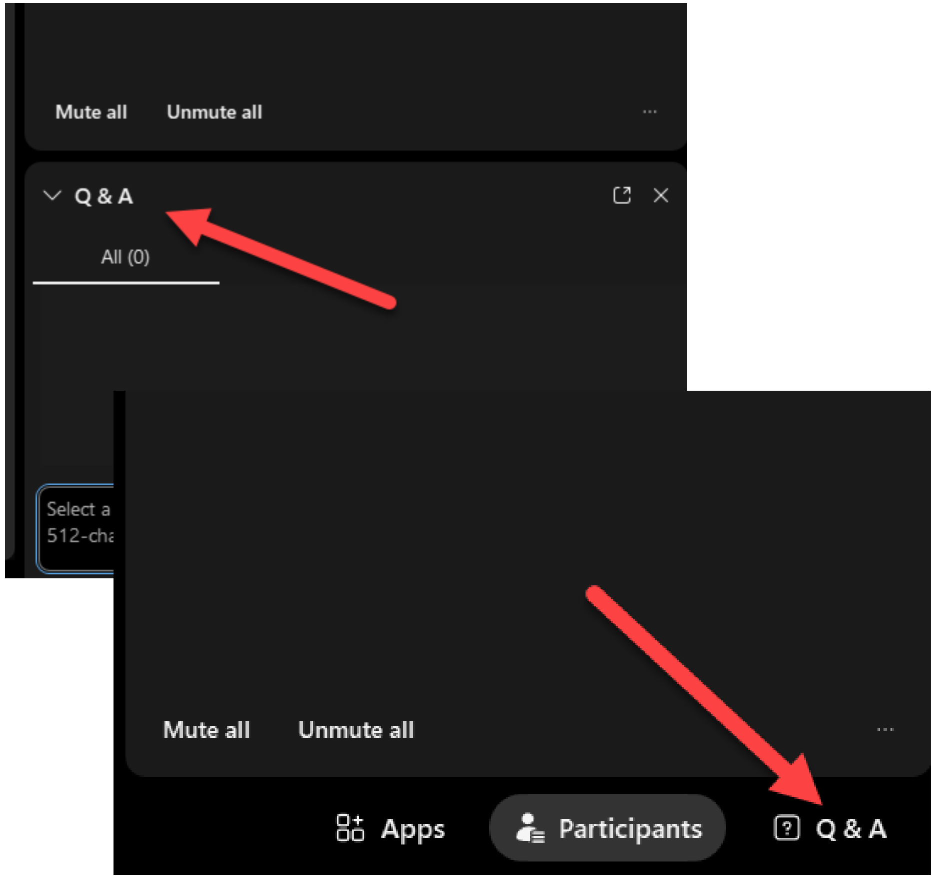
Hosted by:

Kenya Servia

Business Development and Outreach Specialist

NCDIT
NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Housekeeping Items Before We Start



- At the end, if you have a question, you can utilize the Q&A feature.

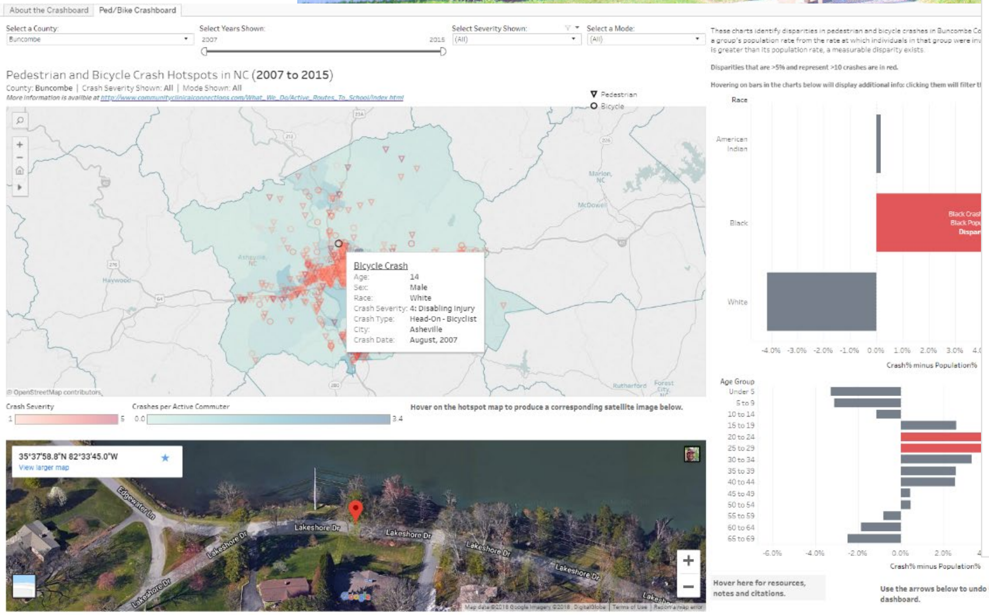
- A copy of the presentation slides will go out to everyone who registered for today's webinar.

Privacy and Security- Agenda

Overview of Topics

❖	Welcome and Introductions	Noon – 12:05	Kenya Servia/Sam Thompson
❖	Third-Party Risk & Security	12:05 – 12:25	Eric Zach
❖	Protecting Privacy	12:25 – 12:45	Cherie Givens
❖	Upgrade Update and More	12:45 – 12:50	Kenya Servia
❖	Questions and Answer	12:50 – 1:00	

How I got here



Select a County: Buncombe

Select Years Shown: 2007 – 2015

Select Severity Shown: (All)

Select a Mode: (All)

Pedestrian and Bicycle Crash Hotspots in NC (2007 to 2015)

County: Buncombe | Crash Severity Shown: All | Mode Shown: All

More information is availble at http://www.communityclinicalconnections.com/What_We_Do/Active_Routes_To_School/index.html

Bicycle Crash

Age: 14

Sex: Male

Race: White

Crash Severity: 4: Disabling Injury

Crash Type: Head-On - Bicyclist

City: Asheville

Crash Date: August, 2007

These charts identify disparities in pedestrian and bicycle crashes in Buncombe Co… a group's population rate from the rate at which individuals in that group were inv… is greater than its population rate, a measurable disparity exists.

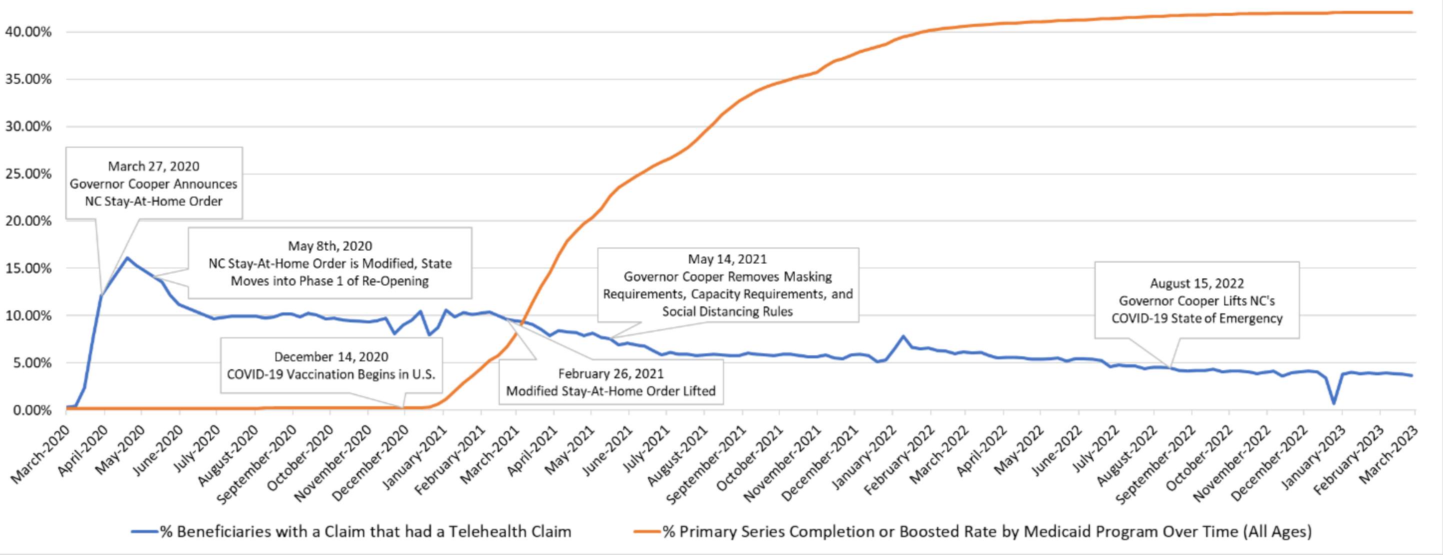
Disparities that are >5% and represent >10 crashes are in red.

Hovering on bars in the charts below will display additional info; clicking them will filter t…

Hover on the hotspot map to produce a corresponding satellite image below.

Hover here for resources, notes and citations.

Use the arrows below to undo (←), redo (→) or reset (|←) the dashboard.



March 27, 2020 Governor Cooper Announces NC Stay-At-Home Order

May 8th, 2020 NC Stay-At-Home Order is Modified, State Moves into Phase 1 of Re-Opening

December 14, 2020 COVID-19 Vaccination Begins in U.S.

February 26, 2021 Modified Stay-At-Home Order Lifted

May 14, 2021 Governor Cooper Removes Masking Requirements, Capacity Requirements, and Social Distancing Rules

August 15, 2022 Governor Cooper Lifts NC's COVID-19 State of Emergency

— % Beneficiaries with a Claim that had a Telehealth Claim

— % Primary Series Completion or Boosted Rate by Medicaid Program Over Time (All Ages)

Third Party Risk & Security

Guest Speaker

Eric Zach

Chief Information Security Officer

Eric Zach joined the N.C. Department of Information Technology in August 2019 and presently serves as the Chief Information Security Officer.

Eric has more than 10 years of IT leadership and experience within the military and federal government He served in the Air Force for 7 years as an electronic warfare technician, network administrator and instructor. He was awarded the Air Force Achievement and Commendation Medals for his actions while deployed.

Zach holds an associate in Instructor of Technology and Military Science and Avionic Systems technology, and a Bachelor of Science in Network Operations and Security from Western Governors University.

Eric currently supports NCDIT in providing security guidance to develop, deliver and maintain cybersecurity programs and tools that safeguard North Carolina’s systems and services from unauthorized use, disclosure, modification, damage or loss.

Third Party Risk – The growing threat landscape

Agenda

- Overview of Third-Party Risk findings
  - ➢ CrowdStrike
  - ➢ Security Score Card

- How do we effectively mitigate third party risks
  - ➢ Cybersecurity best practices
  - ➢ Data Sharing agreements
  - ➢ Contracts and Procurements

Key Findings – Security Score Card

1. At least 29% of breaches have third-party attack vectors
2. Prolific increase in third party compromises during CY 2023 – C10p (MoveIT)
3. Healthcare, Financial services, technology & telecommunications commonly targeted
4. 75% of external relationships involved software or other technology products and services
5. Complexity of healthcare environments adds to risk of third-party compromises

REPORT

Global Third-Party Cybersecurity Breaches

In-depth analysis of the most significant third-party cyber risks and incidents in 2023

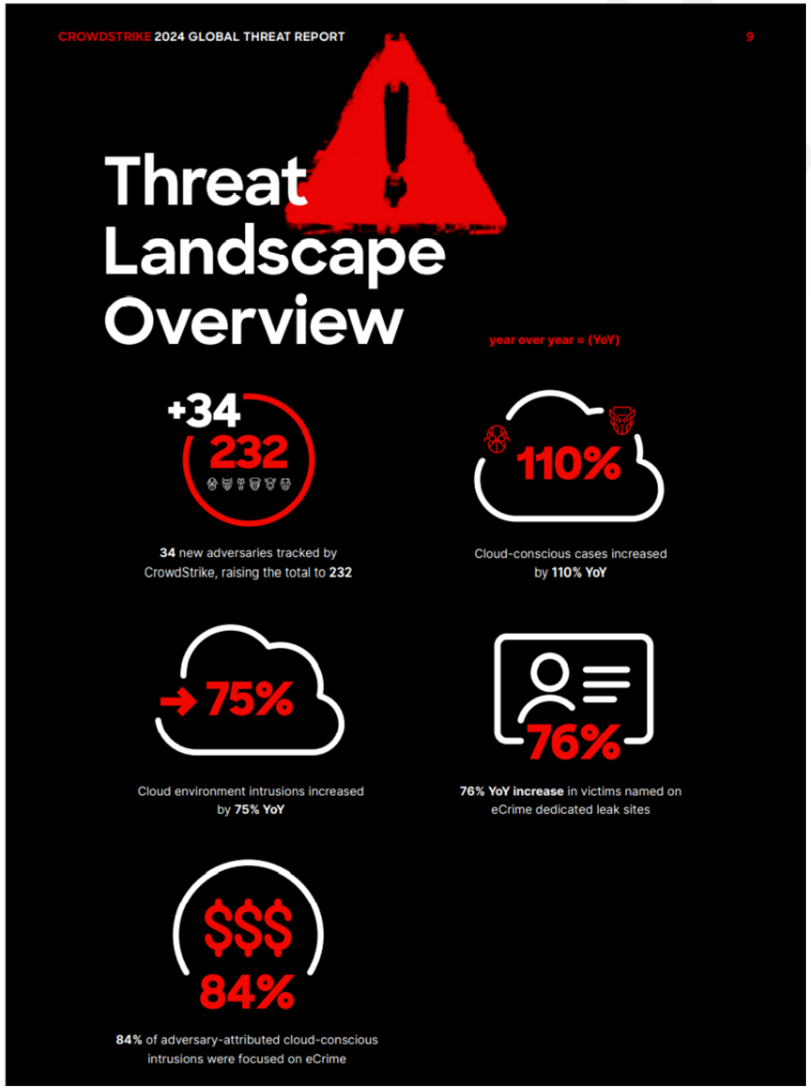
SecurityScorecard

Key Findings – CrowdStrike

- Threat actors consistently attempted to exploit trusted relationships to gain access to organizations across multiple sectors and regions.
- Targeted compromise of supply chain using trusted software and access to vendors supplying IT services.
- Motivated by greater potential return on investment (ROI).

Overview – CrowdStrike

- High ROI for third-party compromises will continue to attract threat actors as a means to initial access to organizations.
- Nearly every trusted-relationship compromise originated as part of an intrusion at a technology sector organization that provided commercial software.



CROWDSTRIKE 2024 GLOBAL THREAT REPORT 9

Threat Landscape Overview

year over year = (YoY)

+34
232

34 new adversaries tracked by CrowdStrike, raising the total to **232**

110%

Cloud-conscious cases increased by **110% YoY**

75%

Cloud environment intrusions increased by **75% YoY**

76%

76% YoY increase in victims named on eCrime dedicated leak sites

$$$
84%

84% of adversary-attributed cloud-conscious intrusions were focused on eCrime

Real World Impacts

UnitedHealth/Change Healthcare Compromise

- Criminals continue to adapt and develop sophisticated and malicious methodologies to impact critical infrastructure.
- Confirmed PII/PHI stolen in the breach involving “substantial portion of people in America”
- Remote access tool was compromised without MFA controls in place, leading to further compromise and ransomware deployment
- Healthcare professionals forced to leverage disaster recovery methods entering manual claim submissions
- https://www.msspalert.com/news/change-healthcare-cyberattack-event-timeline
- https://www.msspalert.com/news/major-healthcare-provider-hit-by-massive-cyber-attack-on-hundreds-of-pharmacies

Timeline of Events

- February 2024 – Reports significant breach of IT Systems resulting in system outages, large hospitals and other groups locked out of processing payments. Ransomware group, BlackCat claims responsibility of the attack.
- March 2024 – Healthcare organizations being faced with minimum cybersecurity standards under proposed bill from the senate. Services suspended and several federal lawsuits enacted against UnitedHealth. Ransomware payment of $22M paid.
- April 2024 – UnitedHealth confirms payment of ransomware as well as confirmed theft of files containing PII/PHI of a “substantial portion of people in America.”
- May 2024 – During testimony to the U.S. House of Energy and Commerce Committee, UnitedHealth indicates threat actors leveraged stolen credentials to access remote access tools without MFA to hijack and deploy ransomware on systems within 9 days of obtaining legitimate access.

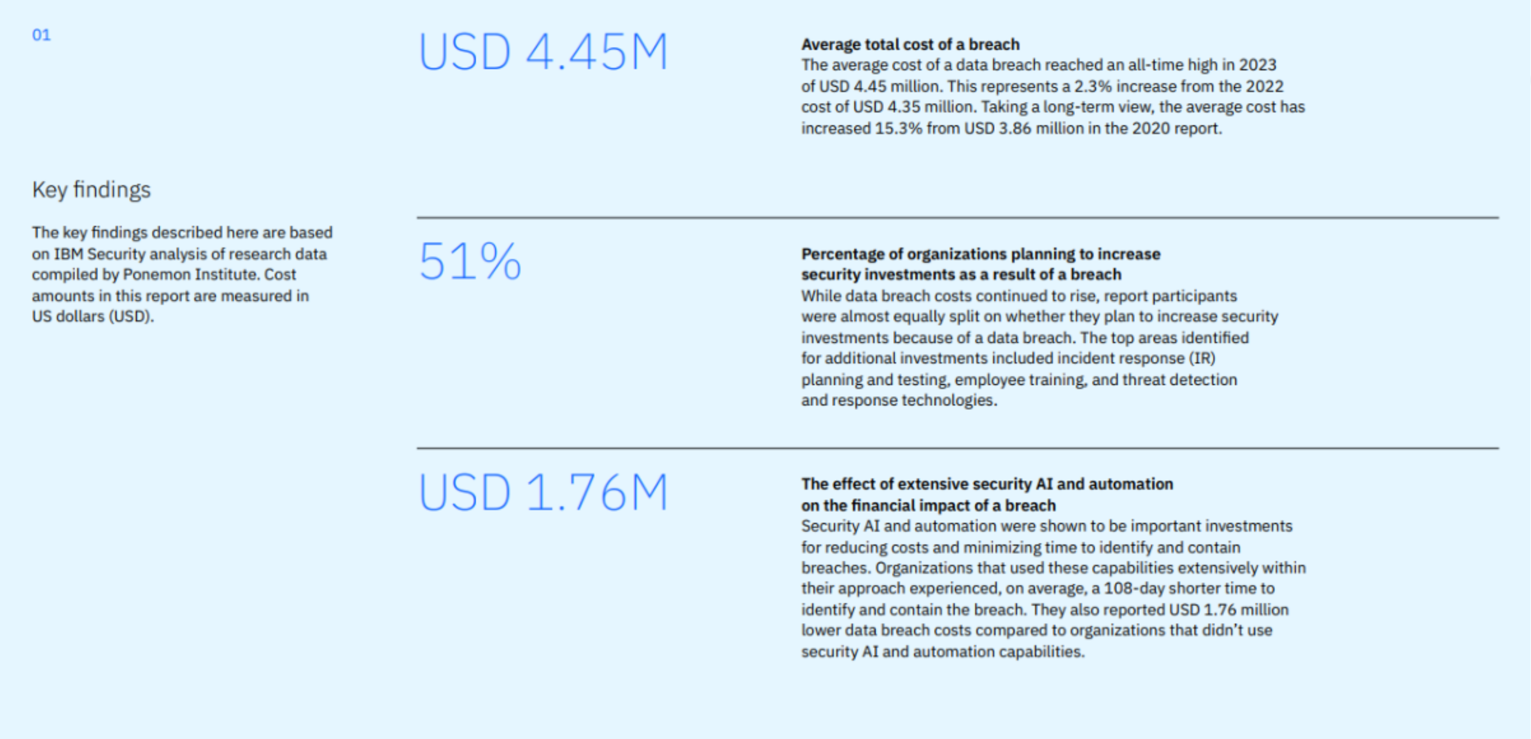
What Can We Do???

Cybersecurity Best Practices

- Request validation of industry compliance and governance frameworks, i.e. NIST, CIS, etc.

Contracts and Procurements

- Require breach notifications between parties
- Require security baseline controls and configurations
- Define responsibilities for breach notifications or other required responses due to data breaches



01

Key findings

The key findings described here are based on IBM Security analysis of research data compiled by Ponemon Institute. Cost amounts in this report are measured in US dollars (USD).

USD 4.45M

Average total cost of a breach
The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million in the 2020 report.

51%

Percentage of organizations planning to increase security investments as a result of a breach
While data breach costs continued to rise, report participants were almost equally split on whether they plan to increase security investments because of a data breach. The top areas identified for additional investments included incident response (IR) planning and testing, employee training, and threat detection and response technologies.

USD 1.76M

The effect of extensive security AI and automation on the financial impact of a breach
Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches. Organizations that used these capabilities extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach. They also reported USD 1.76 million lower data breach costs compared to organizations that didn't use security AI and automation capabilities.

Effective Data Sharing Agreements

- Ensure agreements between parties document responsibilities and requirements to share compromises between partners.
- Create collaborative partnerships and build rapport with vendors and partners

Protecting Privacy: A Presentation for the NC HIEA

Cherie Givens, Chief Privacy Officer

N.C. Department of Information Technology

July 17, 2024

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Guest Speaker

Cherie Givens

Chief Privacy Officer

As chief privacy officer for the state of North Carolina, Dr. Cherie Givens is responsible for a strategic and comprehensive statewide privacy program that defines, develops, maintains and implements policies and processes enabling consistent and effective information privacy practices.

Givens is a Certified Information Privacy Professional (CIPP/US), an attorney with more than 20 years of experience and holds a PhD in information science. She joined NCDIT in December 2021 after more than a decade supporting federal privacy programs in the Washington D.C. area.

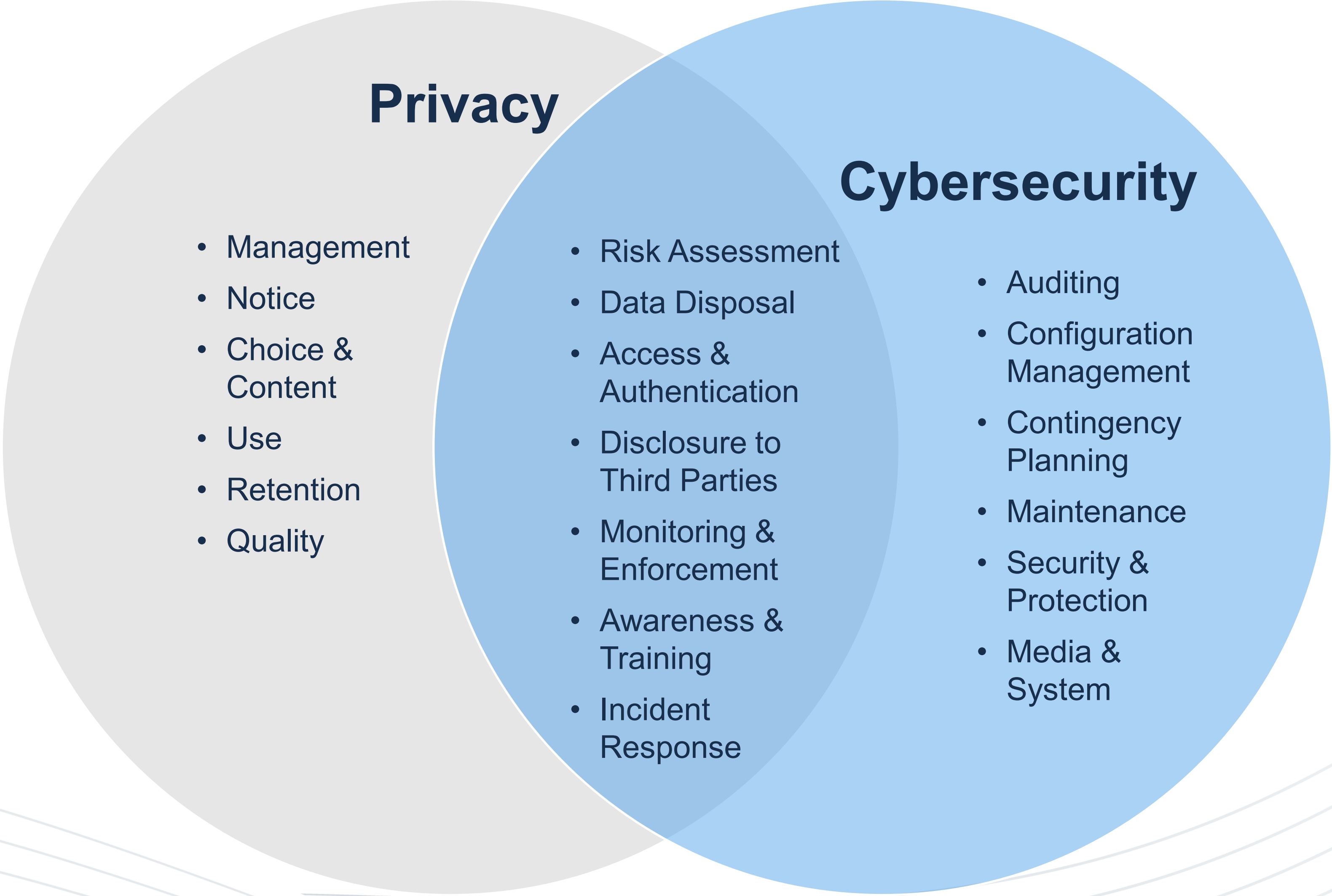
She has supported privacy at several federal agencies, including the U.S. Department of Health and Human Services, the U.S. Centers for Disease Control and Prevention and the U.S. Department of Defense, Chief Digital and Artificial Intelligence Office.

Givens is the author of “Information Privacy Fundamentals for Librarians and Information Professionals” as well as several book chapters on the topics of information privacy, cybersecurity and information governance.

What Is Data Privacy?

The right of individuals and organizations to control the collection and sharing of their personal information without consent.

Privacy: People, Processes, Policy, Privacy by Design



Privacy

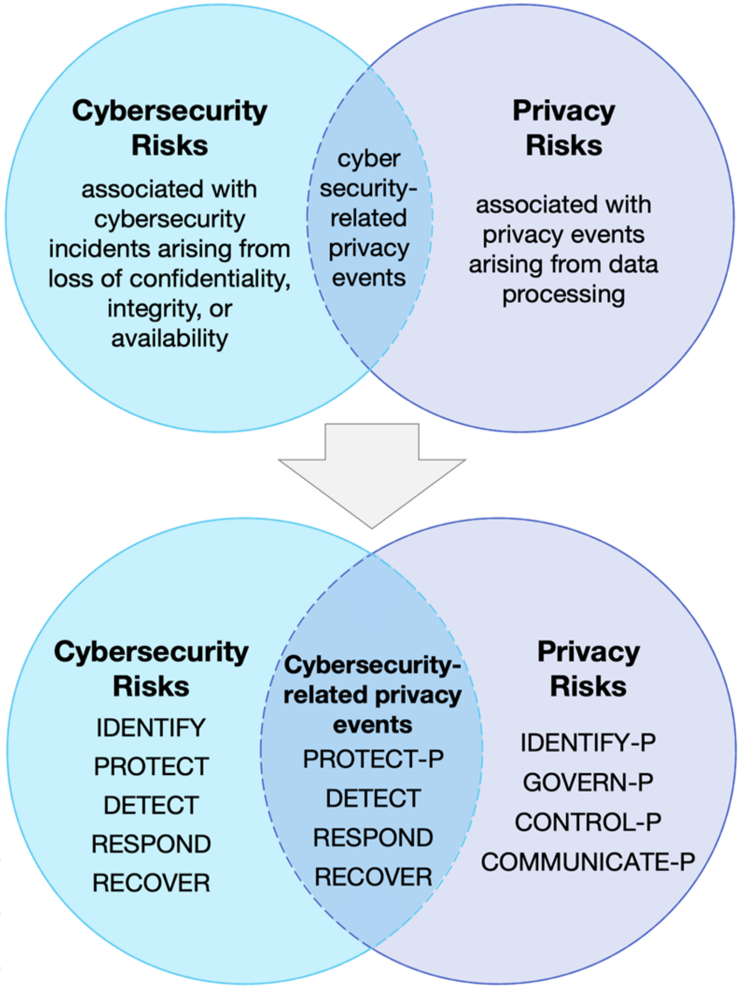
- Management
- Notice
- Choice & Content
- Use
- Retention
- Quality

- Risk Assessment
- Data Disposal
- Access & Authentication
- Disclosure to Third Parties
- Monitoring & Enforcement
- Awareness & Training
- Incident Response

Cybersecurity

- Auditing
- Configuration Management
- Contingency Planning
- Maintenance
- Security & Protection
- Media & System

Managing Privacy Risks



Cybersecurity Risks

associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability

cyber security-related privacy events

Privacy Risks

associated with privacy events arising from data processing

Cybersecurity Risks

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Cybersecurity-related privacy events

PROTECT-P
DETECT
RESPOND
RECOVER

Privacy Risks

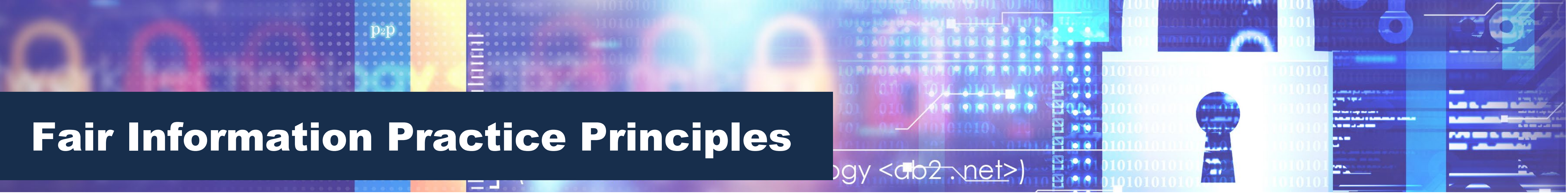
IDENTIFY-P
GOVERN-P
CONTROL-P
COMMUNICATE-P

1. **Identify**: Identify the data you are collecting, using, sharing, storing.
2. **Govern**: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
3. **Control**: Develop and implement appropriate activities to enable the organization or individuals to manage data with sufficient granularity to manage privacy risks.
4. **Communicate**: Develop and implement appropriate activities to enable the organization and individuals to have a reliable understanding about how data are processed and associated privacy risks.
5. **Protect** Develop and implement appropriate data processing safeguards. Security and privacy policies, processes, and procedures are maintained and used to manage the protection of data. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

Services to Agencies

Privacy Services Offered by the Office of Privacy and Data Protection:

- Guidance and Consultation
- Procurement-related Reviews
- Incident Response/Breach Support
- Federal Privacy Law Alignment Support
- Assessments/Assessment Support
- Privacy and Data Protection Maturity Assistance
- Data Breach Exercise Support



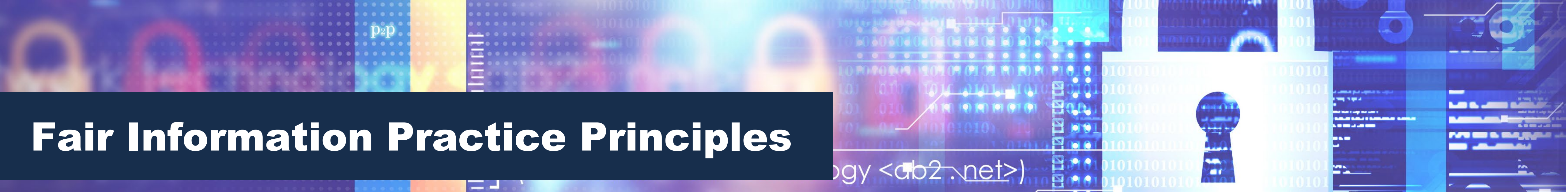
Fair Information Practice Principles

1. **Transparency:** The organization should be transparent and provide notice to the individual regarding its collection, use, dissemination and maintenance of personally identifiable information (PII).

2. **Individual Participation:** Consent should be sought from the individual for the collection, use, dissemination and maintenance of PII. A mechanism should also be provided for appropriate access, correction and redress regarding the organization's use of PII.

3. **Purpose Specification:** The organization should specifically articulate the authority that permits the collection of PII and the purpose(s) for which the PII is intended to be used.

4. **Data Minimization:** The organization should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as it is necessary to fulfill those purpose(s).



Fair Information Practice Principles

5. **Use Limitation:** The organization should use PII solely for the purpose(s) specified in the notice. Sharing PII outside of the organization should be for a purpose compatible with the purpose(s) for which the PII was collected.

6. **Data Quality and Integrity:** The organization, to the extent practicable, should ensure that PII is accurate, relevant, timely and complete.

7. **Security:** The organization should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. **Accountability and Auditing:** The organization should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Proactive Steps to Support Privacy

Supporting Patients’ Right to Privacy Regarding Their Health Information

- Front Desk Operations: It’s important to consider who can hear discussions of a patient’s medical condition.
- Preserve privacy in the waiting room, at the front desk, throughout the visit.
- Discussing a patient’s medical condition where the conversation can be overhead by others violates privacy and can lead to feelings of embarrassment, stigma, or distress for the individual.
- Unauthorized Disclosure: If the conversation reveals specific details about a person's health condition, treatment, or medical history, it constitutes an unauthorized disclosure of PHI. HIPAA regulations strictly prohibit the unauthorized disclosure of PHI, whether intentional or accidental.

Proactive Steps to Support Privacy

Supporting Patients’ Right to Privacy Regarding Their Health Information

- Front Desk Operations: In addition to overhearing information about medical conditions, there is a risk that phone calls can be overheard where patients are asked to confirm their name, address, other personal information and may even be asked about credit card information.
- Adopting a privacy-by-default mindset means that privacy is built in and a concern for when interacting with patients in all contexts – by phone, online, and in person.
- Consider who may be able to overhear and what information they may gain from listening to conversations or reading screens.

Proactive Steps to Support Privacy

Data Quality and Integrity: Instilling Trust by Implementing Fair Information Practice Principles

Implementing Fair Information Practice Principles (FIPPs) increases trust.

Data Quality and Integrity: Data quality and integrity is key not only to providing quality medical care but also to instilling public trust.

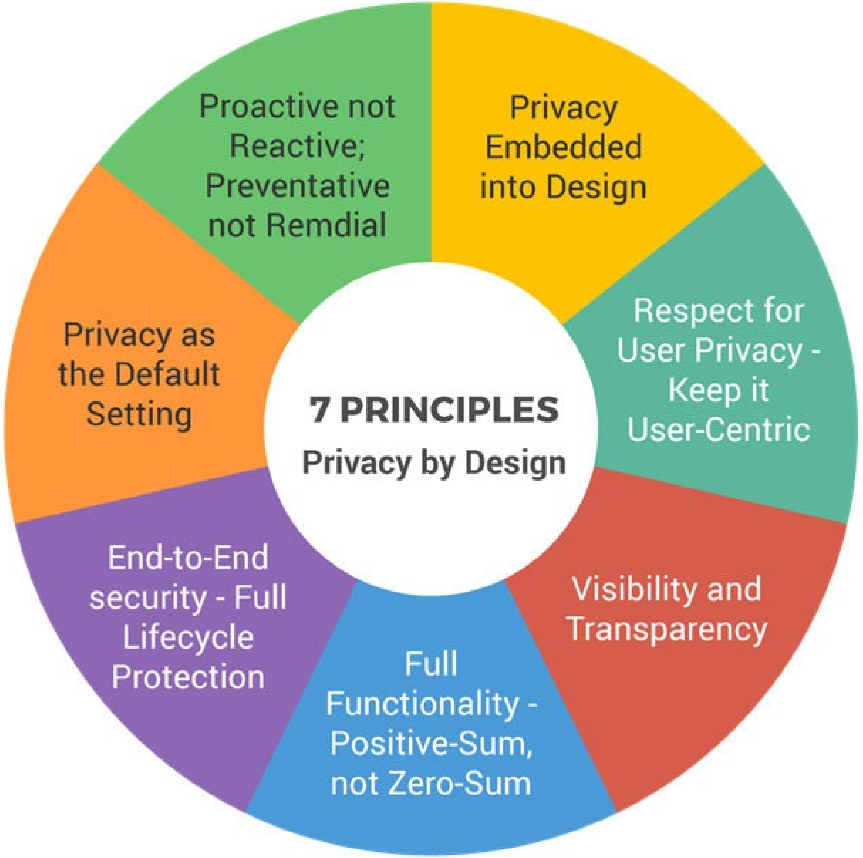
- What process do you have in place to help patients correct mistakes in their records?
- How are staff trained to respond to concerns expressed by patients about incorrect information being held about them and the request to correct that data?

Related Articles:

Problem of mixed-up patient records has been an issue for quite a while: NPR, October 2016, Report: Medical Record Mix-ups Are A Common Problem.

Article: Torrey, Tisha, January 2024, VeryWellHealth, How to Correct Errors in Your Medical Records Mistakes can affect your health care and outcomes.

Privacy by Design (PbD)


7 PRINCIPLES
Privacy by Design
Privacy Embedded into Design
Respect for User Privacy - Keep it User-Centric
Visibility and Transparency
Full Functionality - Positive-Sum, not Zero-Sum
End-to-End security - Full Lifecycle Protection
Privacy as the Default Setting
Proactive not Reactive; Preventative not Remdial

- Concept developed to address the ever-growing and systemic effects of information and communication technologies, and of large-scale networked data systems

- Privacy by Design – Proactive rather than reactive

- Privacy cannot be assured solely by compliance with regulatory frameworks (i.e., HIPAA)

- Privacy as the default mode of operation

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Questions?

cherie.givens@nc.gov

NC HIEA Internal Updates and Approach to Privacy & Security

NC HealthConnex Upgrade

An upgrade is coming to the NC HealthConnex platform in August 2024.

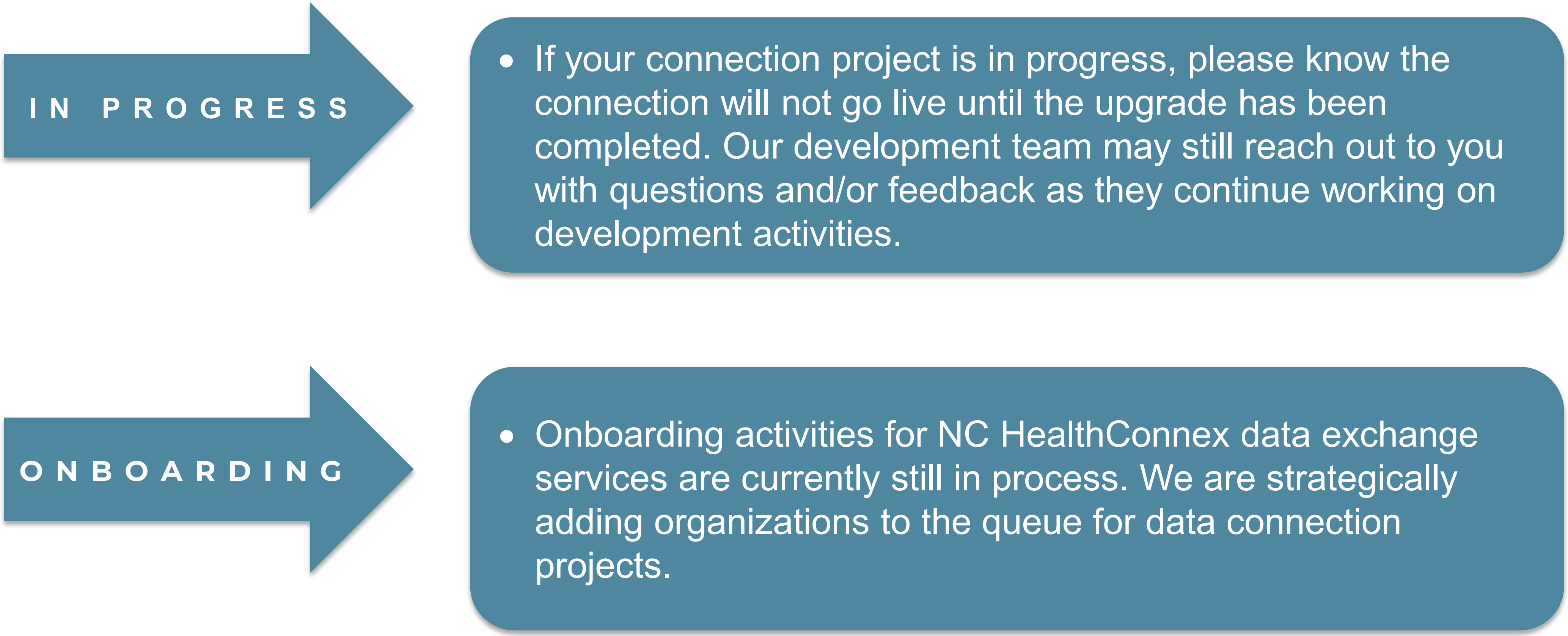
Reasons for the upgrade:

- Modernize the NC HealthConnex infrastructure to current health information exchange standards.
- Improved system performance.
- Better user experience.
- Benefits for Clinical Portal users, including:
    - Improved Clinical Summary section allowing data to be viewed in 2 columns.
    - Ability to do a text search within individual chartbook pages.
    - Additional clinical sections within the patient record.

NC HealthConnex Upgrade

This upgrade may have different considerations for your practice depending on where you are in the connection process.

What This Means For Your Practice:



IN PROGRESS

- If your connection project is in progress, please know the connection will not go live until the upgrade has been completed. Our development team may still reach out to you with questions and/or feedback as they continue working on development activities.

ONBOARDING

- Onboarding activities for NC HealthConnex data exchange services are currently still in process. We are strategically adding organizations to the queue for data connection projects.

NC HealthConnex Upgrade

This upgrade may have different considerations for your practice depending on where you are in the connection process.

What This Means For Your Practice:

NOT STARTED

- If your connection project has not yet started, you will remain in our onboarding queue until after the upgrade is complete.

ALREADY LIVE

- If you are already live, meaning your practice is already submitting data to NC HealthConnex, there is no action you need to take at this time.

NC HealthConnex is a Secure, Private Network

NC HIEA Policies

Privacy and Security Policy	Dec. 16, 2021
User Access Policy	April 5, 2021
Behavioral Health Sensitive Data Policy	Nov. 15, 2018
Opt-Out Information	Aug. 29, 2023

Privacy & Security

User Access

Sensitive Data

Opt Out

NC HealthConnex is a Secure, Private Network

Privacy & Security

- The NC HIEA follows the highest information security standards available
- Information is always encrypted and sent over a private network
- NC HealthConnex is compliant with all federal and state privacy and security laws
- Information that identifies patients will not be sold in any way or shared with anyone other than authorized health care providers or organizations that have entered into HIPAA compliant, data-sharing agreements

Privacy & Security

User Access

Sensitive Data

Opt Out

NC HealthConnex is a Secure, Private Network

User Access

We take our role of data stewards seriously and expect that our participants will as well.

- Role-based access to control access levels for each authorized user
- Participant Account Administrator (PAA) will be responsible for assigning roles to users; NC HealthConnex Help Desk will provide credentials to these users (PAA Reference Guide)
- Access to patient information granted if established treatment relationship with the patient

Privacy & Security

User Access

Sensitive Data

Opt Out

NC HealthConnex is a Secure, Private Network

Sensitive Data Policy

Federal laws and regulations prevent the NC HIEA from receiving and/or managing certain types of mental health or substance use treatment data.

Federal regulations in 42 C.F.R. Part 2 prohibit certain health care providers who participate in that program from disclosing data that would identify a patient as having a substance use disorder (SUD) unless the regulations specifically allow the disclosure. Regardless of patient consent, at this time SUD information CANNOT be sent to NC HealthConnex.

If you are unsure, then consult with your legal counsel to determine if you are a federally-assisted drug abuse program that must comply with 42 C.F.R. Part 2.

Mental health providers should not send psychotherapy notes (as defined in HIPAA) to NC HealthConnex.

Privacy & Security

User Access

Sensitive Data

Opt Out

What Cannot Be Submitted?

Participants cannot submit:

- ❖ 42 CFR Part 2 data (Substance Use Disorder)
- ❖ Psychotherapy Notes*

*The HIPAA Privacy Rule defines “psychotherapy notes” as follows: Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual’s medical record. **Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.**

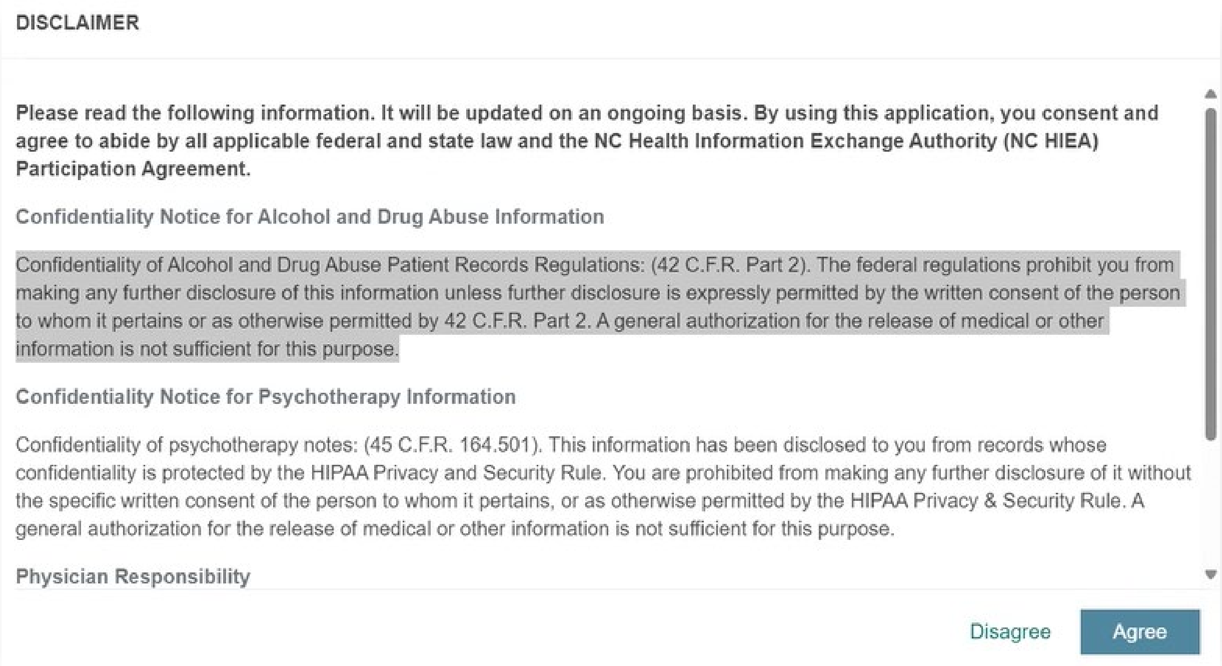
Where We Are Headed on Part 2 Data

Major Changes in the New Part 2 Rule - Patient Consent

- Allows a single consent for all future uses and disclosures for treatment, payment, and health care operations.
- HIPAA covered entities and business associates that receive records under this consent can redisclose the records in accordance with the HIPAA regulations.

Next Steps in Planning:

- **Allowing Part 2 providers to submit panels for notifications and engage in bidirectional exchange**
  - Part 2 data captured for this purpose would be completely and permanently internal.
- **Ingesting/storing/exchanging Part 2 clinical data**
  - We are starting to explore:
    - Solutions for capturing consent
    - Models for ingestion/storage/exchange
    - Major cost considerations



DISCLAIMER

Please read the following information. It will be updated on an ongoing basis. By using this application, you consent and agree to abide by all applicable federal and state law and the NC Health Information Exchange Authority (NC HIEA) Participation Agreement.

Confidentiality Notice for Alcohol and Drug Abuse Information

Confidentiality of Alcohol and Drug Abuse Patient Records Regulations: (42 C.F.R. Part 2). The federal regulations prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose.

Confidentiality Notice for Psychotherapy Information

Confidentiality of psychotherapy notes: (45 C.F.R. 164.501). This information has been disclosed to you from records whose confidentiality is protected by the HIPAA Privacy and Security Rule. You are prohibited from making any further disclosure of it without the specific written consent of the person to whom it pertains, or as otherwise permitted by the HIPAA Privacy & Security Rule. A general authorization for the release of medical or other information is not sufficient for this purpose.

Physician Responsibility

Whe

Maj

s.

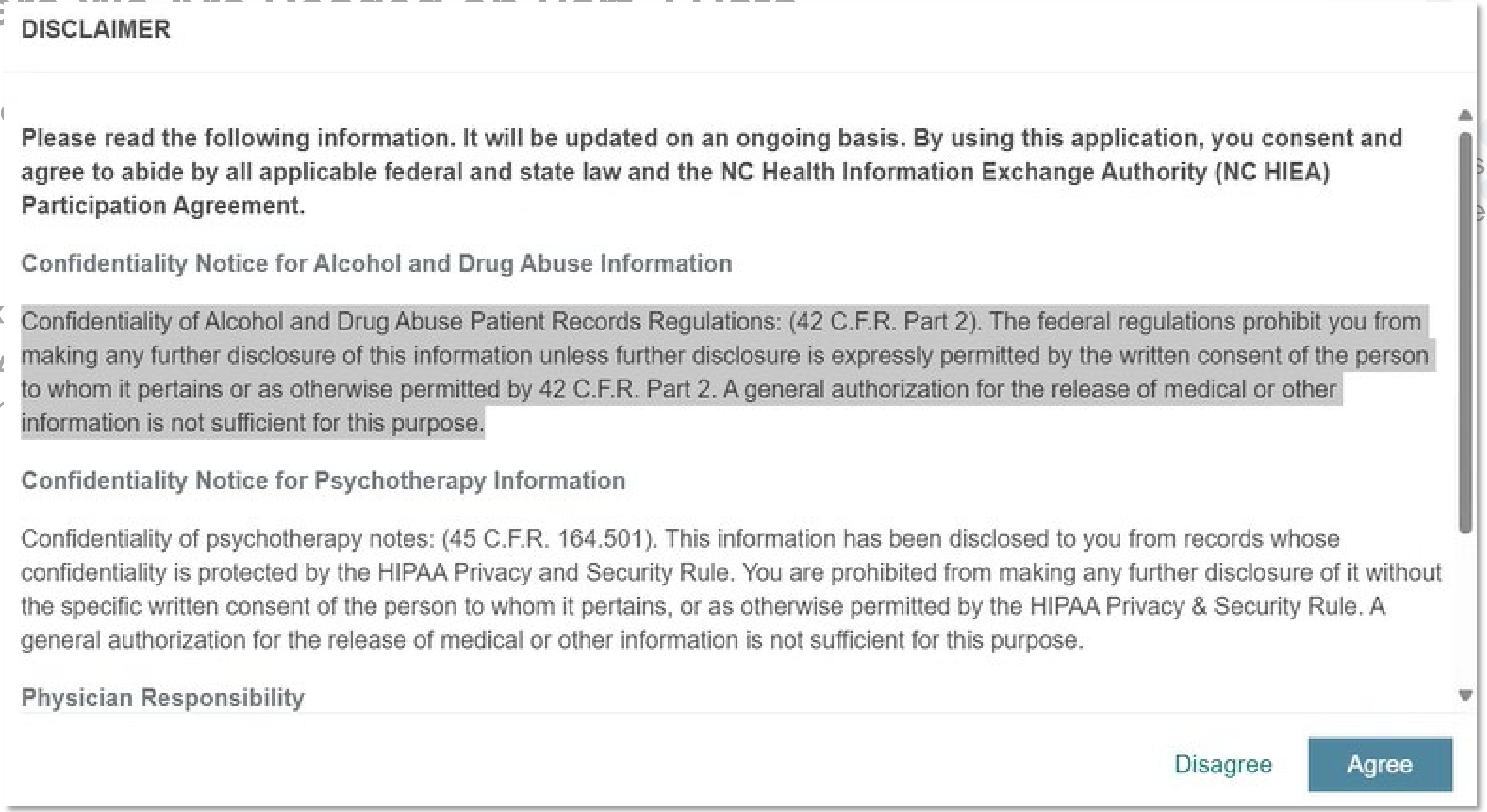
ecords

Nex

- A

r

- I



DISCLAIMER

Please read the following information. It will be updated on an ongoing basis. By using this application, you consent and agree to abide by all applicable federal and state law and the NC Health Information Exchange Authority (NC HIEA) Participation Agreement.

Confidentiality Notice for Alcohol and Drug Abuse Information

Confidentiality of Alcohol and Drug Abuse Patient Records Regulations: (42 C.F.R. Part 2). The federal regulations prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose.

Confidentiality Notice for Psychotherapy Information

Confidentiality of psychotherapy notes: (45 C.F.R. 164.501). This information has been disclosed to you from records whose confidentiality is protected by the HIPAA Privacy and Security Rule. You are prohibited from making any further disclosure of it without the specific written consent of the person to whom it pertains, or as otherwise permitted by the HIPAA Privacy & Security Rule. A general authorization for the release of medical or other information is not sufficient for this purpose.

Physician Responsibility

Direct Secure Messaging (DSM)

Although Part 2 data and psychotherapy notes cannot be submitted to the NC HealthConnex data repository, participants are permitted to share these types of information via Direct Secure Messaging (DSM) with other participants through NC HealthConnex.

The provider sending the message must comply with applicable law and obtain the required consent or authorization from the patient before disclosing the data via DSM.

NC HealthConnex is a Secure, Private Network

Opt Out

North Carolina is an opt out state (since 2012). Patients are opted into health information exchange for HIPAA-approved treatment, payment and operations purposes across all information exchanges (public and private).

The HIE Act requires participating health care providers to provide education materials to patients on the benefits of health information exchange and their right to opt out of exchange (or rescind).

The NC HIEA provides:

- Sample notice of privacy practices
- Tri-fold brochure order form
- Talking points, FAQs, Fact sheet
- Employee education materials

Privacy & Security

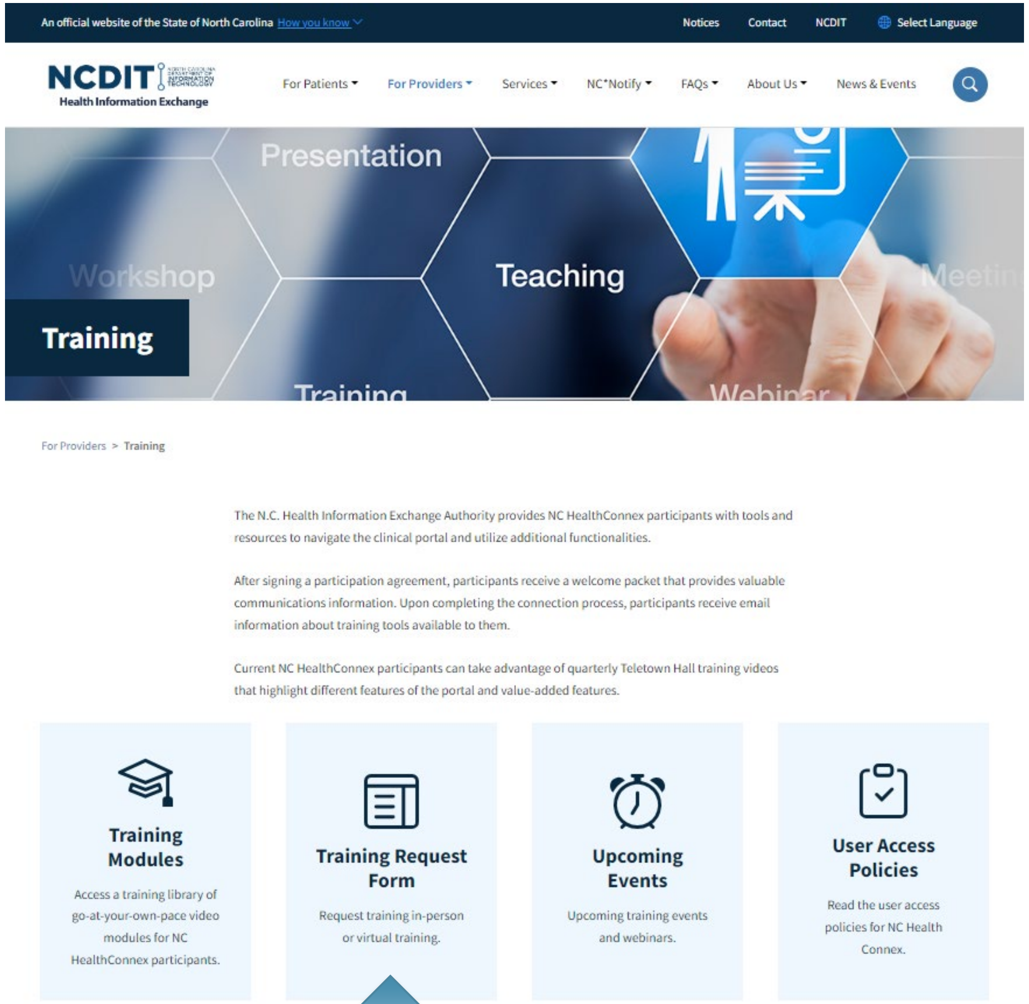
User Access

Sensitive Data

Opt Out

Questions & Answers

Training Opportunities/Upcoming Events



For Providers > Training

The N.C. Health Information Exchange Authority provides NC HealthConnex participants with tools and resources to navigate the clinical portal and utilize additional functionalities.

After signing a participation agreement, participants receive a welcome packet that provides valuable communications information. Upon completing the connection process, participants receive email information about training tools available to them.

Current NC HealthConnex participants can take advantage of quarterly Teletown Hall training videos that highlight different features of the portal and value-added features.

Training Modules
Access a training library of go-at-your-own-pace video modules for NC HealthConnex participants.

Training Request Form
Request training in-person or virtual training.

Upcoming Events
Upcoming training events and webinars.

User Access Policies
Read the user access policies for NC Health Connex.

- On Demand Training
  - NC HIEA Training Modules
- Live 1:1 Training
  - Training Requests
- Online Training (Webinars)
  - Teletown Hall
  - Office Hours

Upcoming Events

- Teletown Hall:

  October 30, 2024, 12:00 p.m. – 1:00 p.m.

- Office Hours:

  August 14, 2024, 12:00 p.m. – 1:00 p.m.

  November 13, 2024, 12:00 p.m. – 1:00 p.m.

Thank You!

For more information visit,

www.nchealthconnex.gov

Tel: 919-754-6912

E-mail: hiea@nc.gov

For technical support,

Tel: 919-531-2700

E-mail: HIESupport@sas.com

DO NOT SEND PHI to the NC HIEA or to the Help Desk!