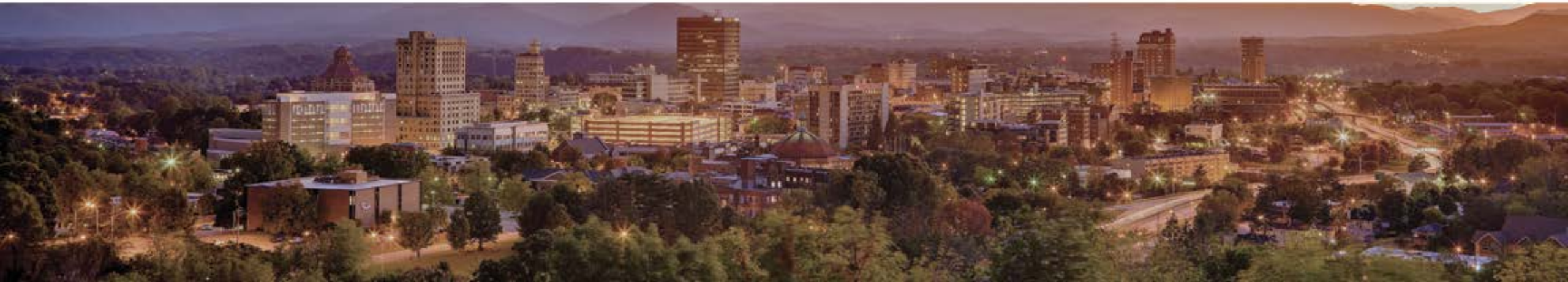
NC DIT

NORTH CAROLINA
DEPARTMENT OF
INFORMATION
TECHNOLOGY

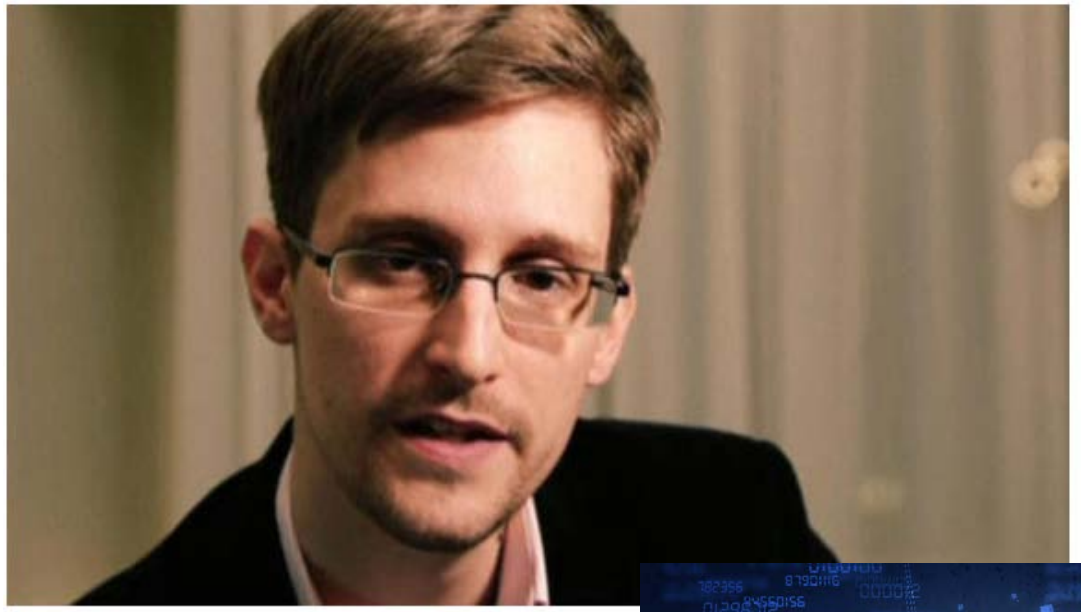
Insider Threats

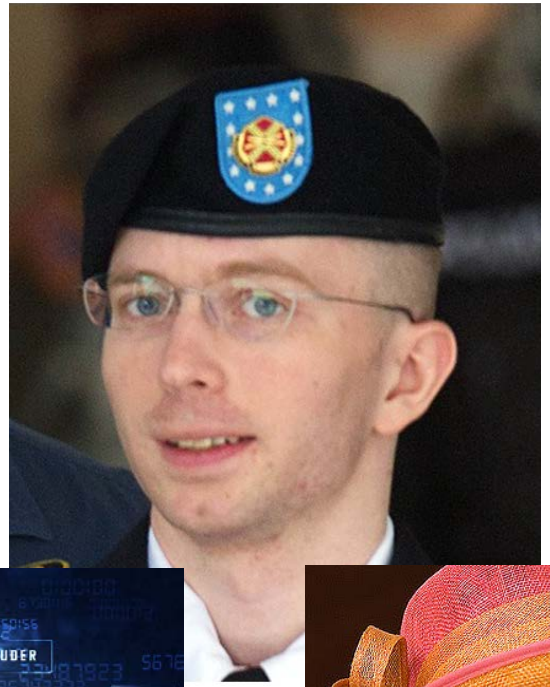
Maria Thompson
State Chief Information Risk Officer

February 1, 2018



Who is an insider?





Who is an insider?

Carnegie Mellon CERT definition of insider:

- Someone who has authorized access to an organization's facilities, data, information systems, and networks (*e.g.*, former or current employee, trusted business partner, contractor, maintenance personnel) who meets the following criteria:
  - ✓ Has or had authorized access to an organization's network, system, or data
  - ✓ Has intentionally exceeded or used that access in a manner that negatively affected confidentiality, integrity, or availability of the organization's information or information systems

Insider threat statistics

- 60-70 percent of attacks came from insider.
- Insider threats can be intentional (*i.e.*, malicious) or unintentional
- Gartner study:
  - 62 percent of insider incidents involved employees looking to establish a second stream of income off of employers' sensitive data
  - 29 percent stole information on the way out the door to help future endeavors
  - 9 percent were saboteurs
- Ponemon Institute study: 43 percent of businesses need a month or longer to detect employee's accessing unauthorized files

What is an insider threat?
What are insider threat damages?

Insider threat actions can:

- intentionally or unintentionally compromise an organization's security
- affect the confidentiality, integrity, and availability of an organization's data, information systems, and networks; and
- degrade an organization's ability to accomplish mission or business functions; and also affect the safety of the organization's workforce

Insider threat damages include, but are not limited to:

- espionage
- criminal enterprise
- unauthorized disclosure of information (sensitive information, intellectual property, trade secrets)
- information technology sabotage
- violation of federal or state laws
- other activity resulting in the loss or degradation of an organization resources or capabilities.

Characteristics of potential insider threats: personal indicators

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Depression	High	Low	Low	Medium	High
Financial obligations	Low	High	High	Medium	Low
Address change (moving)	Low	High	High	Medium	Medium
Death among family or friends	Medium	Medium	Low	Medium	High
Feelings of inadequacy	High	Medium	Low	High	Medium
Break-up or divorce	Medium	Low	Low	Medium	High
Impending termination of contract	High	High	Low	Medium	Medium

** Identified in a study by U.S. CERT as potential indicators of insider action.*

Behavioral indicators of malicious insider threat activity

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Unwillingness to comply with established rules and procedures	High	Medium	Low	Medium	High
Repeated breach of procedures	Medium	High	High	High	High
Excessive or unexplained use of data copy equipment (fax, copy, camera)	Low	High	Low	High	High
Excessive volunteering which would elevate access to sensitive data	Low	High	High	High	Medium
Excessive overtime work	Low	High	High	High	Low
Bringing personal equipment to high-security areas	Low	High	Medium	High	High
Carelessness	Low	Low	Low	Low	High
Concerning statements, jokes, or bragging	Medium	Low	Low	Medium	High
Impulsiveness	Medium	Medium	Low	Low	High
Poor social interaction	High	Medium	Low	Low	Medium
Aggression	High	Medium	Low	Low	Medium

** Empirical data provided by CERT shows that theft is generally conducted by conducted by technical personnel, whereas fraud is carried out by non-technical personnel.*

How can we prevent or deter and detect insider threats?

- Restrict remote access
- Authorize users based on least access privilege and conduct periodic audits to detect inappropriate access or access from previous job functions that should be removed
- Collect information for all remote logins
- Use centralized logging to detect data exfiltration near insider termination
- Monitor failed remote logins
- Educate employees through training and awareness
- Audit:
  - Password sharing
    Entrance barriers
  - Sensitive information
  - Employee attitude

How can we prevent or deter and detect insider threats?

- Provide avenues for employees to vent concerns and frustrations to mitigate insider threat motivated by disgruntlement
- Implement employee recognition programs that offer public praise to mitigate insider threat motivated by ego

Security technologies and tactics to detect and prevent insider attacks	
Data and file encryption	Enterprise identity and access management
Data access monitoring	Data access control
SIEM or other log analysis	Intrusion detection and prevention systems
Data loss prevention	Enterprise digital rights management solutions
Data redaction	

Insider threat reporting

What should a State employee do if he or she suspects insider threat activity?

- Do not attempt to investigate
- Report suspicion to human resources department
- If an IT-related incident → report anomalous network activities to Enterprise Security Risk Management Office (ESRMO) through incident reporting portal
  https://it.nc.gov/cybersecurity-situation-report

Questions?

NC HealthConnex
Powering Health Care Outcomes

NORTH CAROLINA HEALTH INFORMATION EXCHANGE AUTHORITY

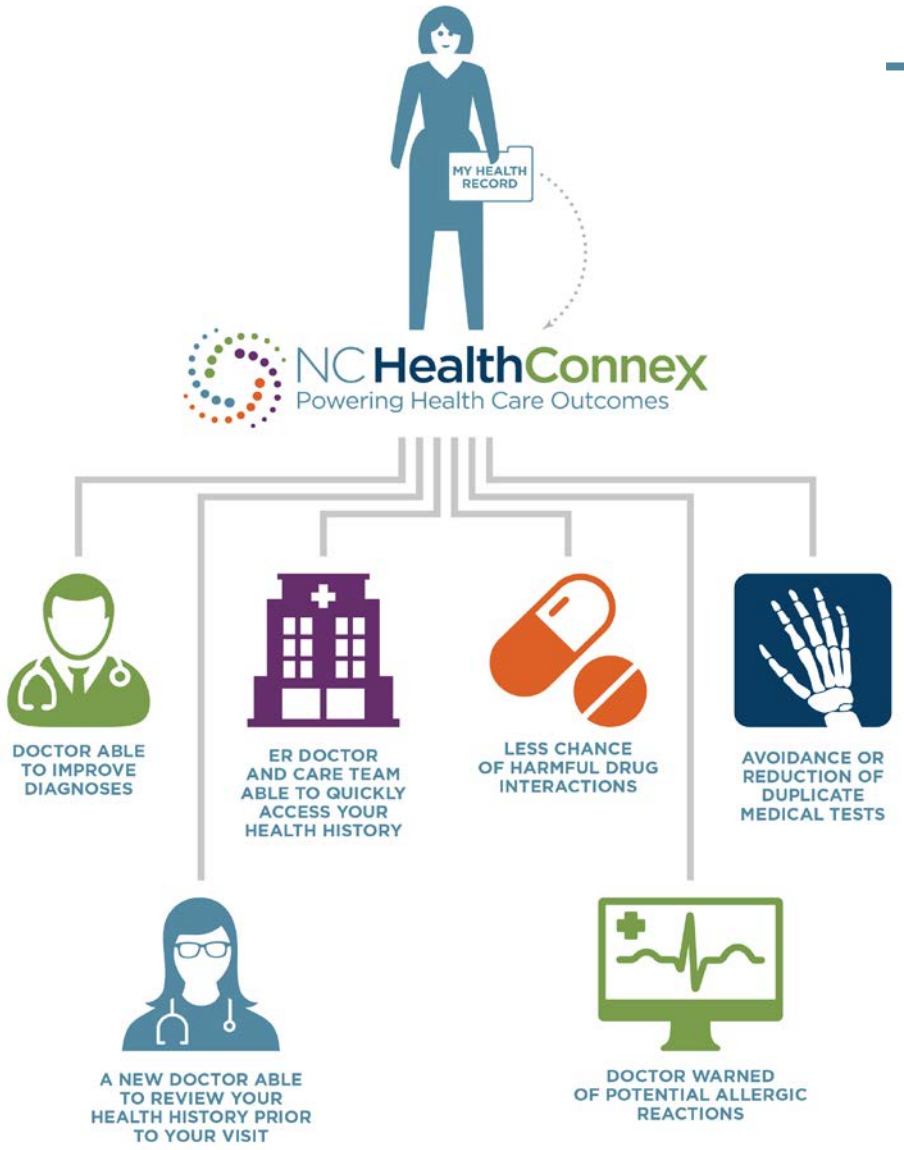
Christie Burris, HIEA Executive Director
Department of Information Technology

Who is the North Carolina Health Information Exchange Authority?

- The North Carolina General Assembly created the North Carolina Health Information Exchange Authority (NC HIEA) in 2015 to facilitate the creation of a modernized HIE to better serve North Carolina's health care providers and their patients. *(NCGS 90-414.7)*
- Housed within the Department of Information Technology's Government Data Analytics Center (GDAC).
- Our technology partner is SAS Institute.
- Eleven-member Advisory Board, appointed by the General Assembly and made up of various IT and health care representatives that include the Secretary of Department Health and Human Services, Secretary of Department of Information Technology and the Government Data Analytics Center Director.

NC HealthConnex
Powering Health Care Outcomes

What is NC HealthConnex?



- North Carolina's state-designated Health Information Exchange.
- A tool to facilitate conversations between all health care provider types across the state to break down the silos between existing networks.
- Enables participating providers to access their patients' comprehensive records across multiple providers, as well as review labs, diagnostics, history, allergies, medications and more.

NC HealthConnex
Powering Health Care Outcomes

Legislative Requirements

- Feasibility study underway with target completion date end of February/early March (NCSL 2015-241 as amended by NCSL 2017-57, Section 11A.5.(h))
- Extension process (NCSL 2015-241 as amended by NCSL 2017-57, Section 11A.5.(b))
- Connection timelines (NCSL 2015-241 as amended by NCSL 2017-57, Section 11A.5.(a))

NC HealthConnex
Powering Health Care Outcomes

Feasibility Study

Statute asks the agencies to examine:

(1) The availability of **connection, exchange, and data submission standards established by the Office of the National Coordinator** for Information Technology within the U.S. Department of Health and Human Services.

(2) The **adoption of national standards** for the connection, exchange, and data submission standards by provider type.

(3) **Cost estimates by provider type to connect** and submit data to the HIE and any **availability of federal or State funds** to meet connection or submission requirements.

(4) Data captured in the treatment of patients, segmented by provider type.

(5) Activity of **other states and payor plans** with respect to the establishment of an HIE Network.

(6) **Alternatives to the connection and submission** of demographic, clinical, encounter, and claims data through the HIE Network.

NC HealthConnex
Powering Health Care Outcomes

Extension Process

The process for granting an extension of time must include:

- a presentation by the provider or entity to both agencies on the expected time line for connecting to NC HealthConnex
- neither agency shall grant an extension of time to any provider or entity that fails to provide this information or that would result in the provider or entity connecting to NC HealthConnex later than June 1, 2020.
- both agencies will consult on formal requests for extension and decide upon a request within 30 days after receiving a request for an extension.

NC HealthConnex
Powering Health Care Outcomes

Current State

	1200+ Live
30 +	County Health Departments and Federally Qualified Health Centers
20+	Hospitals & Health Systems
200+	Primary Care Providers
400+	Ambulatory Sites, including specialty providers
	300+ in queue for onboarding

- **To date, all participants are sending all patient data**
- **Over 4 million unique patient records as of 11/30/17**
- **Numerous EHR vendor, cloud-based integrations in flight**

NC HealthConnex
Powering Health Care Outcomes

Value-Added Features

Communicate | Direct Secure Messaging Accounts provided by NC HealthConnex allow connection with other providers by sending and receiving secure, encrypted messages.

Connect | Access to DSM Provider Directory with over 16,000 (and growing) secure messaging addresses of health care providers.

Contribute | Public Health Reporting via Registries – Diabetes Declaration of Readiness, December 1, 2017.

Convey | Utilize the clinical data an organization captures with timely analytics and reporting about patient population via Clinical Notifications.

NC HealthConnex
Powering Health Care Outcomes

Key Operational Activities

- Budget & Staffing
- Federal Grant - $27M
- HIEA Work Groups
- EHR Vendor Outreach
- DHHS Roadmap to Strategically Align HIEA with DHHS Programs
- Participation Agreement
- Data Connections – Georgia (GaHIE) and USDVA (VHIE)

NC HealthConnex
Powering Health Care Outcomes

Future State…

- Approx. 98% of North Carolina's health care providers will be connected to NC HealthConnex by June 1, 2020
    - o includes labs, pharmacy, behavioral health, transportation, etc.
- LME/MCOs as well as PHPs required to connect and submit encounter claims data by June 1, 2020
- Project that we will have visibility into +/- 90% of citizens receiving treatment in North Carolina (Current population est. @ 10M; UNC Carolina Population Center)
- Will have access to data from other states through connections to national health care data networks (Migration accounted for 72% of the state's growth last year; UNC Carolina Population Center)

NC HealthConnex
Powering Health Care Outcomes

Questions?

Please do not hesitate to contact DIT legislative liaison Nate Denny at nate.denny@nc.gov.

NC HealthConnex
Powering Health Care Outcomes