N.C. Department of Information Technology Cybersecurity Presentation for HIE

Rob Main
State Chief Risk Officer

June 2022

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

NCDIT Overview

Rob Main
State Chief Risk Officer

- Appointed October 2021
- More than 32 years IT experience
- Formerly deputy state chief risk officer; CIO for N.C. Department of Military and Veteran Affairs, N.C. Office of State Human Resources and N.C. Department of Insurance
- Retired in May 2015 from the United States Air Force after 25 years of service

NCDIT Agency Priorities

- Broadband and connectivity

- Cybersecurity and privacy
  - Pertaining to Protected Health Information, areas of effort include:
    - Ensuring the confidentiality, integrity, and availability of all e-PHI created, received, maintained or transmitted
    - Identify and protect against reasonably anticipated threats to the security or integrity of the information
    - Protect against reasonably anticipated, impermissible uses or disclosures
    - Ensure compliance by our workforce
    - Provide safeguards to protect the privacy of protected health information

- Digital transformation

NCDIT ESRMO Overview

- Cyber policies, procedures and project reviews
- Cyber awareness and training
- Forensics
- Vulnerability management and incident response
- Security control assessments and audits
- NIST SP 800-53 as risk management framework
- Continuous monitoring plan for annual reporting

NCDIT ESRMO Overview

- NCDIT's state security operations center processes nearly 14 billion events per week.

- The N.C. Joint Cybersecurity Task Force, under the technical leadership of NCDIT's Enterprise Security and Risk Management Office, extended intrusion detection and prevention services to 42 North Carolina counties, adding iSensors to augment local governments' existing security controls and ability to defend themselves against cyberthreats.

NCDIT ESRMO Overview

- NCDIT, as a founding member and equal partner in the N.C. Joint Cybersecurity Task Force, supported 42 state, local and academic institutions with incident response support, remediation and recovery from significant cybersecurity incidents.

- More than 100 events; 31 incident responses.
  - 8 county governments
  - 8 municipal governments
  - 5 state agencies
  - 4 community colleges/universities
  - 1 K-12 school system
  - 1 county rescue squad
  - 1 regional airport
  - 1 city utility provider

Threat Landscape

- Geopolitical and criminal concerns
- SolarWinds (2019)
- Microsoft Exchange HAFNIUM (2021)
- Log4J (2021- ?)
- Vendor supply-chain risks
- Phishing, vishing, smishing, pharming
- Email spoofing
- Social engineering

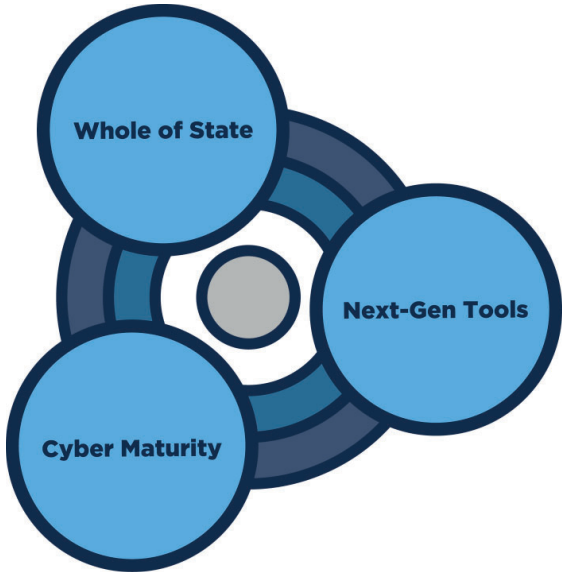
2021 Health Care Related Cyber Crime

- 16 CONTI ransomware attacks targeting healthcare and first responder networks in May 2021
- Healthcare and Public Health CIKR sector the most frequent victim of ransomware attacks (nearly double the amount of the next highest sector)
- Over $7M in victim loss resulting from health care related cyber incidents

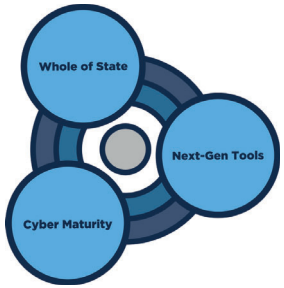
Source: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Priorities

- Strengthen the whole-of-state approach to cybersecurity.
- Increase the cyber maturity for the state.
- Integrate next-generation security tools across the enterprise.



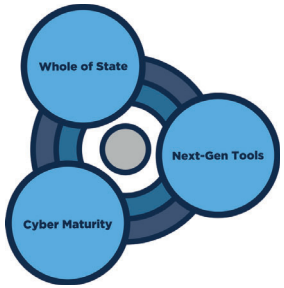
Priorities



Strengthen the whole-of-state approach to cybersecurity.

- Continue to build upon the N.C. Joint Cyber Security Task Force's success in proactive and responsive activities.
- Expand the scope of continuous monitoring for state and local governments.
- Establish a statewide program for monitoring of threats.
- Enhance visibility and optimize cyber intelligence sharing.

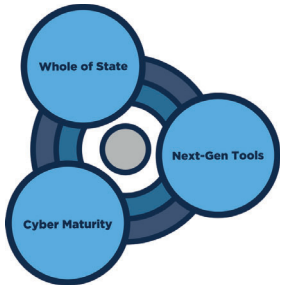
Priorities



Increase the cyber maturity for the state.

- Create standard and repeatable processes.
- Align cyber strategies to strategic business plans.
- Gain insight into current state through cybersecurity risk visualization and focus on high-value/high-risk objectives.
- Adopt StateRAMP for verification of cloud security for service providers.
- Promote inclusive and innovative cyber education programs and opportunities to broaden the talent pool of cybersecurity professionals.

Priorities



Integrate next-generation security tools across the enterprise.

- Incorporate a mixture of machine learning and artificial intelligence to shift from reactive to proactive postures.
- Automate cyber responses to allow teams to focus on significant incidents.
- Reduce the IT footprint and excessive pivoting by incident response team across multiple solutions.
- Reduce redundancy across state agencies through leveraging common platforms.
- Consolidate work force training and resource needs.

Legislative Updates

$7.5 million in recurring funding for cybersecurity and risk management in the 2021-2023 state budget.

- NCDIT will strengthen its cyber defense and enhance the whole-of-state approach to cybersecurity.
- Previously, we only had one-time funding sources, which was not a reliable means by which cyber programs and initiatives can be sustained and matured.

Legislative Updates

House Bill 813: *Prohibit State Agencies Payment of Ransom*

- Filed in May 2021
- Supported but not endorsed by NCDIT
- Prohibits state agencies and local government entities from paying ransoms or engaging with attackers

Exercises & Training

- N.C. Cybersecurity Awareness Symposium (2021)
  - 19 sessions
  - 628 attendees from state and local agencies, K-12 and community colleges
  - 14% increase in attendance from 2020
- Cyber Shield 2021
- Vendor Risk Management Workshop
- Mandatory training for state employees
- State employee town hall

Thank you.

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Privacy Presentation for HIEA Advisory Board

Cherie Givens, Chief Privacy Officer
June 16, 2022

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

NCDIT has implemented the Fair Information Practice Principles (FIPPs)

1. Transparency
2. Individual Participation
3. Purpose Specification
4. Data Minimization
5. Use Limitation
6. Data Quality and Integrity
7. Security
8. Accountability and Auditing

NCDIT FIPPS: https://it.nc.gov/resources/data-protection-privacy
Adapted from Teufel, H. (2008, December 29) The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security [Memorandum]. Department of Homeland Security.

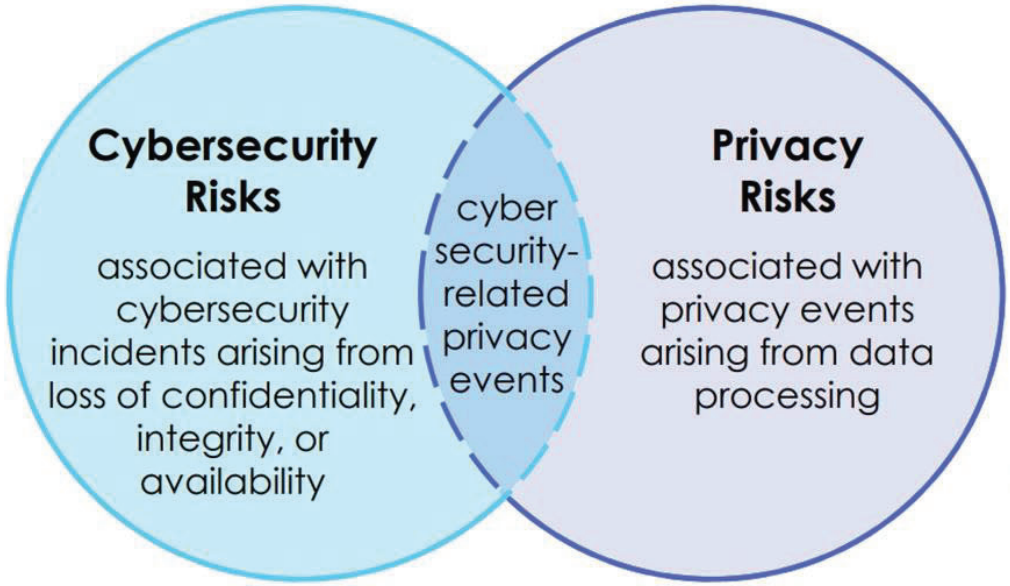
NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Implementing Privacy by Design (PbD)

- Proactive not reactive; preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Relationship Between Cybersecurity and Privacy Risks



Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions.

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal).

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

NIST, Privacy Framework Presentation, December 2019

Five Privacy Risk Management Areas

1.Identify: The data you are collecting, using, sharing, storing (map the flow, inventory the data to know the risks and mitigate).

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 agencies or individuals to manage data with sufficient granularity to manage privacy risks.

4. Communicate: Develop and implement appropriate activities to enable the agency and individuals to have a reliable understanding about how data are processed and associated privacy risks.

5. Protect (Overlapping with Security): Develop and implement appropriate data processing safeguards.

*See NIST SP 800-53 and NIST Privacy Framework for more guidance

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Privacy and Data Protection Joint Effort

Enterprise Security and Risk Management & Privacy:

- Develop and implement appropriate data processing safeguards.
- Create inclusive incident response policies and processes.
- Inventory and track HIE data.
- Work with HIE vendors to ensure privacy and security including requiring HIE vendors to complete privacy and security training.
- Include privacy and security provisions in HIE vendor agreements – training, audit, compliance acknowledgement, support for privacy and security.

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Privacy questions?
Send questions to ditprivacy@nc.gov.

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

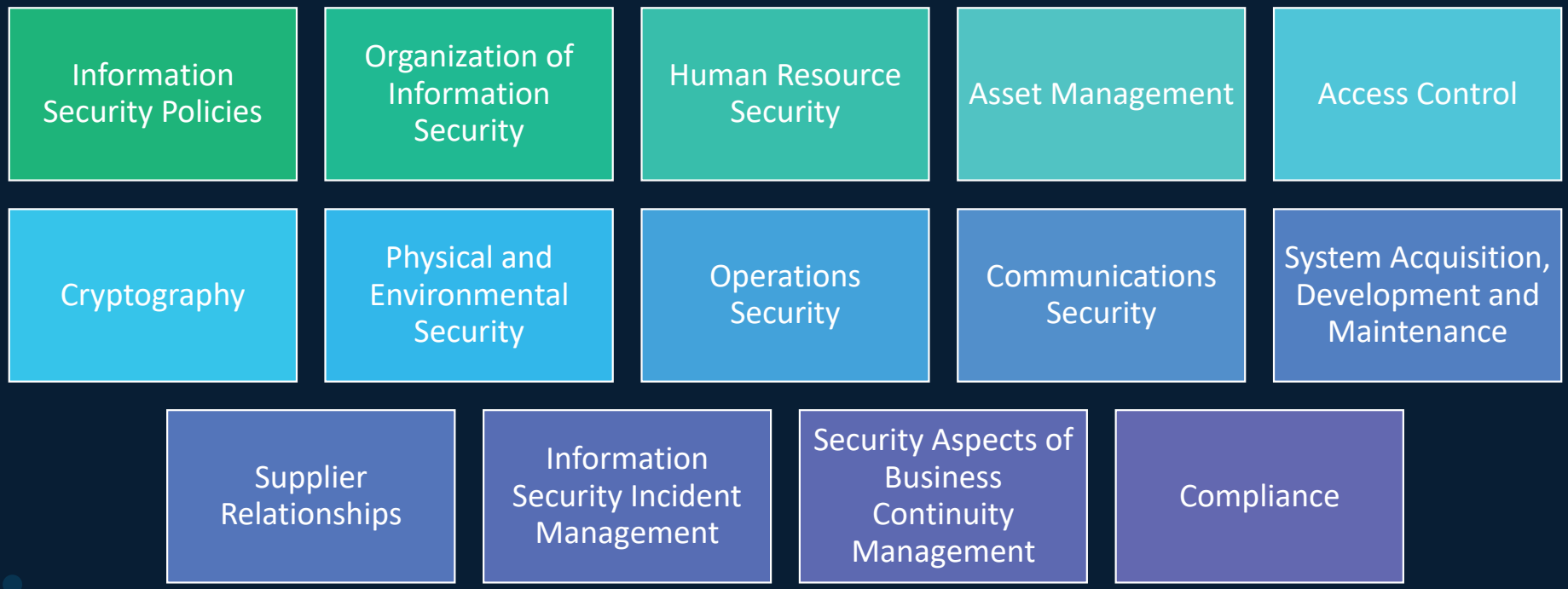
SAS Security and Privacy Standards

SAS Security and Privacy Standards

Security in the Cloud

- The SAS Trust Center provides information related to security, privacy, compliance and quality.
- Security strategies to maintain the confidentiality, integrity and availability of hosted customer data include technical and organizational controls that allow SAS to maintain the following certifications and audit reports:
  - ISO 27001 (including ISO 27017 & ISO 27018)
  - SOC 2/3 Type II
- SAS monitors other external standards, industry and regulatory requirements, such as: HIPAA, HITECH, FISMA, etc.

ISO 27001 Controls



SAS Security and Privacy Standards

Security in the Cloud (continued)

- Annual full-scope network penetration tests performed.
- Defined policies around required security testing for public, internet-facing web services.
- Attack surface monitoring for Internet-facing resources.
- Maintenance of a Security Incident Response Team
  - Consists of cross-divisional members, including Chief Information Security Officer and Chief Privacy Officer
  - Identify/triage/respond to any possible security incidents rapidly
  - Employees trained to report incidents.
  - SIRT Process follows regulatory requirements and best practices for notice to SAS customers
  - Annual Tabletop exercise to test processes

SAS Security and Privacy Standards

Privacy in the Cloud

- SAS' data privacy strategy - use of data by minimum individuals only for the purposes of the services SAS provides.
- Customers define data classification.
- Annual privacy and security training required for all SAS personnel with access to hosting environment. Personnel are trained to handle PHI properly.
- Compliance with applicable regulations, including HIPAA Privacy Rule.
- SIRT team includes Chief Privacy Officer (Legal).
- Privacy Champions in divisions across SAS who are in place to help divisions keep a privacy mindset.

Thank you!

sas.com

Links

Reference Links

- SAS Trust Center
- SAS Security in the Cloud
- SAS Hosted Managed Services Privacy Policy
- https://video.sas.com/detail/video/6053450038001/security-in-the-sas-cloud-%7C-data-security-and-data-privacy

NC HealthConnex
Powering Health Care Outcomes

NORTH CAROLINA HEALTH INFORMATION EXCHANGE AUTHORITY

June 16, 2022
Advisory Board Meeting

Christie Burris
Executive Director

NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

NC HIEA – Privacy & Security

Overview of Topics:

- **Statutory Requirements:**
  - Patient Education & Opt-Out
  - Prohibition on Commercialization of Data
  - Redirecting Patient Requests to Providers
- **Contractual Governance**
  - Vendor Contract Requirements
  - Participation Agreement Terms & Conditions
- **NC HIEA Policies**
  - Privacy & Security
  - User Access
  - Sensitive Data
- **Role of the Participant Account Administrator**
  - User Credentials
  - User Account Audits
- **Continuous Monitoring**
- **Accounting of Disclosures**
- **NC HIEA Workforce Policies**

NC HealthConnex
Powering Health Care Outcomes

State Requirements

- Patient Education & Opt-Out - N.C. Gen. Stat. § 90-414.6
- Prohibition on Commercialization of Data - N.C. Gen. Stat. § 90-414.6
- Redirecting Patient Requests to Providers – N.C. Gen Stat. § 90-414.6

Patient Education & Opt-Out

Participants are responsible for educating their patients about the benefits of NC HealthConnex and their right to opt out.

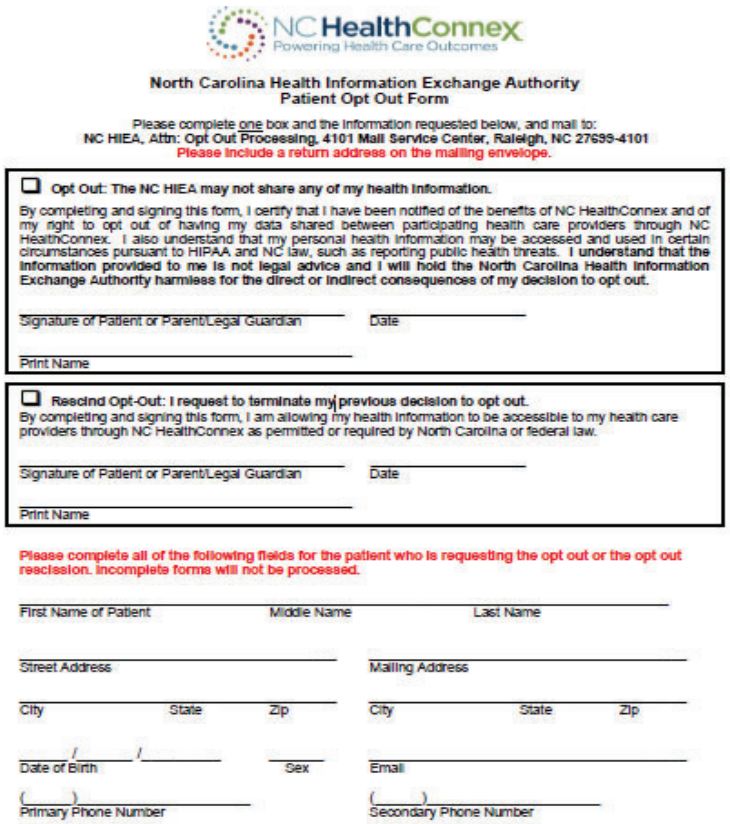
NC HIEA makes available to providers patient education materials in the welcome packet once the Participation Agreement has been executed.

Includes:

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

NC HealthConnex
Powering Health Care Outcomes

Opt Out Process



NC HealthConnex
Powering Health Care Outcomes

North Carolina Health Information Exchange Authority
Patient Opt Out Form

Please complete one box and the information requested below, and mail to:
NC HIEA, Attn: Opt Out Processing, 4101 Mail Service Center, Raleigh, NC 27699-4101
Please include a return address on the mailing envelope.

☐ **Opt Out: The NC HIEA may not share any of my health information.**

By completing and signing this form, I certify that I have been notified of the benefits of NC HealthConnex and of my right to opt out of having my data shared between participating health care providers through NC HealthConnex. I also understand that my personal health information may be accessed and used in certain circumstances pursuant to HIPAA and NC law, such as reporting public health threats. **I understand that the information provided to me is not legal advice and I will hold the North Carolina Health Information Exchange Authority harmless for the direct or indirect consequences of my decision to opt out.**

Signature of Patient or Parent/Legal Guardian _____ Date _____

Print Name _____

☐ **Rescind Opt-Out: I request to terminate my previous decision to opt out.**

By completing and signing this form, I am allowing my health information to be accessible to my health care providers through NC HealthConnex as permitted or required by North Carolina or federal law.

Signature of Patient or Parent/Legal Guardian _____ Date _____

Print Name _____

Please complete all of the following fields for the patient who is requesting the opt out or the opt out rescission. Incomplete forms will not be processed.

First Name of Patient _____ Middle Name _____ Last Name _____

Street Address _____ Mailing Address _____

City _____ State _____ Zip _____ City _____ State _____ Zip _____

___/___/___ Sex _____ Email _____

Date of Birth

(___) _____ (___) _____

Primary Phone Number Secondary Phone Number

- By statute North Carolina is an Opt Out state, which means patients are automatically *Opted In* to the HIE for treatment, payment, operations per HIPAA, unless they exercise their right to Opt Out.
- If a patient chooses to submit an Opt-Out form, all fields must be completed and form is mailed to the NC HIEA Business Office.
- Complete opt out requests are processed within two business days.
- Note: Patient electronic health information is not opted out of public health use cases or per specific state law.

NC HealthConnex
Powering Health Care Outcomes

Adult Opt Out vs Minor Opt Out

Adult Patient Opt Out Model
Once a patient submits a full patient Opt Out, their data is blocked from being shared within NC HealthConnex.

Minor Opt Out Model
Under NC law minor patients are allowed to be treated by a health care provider for certain conditions without needing parent or legal guardian permission.

A minor patient can opt out of sharing specific services identified in statute, including treatments for some contagious diseases, family planning/pregnancy, emotional issues, and drug or alcohol use. This opt out process is encounter based and requires the treating physician to submit the request on behalf of the patient via DSM within two days of the encounter.

NC HealthConnex
Powering Health Care Outcomes

Prohibition on Commercial Uses

What Constitutes Commercialization of Data?

- Propose defining commercial purposes…. *Commercial Purposes are defined as:*
  - *Access, use, redisclosure, and storage of clinical and demographic data sent to or through NC HealthConnex ("HIE data") beyond the purposes of supporting (i) treatment, payment, and health care operations as they are described in HIPAA.; (ii) population health; (iii) government programs; or (iv) academic research;*
  - *Redisclosure or exchange of HIE Data with third-party organizations for the primary purposes of improving business operations, cost-cutting, or profit-seeking, without explicitly stated benefits to patients.*
  - *Sale of HIE Data in exchange for money, other clinical or demographic data, services, and other items of value.*

NC HealthConnex
Powering Health Care Outcomes

Redirecting Patient Requests to Providers

NCSL 2021-26 - § 90-414.6

Section 6 prohibits the NC HIEA from fulfilling requests for electronic health information from an individual, individual's personal representative, or an individual or entity purporting to act on an individual's behalf and requires the Authority to provide educational materials on accessing this information from other sources.

NC HealthConnex
Powering Health Care Outcomes

Information Provided on the Website

For Patients | NC HIEA - Your Choices | NC HIEA –

How to Request Copies of Your Medical Record from Your Provider

Individuals may seek a copy of their medical records directly from the medical provider or providers with whom they have or have had a relationship. Frequently, medical providers include directions on their website to help patients access or request their records. If an individual's medical provider is a full participant in the NC HIEA, they can request that their medical provider also provide a copy of electronic health information that is available to them through NC HealthConnex. Learn more about whether your provider or your provider's practice or organization has executed a full agreement with the NC HIEA here: https://hiea.nc.gov/patients/nc-healthconnex-participant-map.

Additional resources about how to access health records are available online:

"How to Get It" webpage published by the Office of the National Coordinator for Health Information Technology, which is part of the US Department of Health and Human Services (https://www.healthit.gov/how-to-get-your-health-record/get-it/#:~:text=You%20may%20be%20able%20to,mail%20or%20fax%20a%20letter).

"Your Medical Records" webpage published by the Office of Civil Rights in the U.S. Department of Health and Human Services:(https://www.hhs.gov/hipaa/for-individuals/medical-

NC HealthConnex
Powering Health Care Outcomes

Vendor Contract Requirements

Provisions from the NC HIEA's public-private partnership agreement with SAS concerning privacy and security include, among others, the following:

- Business Associate Agreement
- NC Statewide Security Manual and NIST Modernization
- Virus screening; penetration testing & remediation
- No offshore development by SAS employees or contractors; background and security investigations; HIPAA and security training
- Breach notification (24 hours)
- Media sanitization: Standards and processes
- Agreement does not transfer ownership rights
- Incident response plan and disaster recovery plan

NC HealthConnex
Powering Health Care Outcomes

Participation Agreement Key Terms and Conditions

Provisions from the NC HIEA's various participation and submission agreements include the following:

- System Access provisions: requires full participants to (i) implement user access and privacy and security policies; (ii) ensure authorized users and participating entities access and use HIE data per agreement; (iii) validate identities for unique users
- Security
- Incorporation of NC HIEA's Policies and Procedures
- HIEA: Disclosure of Entities, BAs, Approved Third Parties
- Participant Use of Message Content and NC HealthConnex Resources: authorized user with legal authority for a permitted purpose
- Responsibility for "Participating Entities"
- Opt-Out: Patient education obligations
- Compliance with HIPAA regulations and applicable law
- Breach notification

NC HealthConnex
Powering Health Care Outcomes

NC HIEA Policies

NC HealthConnex
Powering Health Care Outcomes

Privacy & Security

NC HealthConnex is a secure, private network

- NC HealthConnex is required to comply with all federal and state privacy and security laws
- Information is always encrypted and sent over a private network
- 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
Powering Health Care Outcomes

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; Access to patient information granted if established treatment relationship with the patient
- Participant Account Administrator (PAA) will be responsible for assigning roles to users; NC HealthConnex Help Desk will provide credentials to these users
- ***PAAs are not authorized to give user credentials to persons or entities that are not Participating Entities**

Privacy & Security

User Access

Sensitive Data

Opt Out

NC HealthConnex
Powering Health Care Outcomes

Sensitive Data

- 42 C.F.R. Part 2 **prohibits** certain health care providers from disclosing data that would identify a patient as having a substance use disorder without patient consent
- HIPAA covered entities are **prohibited** from sharing a patient's psychotherapy notes (See 42 C.F.R. 164.508)

See C.F.R. 2.12(b) and consult with your legal counsel to determine if you are covered by this regulation.

**Participants are prohibited from submitting psychotherapy notes or SUD data covered by 42 C.F.R. Part 2 – compliance with the law*

Privacy & Security

User Access

Sensitive Data

Opt Out

NC HealthConnex
Powering Health Care Outcomes

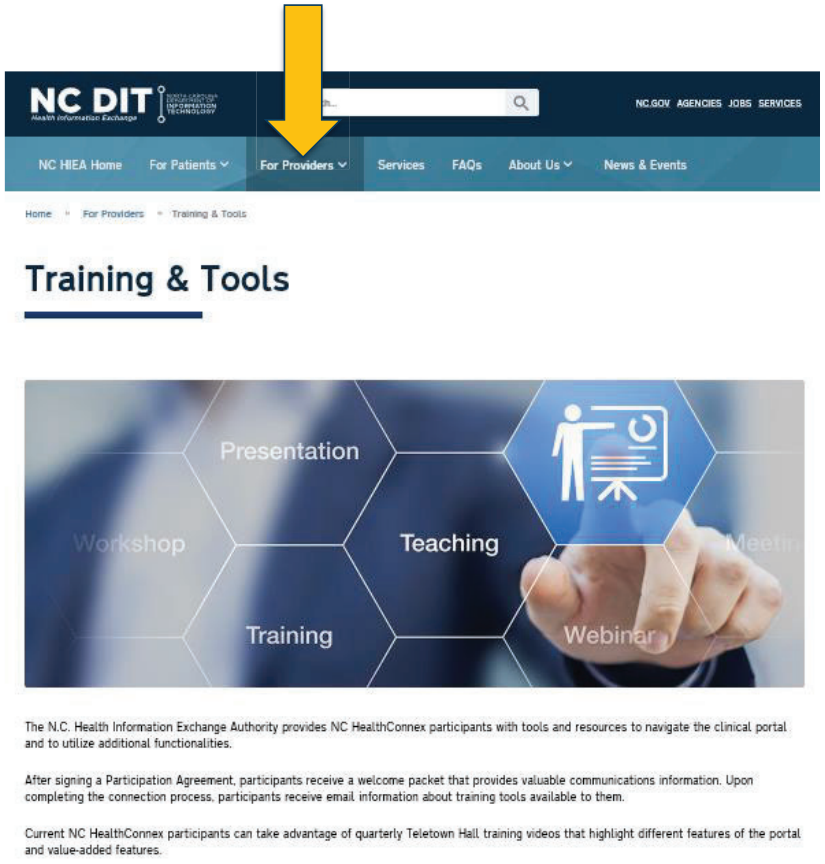
Participant Account Administrator Role and Responsibilities

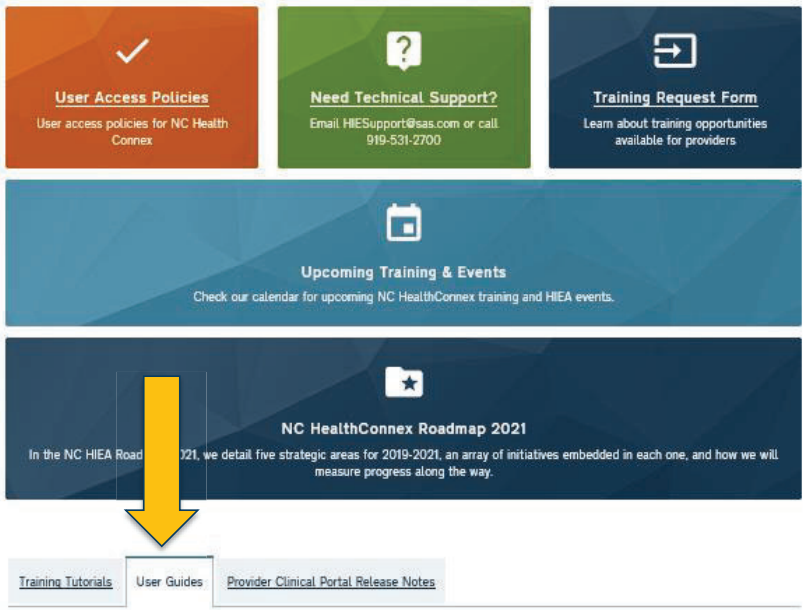
- Serves as the Main Point of Contact for the NC HIEA
- Reviews the Quarterly User Account Audit
  - ✓ Reviews active users, patient searches, and break the seal activity
- Manages the Creation and De-activation of Portal User Accounts
  - ✓ PA manages credentials via a User Management Spreadsheet in the portal

NC HealthConnex
Powering Health Care Outcomes

PAA User Guide

All of this information can be found in more detail in the PAA User Guide.





NC HealthConnex
Powering Health Care Outcomes

Audits/Disclosures

Continuous Monitoring - The Continuous Monitoring project provides a set of SAS Visual Analytic reports that can be accessed at any time, will give a visual representation of usage (patient search and break the seal), and allow analysis of usage by NC HIEA designated team members.

Accounting of Disclosures – Patients are able to request an accounting of disclosures from the NC HIEA. These requests are processed by a member of the NC HIEA provider relations team and sent to a designated privacy officer at SAS. Your Choices | NC HIEA

Data Disclosures to Approved Third Parties – Per HIPAA, the NC HIEA provides public notice on the website of approved third-party disclosures of HIE data. NC HIEA Data Disclosures | NC HIEA

NC HealthConnex
Powering Health Care Outcomes

NC HIEA Workforce Policies/Training

Policies:

Background checks, access to sensitive data SBI fingerprint checks, NDAs
State and Department access and security policies

Training:

DIT-assigned Security Training
Annual HIPAA training
Information Blocking educational training

Continuous Improvement:

Industry best practices, professional development
Civitas Networks for Health
Dedicated Compliance Officer

NC HealthConnex
Powering Health Care Outcomes

Operations Update

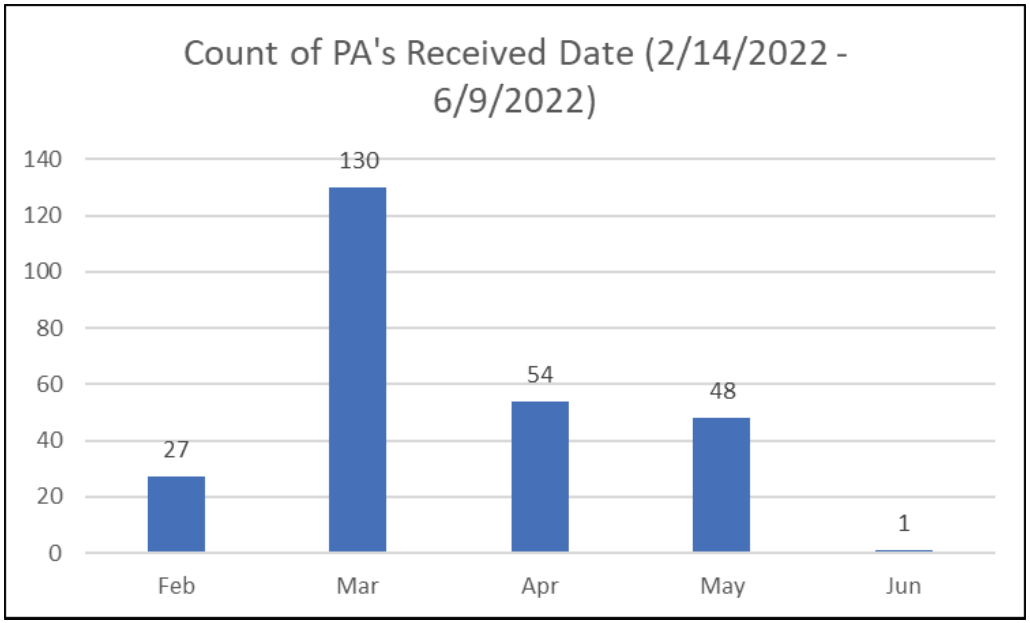
NC HealthConnex
Powering Health Care Outcomes

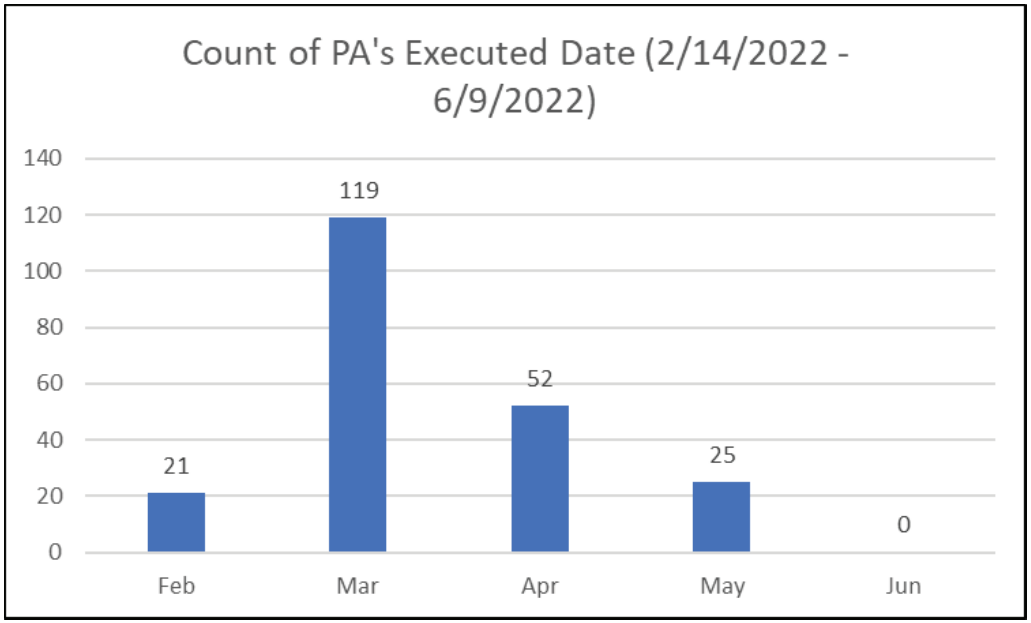
Outreach and Provider Relations Updates

- Of the 109 Participation Agreements (PAs) received between 2/14 and 3/17 there were a total of 239 associated providers.
- Between the period of 2/14 and 6/9:
  - PAs Received: 260
  - PAs Executed: 127
  - Most common provider type: behavior health
  - Most common facility type: ambulatory/outpatient clinic

NC HealthConnex
Powering Health Care Outcomes

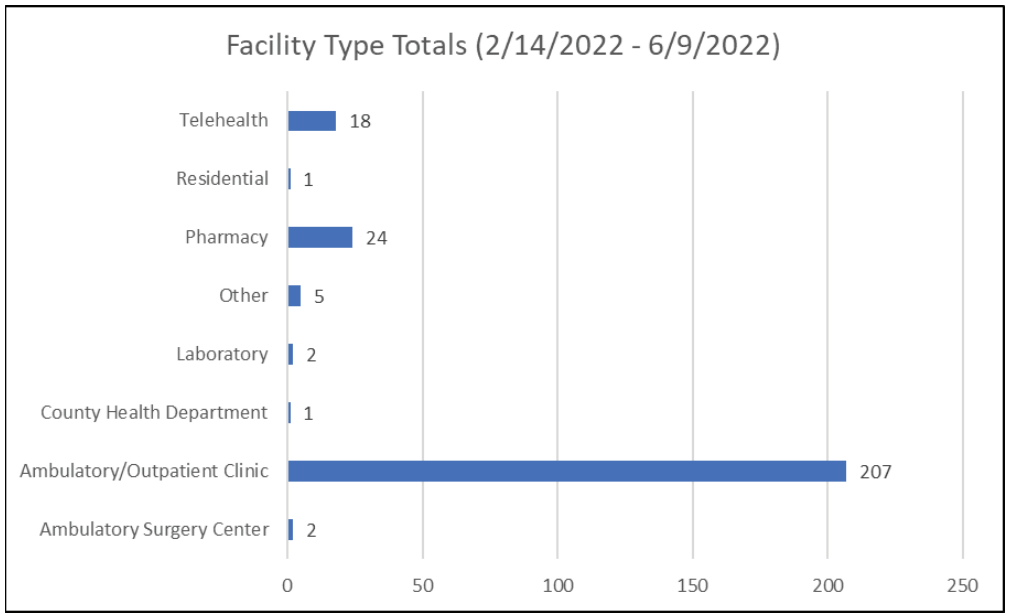
PAs Received & Executed

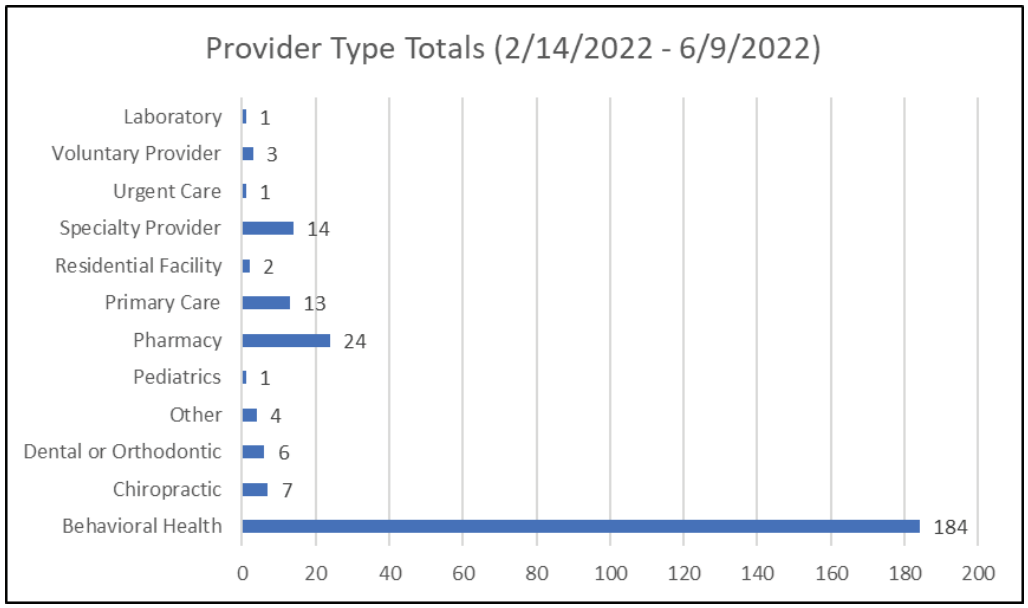




NC HealthConnex
Powering Health Care Outcomes

Provider & Facility Types

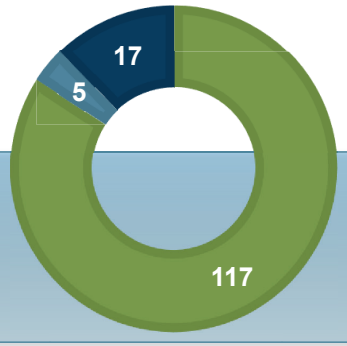




Enrollment in Services

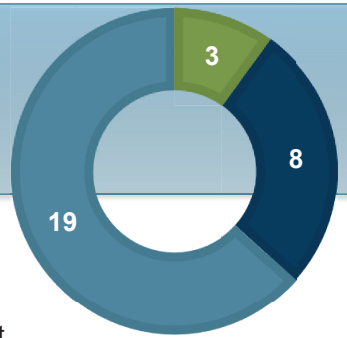
(as of June 2022)

NC*Notify



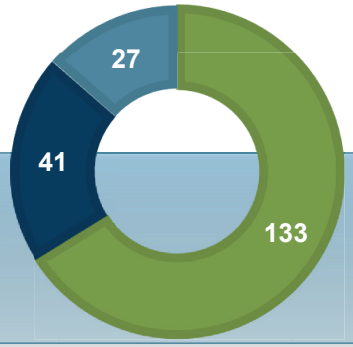
- 117 Integrations Live (661 Participants)
- 17 Integrations in Development
- 5 Integrations Enrolled

NCIR



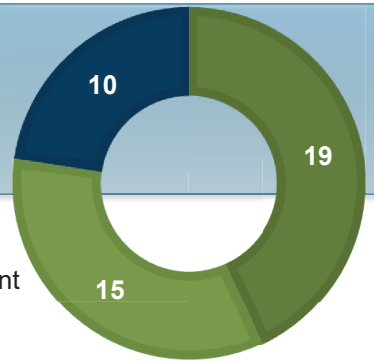
- 3 EHRs Live (163 Participants)
- 8 EHRs in Development
- 19 EHRs Enrolled

CVMS



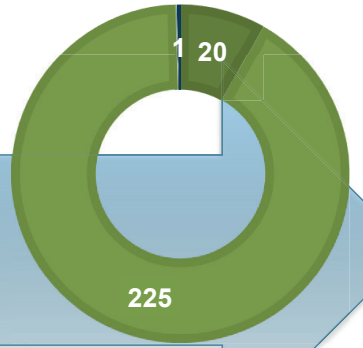
- 133 Participants Live
- 41 Participants in Development
- 27 Participants Enrolled

ELR



- 34 Live: 19 full ELR feeds Live; 15 COVID-only
- 10 full ELR feeds in Development

DSM



- 245 Domains Live: 20 XDR, 225 Webmail
- 1 Participants in Development

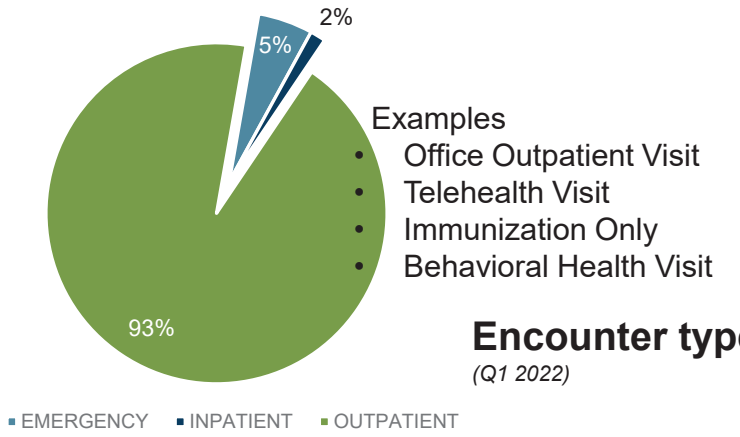
NC HealthConnex
Powering Health Care Outcomes

Clinical Data Content

- **Encounters: 356M**
- **Diagnosis: 747M**
- **Medications: 394M**
- **Lab Results: 301M**
- **Immunizations: 75M**
- **Allergy: 21M**
- **Procedures: 227M**
- **Vitals: 556M**

Description	Clinical concepts represented in Patient records Distribution of clinical encounters by Encounter Type – Inpatient, ED, Other
Strategy	GROWTH
How to Use	Describe the breadth of data available to stakeholders

Clinical Data Volume
(as of May 2022)



Examples
- Office Outpatient Visit
- Telehealth Visit
- Immunization Only
- Behavioral Health Visit

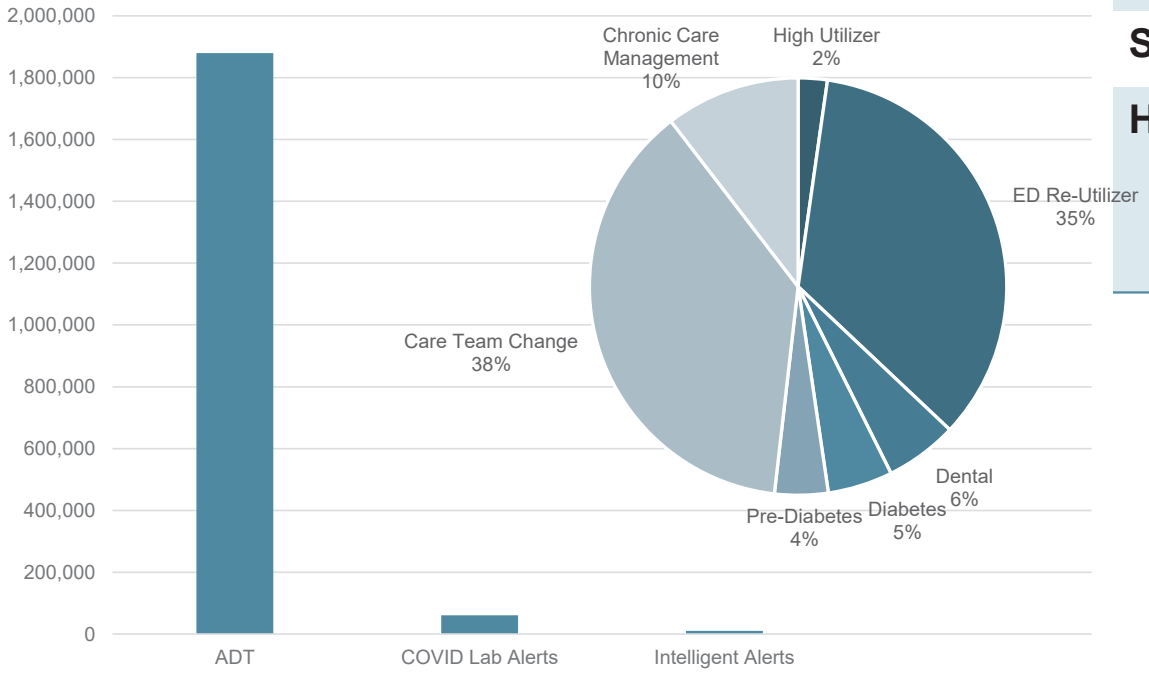
Encounter types captured in Patient records
(Q1 2022)

NC HealthConnex
Powering Health Care Outcomes

NC*Notify Utilization

Event Notification Alerts

(April 2022)

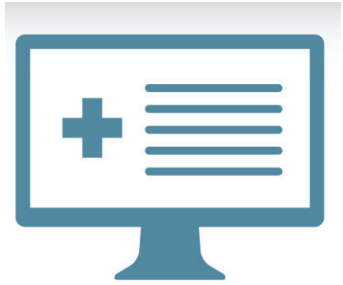


Description	Distribution of Event Notification Alert Types
Strategy	UTILIZATION, IMPACT
How to Use	Understand how NC HealthConnex data can be used to impact outcomes with the NC*Notify service.

NC Notify
Event Notifications Powered by NC HealthConnex

NC HealthConnex
Powering Health Care Outcomes

2nd & 3rd Quarter 2022 Activities:



- Staffing – Newly hired Compliance Officer, Outreach Specialist, Data Quality Analyst, Applications Systems Specialist; additional analyst hires underway
- Data Connections
- CCHIE joint outreach
- Data Retention Planning
- Data Quality Dashboard Enhancements; Data Integrity Audits
- Stroke Registry in Production; Phase 2 to begin
- CVMS, NCIR & IDDHUB
- Use Case Work Group
- Pharmacy Connection Pilot
- State Lab Integration & Electronic Order and Results Delivery

NC HealthConnex
Powering Health Care Outcomes

Use Case Workgroup (UCW) Update

- **UCW Sub-committee kicked off 6/8/2022**
- **Reviewed UCW workflow and expectations**
- **One use case was unanimously voted yes**
- **Follow up meeting scheduled to review UCW Charter**

NC HealthConnex
Powering Health Care Outcomes

Use Case Workgroup (UCW) Update

ACURE4Moms
Accountability for Care through Undoing Racism & Equity

ACURE4Moms Study Aims & Outcomes

Aim 1: Compare proportion of Black women who deliver a **low birthweight** baby between Arms (**Primary Outcome).**

- Secondary: **Maternal Morbidity and Mortality**

Aim 2: Compare **# ED visits and hospitalizations** during pregnancy and up to 1 year after delivery between Arms.

Aim 3: Explore trends in **self-reported racism** during pregnancy and up to 4 months after delivery between Arms through patient surveys.

Four arm cluster RCT of 40 practices:

1) Standard Care Management (**Control Arm**)→ 10 practices
2) Data Interventions-Only (**Data Arm**)→ 10 practices
3) Community-Based Doula Support-Only (**Doula Arm**)→ 10 practices
4) Data Interventions + Doula Support (**Data+Doula Arm)→** 10 practices

- Looking for HIE support because practices are spread across the state
- Complicated patients, e.g. uncontrolled diabetes or hypertension, will often get care at multiple practices
- Hospital birth data will be essential
- A successful fetal maternal dashboard could be used as a care improvement utility throughout the state

NC HealthConnex
Powering Health Care Outcomes

Legislative Update

NC HealthConnex
Powering Health Care Outcomes

Legislative Updates

- **March 23** - NC HIEA Report Submitted to HHS JLOC
- **May 11** – Governor Cooper released his budget proposal - Building on Success
  - $16M non-recurring funds included for the HIE for data connections and additional resources for outreach/education
- **May 18** – Short Session Convened
- **NCDIT Short Session Activities:**
  - Engaged in conversations with select House and Senate staffers on DIT's comprehensive enforcement framework for the HIE Act gauging interest in bill introduction
  - Delivered one-pager and targeted legislative proposal to suspend the ' HIE Mandate' to 25+ legislators (House and Senate) and to the Governor's office urging action this session to provide relief from the "condition of payment" language in the HIE Act until an actor has been named to lead enforcement.

NC HealthConnex
Powering Health Care Outcomes

Questions?

NC HealthConnex
Powering Health Care Outcomes