Georgia Department of Community Health

Balancing Privacy and Data Access During a Crisis

Annika Jones

DCH OIT – Health Information Technology

March 25, 2020

Georgia Department of Community Health

Mission:

The mission of the Department of Community Health is to provide access to affordable, quality health care to Georgians through effective planning, purchasing, and oversight.

Georgia Department of Community Health

Partnering for Success

The Department of Community Health and the Georgia Health Information Network (GaHIN) work closely to ensure that providers and caregivers can access patient health information at the point of care to optimize outcomes and reduce costs.

GAMMIS Online User Training

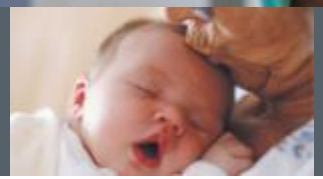
We have developed training on the simple steps needed to sign up to access GaHIN as well as how to navigate within the electronic record

- Part 1 – accepting the Terms and Conditions required prior to access
- Part 2 – primary functions and navigation within the GAMMIS Clinical Viewer

https://ibmwh.adobeconnect.com/gammis-training

You must have an active, authorized GAMMIS login and accept the terms and conditions (one time) prior to gaining access to GaHIN data

Note: Your facility may block streaming content on the internet, including content streaming from the truvenhealth.com domain. In this case, you will need to contact your IT Team for information on how to access streaming content.



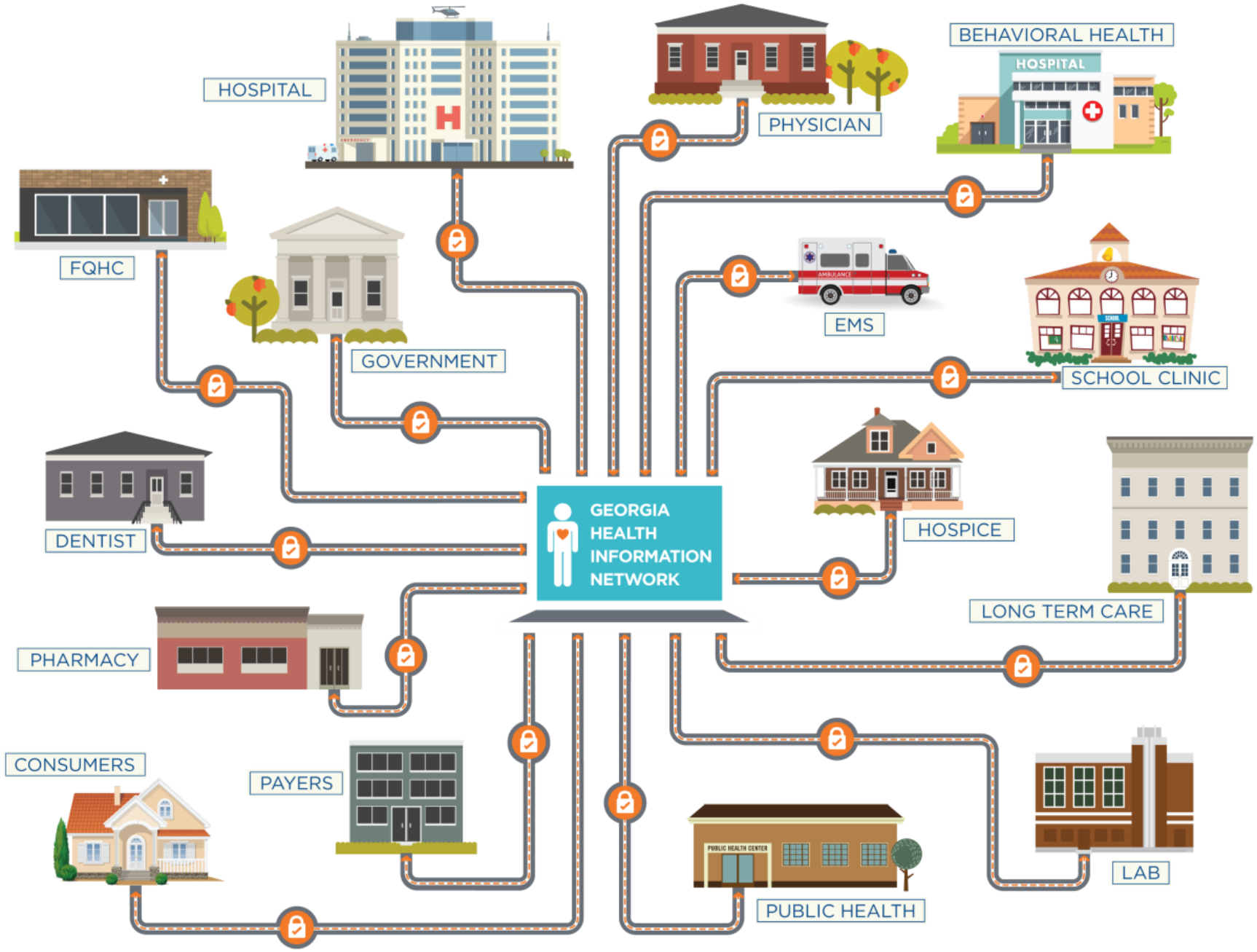
GaHIN – Georgia’s Statewide Health Information Exchange

Georgia Health Information Network (GaHIN)

GaHIN is Georgia's state-designated Health Information Exchange (HIE)

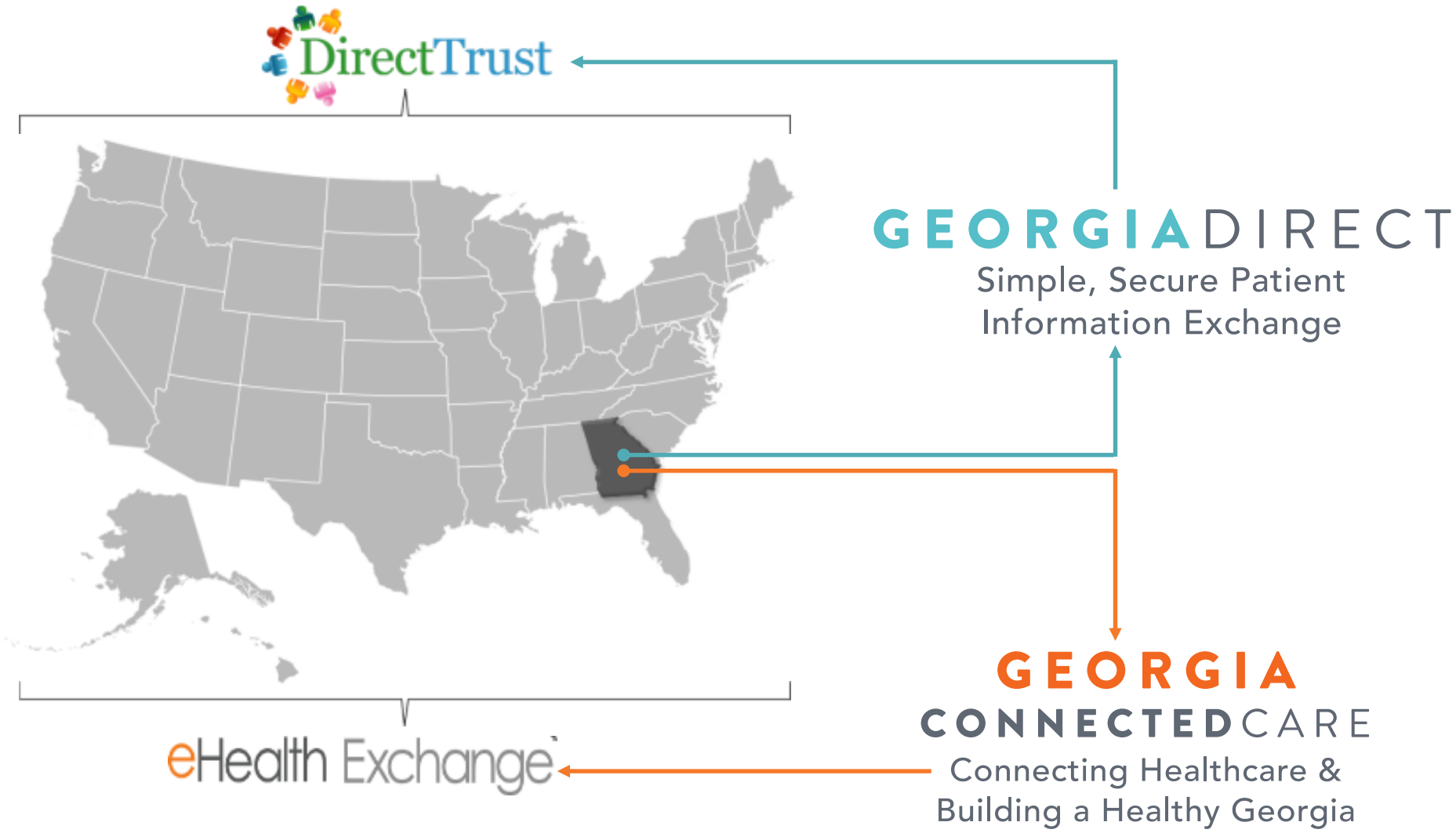
Dedicated to creating a healthier Georgia through the use and exchange of electronic health information

- Advance patient-centered healthcare
- Increase efficiency
- Improve the health of the state's entire population



Creating a Statewide Electronic Network

GaHIN Products and Services



Connecting Georgia

GEORGIADIRECT

Basic Data Exchange

Free email messaging service to securely send patient health information to other authorized healthcare professionals

2019 Totals

- 1,108,303 send & receive transactions
  - 2018 – 747,960 Direct transactions
- 6,445 registered providers
- 356 member organizations

DirectTrust

Connecting Georgia

GEORGIA CONNECTEDCARE

Robust Integrated Patient Search (Query)

Providers can use their EHR to quickly access patient health data from hospitals, physician practices, state health systems and much more

2019 Totals

- ~14,641 connected providers
- 3,885,730 queries
  - 2018 – 2,388,290 queries
- 36,513,390 MPI records

eHealth Exchange™

Connected Organizations

GEORGIA CONNECTEDCARE

State Agencies

- GA Medicaid/Department of Community Health (DCH)
- GA Department of Public Health (DPH)
- GA Division of Families and Children Services (DFCS)
- GA Department of Juvenile Justice (DJJ)
- GA Department of Behavioral Health and Developmental Disabilities (DBHDD)

Health Systems/Hospitals

- Children's Healthcare of Atlanta (Epic)
- Emory Healthcare (Cerner)
- Grady Health System (Epic)
- Gwinnett Health System (RelayHealth)
- WellStar Health System (Epic)

Regional HIEs

- GRAChIE/Chatham HealthLink (Cerner)
- Health*e*Connection (Cerner)
- HealtHIE Georgia (Azalea)
- HI-BRIDGE HIE (formerly Georgia Health Connect)

Care Management Organizations

- Amerigroup (with IHE)
- CareSource
- Peach State
- WellCare

Specialty Connections

- Atlanta Gastroenterology Associates (Greenway)
- Georgia Partnership for Telehealth (Azalea)

National Exchange

- Veterans Health Administration
- Department of Defense
- DaVita Healthcare Partners
- Alabama (AOHR)
- East Tennessee HIE (etHIN)
- South Carolina HIE (SCHIEx)
- North Carolina HIE (NCHIEA)

Balancing Privacy and Data Access During a Crisis

Michele Madison, Partner, Morris, Manning & Martin LLP

Michele Person Madison is a Partner in the Healthcare Practice, where she provides general legal advice to health systems in various regulatory and business matters.

Ms. Madison is highly experienced in managing legal issues arising in hospitals, physician offices or integrated health systems including employment, investigations, risk management assessment and corporation management, and she provides legal education for health systems' medical staff, management team and employees in these areas.

She often facilitates and manages implementation of compliance plans for HIPAA privacy and security regulations, drafts and completes Certificate of Need applications and facilitates regulatory compliance, and provides oversight and guidance regarding medical staff governance and credentialing issues.

She is a member of the firm's COVID-19 task force.

Balancing Privacy and Data Access During a Crisis

Michele Madison
mmadison@mmmlaw.com
March 25, 2020

General Rule on Disclosures and Obligations

Privacy Rule: Covered Entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures.

Security Rule: Covered Entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information.

General Rule on Disclosures

Covered Entities (Healthcare Provider, Clearinghouse and Health Plans) cannot disclose protected health information (other than for TPO) without the patient's consent or in limited circumstances when there is a crisis.

Risk in a Crisis…..

- ***Press Releases***
- ***Employee Disclosures in the Public***
- ***Unauthorized access to clinical records by employees***
- ***Press Inquiries***

Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification

Unless an exception applies, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, may not be done without the patient's written authorization.

No patient objection and you get a request BY NAME, the Covered Entity may release facility directory information and may provide basic information about the patient's condition in general terms (i.e. stable, critical).

Permitted Uses and Disclosures

Treatment: Healthcare providers may release the information for treatment purposes without an authorization.

Public Health Purposes: Disclosure is permitted for the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information that is necessary to carry out their public health mission.

Public Health Authority

To a Public Health Authority:

A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency See 45 CFR §§ 164.501 and 164.512(b)(1)(i)

Mandatory reporting to the CDC and Department of Public Health

OCGA Section 31-12-2(b).

To a foreign government agency at direction of public health authority .

Public Health and Safety

To persons at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations. See 45 CFR 164.512(b)(1)(iv).

Georgia laws permit DPH to notify a person who may have been exposed to a disease or may be at risk of contracting or spreading a disease or condition.

Disclosures to Family, Friends, and Others Involved in an Individual's Care and for Notification

Covered Entity may share information with a patient's family members, relatives, friends, or other persons identified by the patient as involved in the patient's care.

Covered Entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death. This may include, where necessary to notify family members and others, the police, the press, or the public at large. See 45 CFR 164.510(b).

Disclosures to Prevent or Lessen a Serious and Imminent Threat

Providers may disclose a patient's health information to anyone who is in a position to prevent or lesson the serious and imminent threat, including family, friends, caregivers, and law enforcement without a patient's permission.

This disclosure is expressly subject to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety. See 45 CFR 164.512(j).

Minimum Necessary

ALL disclosures to third parties,
including the public health authorities
should be the
minimum necessary information
to serve the purpose of the disclosure.

HIPAA Privacy Waiver

For 72 hours after a Hospital implements its Disaster Protocol; there is a Waiver of the following obligations:

- the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care. See 45 CFR 164.510(b).
- the requirement to honor a request to opt out of the facility directory. See 45 CFR 164.510(a).
- the requirement to distribute a notice of privacy practices. See 45 CFR 164.520.
- the patient's right to request privacy restrictions. See 45 CFR 164.522(a).
- the patient's right to request confidential communications. See 45 CFR 164.522(b).

Security Considerations

Teleworking—

1. Secure Portal Entry
2. Training
3. No Downloading of information
4. Confidentiality Requirements

Workstation Use (Policy from Physical Safeguards)

Encrypted Laptops

Additional Training on HIPAA Privacy and Security Restrictions

Administrative Safeguards

Security Management Process	**§ 164.308(a)(1)**	**Security Policy**
Assigned Security Responsibility	§ 164.308(a)(2)	**Cyber Security Officer**
Workforce Security	§ 164.308(a)(3)	**Security Policy**
Information Access Management	§ 164.308(a)(4)	**Security Policy**
Security Awareness and Training	§ 164.308(a)(5)	**Training of Employees Orientation and Ongoing Education**
Security Incident Procedures	§ 164.308(a)(6)	**Security Policy**
Contingency Plan	§ 164.308(a)(7)	**Security Policy**
Evaluation	**§ 164.308(a)(8)**	**Security Policy**

Physical Safeguards

Workstation Use	**§ 164.310(b)**	**Security Policy**
Workstation Security	§ 164.310(c)	**Security Policy**
Device and Media Controls	**§ 164.310(d)(1)**	**Security Policy**

Technical Safeguards

Access Control	**§ 164.312(a)(1)**	**Security Policy**
Auto Controls	§ 164.312(b)	**Security Policy**
Integrity	§ 164.312(c)(1)	**Security Policy**
Person or Entity Authentication	§ 164.312(d)	**Security Policy**
Transmission Security	**§ 164.312(e)(1)**	**Security Policy**

Telemedicine Waiver

Office of Civil Rights ("OCR") will waive penalties for HIPAA violations against healthcare providers who serve patients in good faith through the use of audio or video communication technology during the COVID-19 nationwide public health emergency.

1. **Non-public facing** remote communication product that is available to communicate with patients.
2. It can be used for any reason, not just for the diagnosis and treatment of COVID-19.

Examples of non-public facing technology:

- Apple FaceTime,
- Facebook Messenger
- video chat,
- Google Hangouts video, or
- Skype.

Secure Telemedicine Transmissions

Covered health care providers that seek additional privacy protections for telehealth while using video communication products should provide such services through technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products.

OCR is not enforcing the penalties if the healthcare provider does not have a business associate agreement.

Disclaimer

The materials and information presented and contained within this document are provided by MMM as general information only, and do not, and are not intended to constitute legal advice.

Any opinions expressed within this document are solely the opinion of the individual author(s) and may not reflect the opinions of MMM, individual attorneys, or personnel, or the opinions of MMM clients.

The materials and information are for the sole use of their recipient and should not be distributed or repurposed without the approval of the individual author(s) and Morris, Manning & Martin LLP.

This document is Copyright ©2020 Morris, Manning & Martin, LLP. All Rights Reserved worldwide.

QUESTIONS??

Georgia Health Information Network

Please participate in the brief survey following this webinar.

Georgia Department of Community Health

Thank you!