DEPARTMENT OF HEALTH AND HUMAN SERVICES
PRIVACY AND SECURITY OFFICE

ROY COOPER
GOVERNOR

MANDY COHEN, MD, MPH
SECRETARY

PYREDDY REDDY
CHIEF INFORMATION SECURITY OFFICER

COVID-19 DHHS Privacy and Security Office Guidance

This document is a high-level summary of the various COVID-19 specific guidelines distributed by NC DHHS, Federal, and State regulations. This document shall continue to be updated as public health emergency related guidance evolves throughout the nation and impacting how we implement Privacy and Security policy in our standard operations. For more in-depth analysis of each topic please refer to the referenced links at the bottom of each section.

- Data types may include, but not limited to: Protected Health Information (PHI), Personally Identifiable Information (PII), Family Educational Rights and Privacy Act (FERPA), 42 CFR Part 2 Substance Abuse Data, Internal Revenue Services (IRS), Federal Tax Information (FTI), Social Security Administration (SSA) and CMS.

- Data Type safeguard example: HIPAA Privacy Rule and North Carolina Confidentiality Laws allows special circumstances to share PHI for public health purposes "to prevent a serious and imminent threat"

- Safeguards and tips to help provide guidance:

    - Ensure confidential and sensitive information stored on or sent to or from remote devices are encrypted during transmission and when at rest or being stored on the device - this applies to any removable media used by the device.

    - Understand how to detect and handle phishing attacks and other forms of social engineering that involves remote devices and access to State information systems.

    - Work devices should not be shared with or used by anyone else in the home.

    - Only use the VPN when accessing State information systems for working remotely.

    - No personal devices, thumb drives or cloud services such as their personal Google Drive or Dropbox accounts when using NC State resources.

    - Personal devices may be used when accessing work emails and outlook calendars.

    - Ensure that "Remember password" functions remain turned off when logging into DHHS or State information systems and applications.

  - Limit access to protected information to the minimum scope and duration needed to perform your duties.

- Report **all** privacy and security incidents via https://www.ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security.

- **COVID-19 Guidance Questions may be sent to:** COVID.PrivacySecurityGuidance@dhhs.nc.gov

Contents

Telehealth Remote Communications

On March 17th, 2020 HHS OCR issued a "Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency." The following are the high-level summary points from the OCR notification.

- **HIPAA Penalty Waivers:** OCR will not impose penalties for noncompliance with HIPAA Rule regulations for covered providers who are providing telehealth in good faith during the nationwide public health emergency. Waived penalties include those associated with lack of a BAA with the communications vendor.
    - "Good Faith" use will be reviewed by OCR for all facts and circumstances.
        - "Bad Faith" examples include use of telehealth services include acts that are criminal, fraudulent, identity theft, or intentional invasion of privacy; Any sale of data, or use for marketing purposes; violations of state licensing laws or professional ethical standards; use of public facing remote communication products described below.
    - Specifically, covered health care providers will not be subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules. However, these rules must be applied to other areas outside of telehealth during the emergency.
    - Reporting of security breaches or interception during the use of telehealth services shall be reported to the DHHS Privacy and Security office using the link provided in the *COVID-19 DHHS Privacy and Security Office Guidance* section.
- **Telehealth Technologies:** Non-public facing remote communication products (audio and video).
    - Approved: Skype for Business; Updox; VSee; Zoom for Healthcare; Doxy.me; Google G Suite Hangouts Meet, Apple FaceTime, Facebook Messenger Video, WhatsApp video chat
    - Unapproved: Facebook Live, Twitch, TikTok, Slack
- **Patient Notification Disclaimer:** Providers should notify patients about the privacy risks to their information while using approved telehealth communication products. The following script shall be considered:
    - "Dear (Patient Name),

      Our facility has the ability to implement an alternative way to deliver health care to you in response to the COVID-19 Nationwide Public Health Emergency. A Telehealth communication application will be used during our encounter. I must inform you that while using this application, there is potential risk to your personal and protected health information however, we have put in measures to reduce that risk to the maximum extent".

For more information please go to the following websites:

The Notification of Enforcement Discretion on Telehealth Remote Communications: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

The FAQ's on telehealth remote communications: https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

COVID-19 and North Carolina Confidentiality Laws

Medical first responders need additional information for treatment purposes. Information that identifies a person who has or may have COVID-19 is protected by confidentiality laws. In compliance with North Carolina Confidentiality laws (Confidentiality Laws), certain procedures must be taken into account in providing information to medical and non-medical first responders. The following provides the limitations under North Carolina Confidentiality Laws.

Applicable Confidentiality Laws

- **North Carolina's Communicable Disease Confidentiality Law** (G.S. 130A-143) allows disclosure necessary to protect public health in accordance with statewide communicable disease rules G.S. 130A-143(4). North Carolina communicable disease rules do not include COVID-19 specific provisions. Where state confidentiality law is silent, state public health officials are to use CDC guidelines and recommended actions and provide guidelines to use for control measures.
    - Disclosures to 911 call centers:
        - Local health departments may provide individually identifiable information about individuals with known or suspected COVID-19.
        - Local health departments shall notify dispatchers that the information is not public record and shall be treated as strictly confidential under North Carolina and HIPAA laws.
    - Disclosures to Non-Medical First Responders (Fire or Law Enforcement):
        - Unless exceptions apply to the confidentiality laws, disclosures to non-medical first responders shall be limited to the type of PPE needed or other measure to protect their health and safety. Specific health information about the health of the individual shall not be disclosed.
    - Disclosures to court or law enforcement officials:
        - For the purpose of enforcing North Carolina's communicable disease laws, local health departments or NC DHHS may disclose information to a court or law enforcement official. However, this applies when a person has violated a communicable disease law, isolation, or quarantine order where criminal charges are being sought.
        - Redisclosure of information under these purposes is prohibited.
- **North Carolina EMS Confidentiality Law** G.S. 143-518.
    - Permits disclosures to health care personnel providing medical care to a patient
    - Patient identifiable data that are complied and maintained by hospitals, statewide trauma systems, or EMS providers in connection with the dispatch, response, treatment, or transport of patients is strictly confidential, is not public record, and may be disclosed within the provisions of the statute.
    - Permits disclosure allowed by any other law such as HIPAA.

For more information please go to the following website: https://canons.sog.unc.edu/disclosing-information-about-people-with-covid-19-to-first-responders/

COVID-19 HIPAA Privacy and Coronavirus

- HIPAA Privacy Rule protects the privacy of patients' health information (PHI – Protected Health Information)
    - Privacy Rule is balanced to ensure appropriate uses and disclosures of information to the extent necessary to treat a patient, to protect the nation's public health, and for other critical purposes.
- **Sharing Patient Information - Treatment:**
    - HIPAA Privacy Rule allows covered entities to disclose, without a patient's authorization, PHI about the patient, as necessary, to treat the patient or to treat a different patient.
    - Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment.
    - See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of "treatment" at 164.501 for more information.
- **Sharing Patient Information – Public Health Activities**:
    - Public Health Authority
        - 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.
        - Also inclusive of CDC or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability.
        - A covered entity may disclose to the CDC PHI on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have Novel Coronavirus (2019-nCoV).
        - A covered entity may disclose PHI of an individual who has been infected with, or exposed to COVID-19, with law enforcement, paramedics, or other first responders without obtaining the patient's HIPAA authorization when the disclosure is for treatment, required by law, or to prevent or control the spread of disease.
        - See 45 CFR §§ 164.501 and 164.512(b)(1)(i) for more information.
    - At the direction of a public health authority to a foreign government agency.
        - Acting in collaboration with the public health authority.
        - See 45 CFR 164.512(b)(1)(i) for more information.
    - To persons at risk.
        - Persons 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) for more information.

- **Sharing Patient Information - Disclosures to Family, Friends, and Others Involved in an Individual's Care and for Notification:**
    - Covered entities may share PHI with a patient's family members, relatives, friends, or other persons identified by the patient as involved in the patient's care.
    - Covered entities 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.
    - Sharing may also include, where necessary, to notify family members and others, the police, the press, or the public at large.
    - See 45 CFR 164.510(b) for more information.
    - Important Notes:
        - Covered Entity will need verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object,
            - If the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.
        - Patients who are unconscious or incapacitated:
            - A health care provider may share relevant information about the patient with family, friends, or others involved in the patient's care or payment for care, if the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient.
                - Example - a provider may determine that it is in the best interests of an elderly patient to share relevant information with the patient's adult child, but generally could not share unrelated information about the patient's medical history without permission.
            - A covered entity may share PHI with disaster relief organizations (e.g., American Red Cross) authorized by law or by their charters to assist in disaster relief efforts, for the purpose of coordinating the notification of family members or other persons involved in the patient's care, of the patient's location, general condition, or death.
                - It is unnecessary to obtain a patient's permission to share the information in this situation if doing so would interfere with the organization's ability to respond to the emergency.
- **Sharing Patient Information - Disclosures to Prevent a Serious and Imminent Threat:**
    - Providers may disclose a patient's PHI to anyone who is in position to prevent or lesson the serious and imminent threat, including family, friends, caregivers, and law enforcement without a patient's permission.
    - HIPAA defers to the professional judgment of health professionals in making such determinations.
    - See 45 CFR 164.512(j) for more information.

- **Sharing Patient Information - Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification:**
    - 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 (or the written authorization of a personal representative who is a person legally authorized to make health care decisions for the patient).
    - Unless patient has objected or restricted the release of PHI, a covered hospital or other health care facility may, upon a request to disclose information about a particular patient asked for by name, release limited facility directory information to acknowledge an individual is a patient at the facility, and may provide basic information about the patient's condition in general terms (*e.g*., critical or stable, deceased, or treated and released).
    - Covered entities may disclose information when the patient is incapacitated, if the disclosure is believed to be in the best interest of the patient and is consistent with any prior expressed preferences of the patient.
    - See 45 CFR 164.510(a) and 45 CFR 164.508 for more information.
- **Sharing Patient Information - Minimum Necessary:**
    - Covered entities must make reasonable efforts to limit the information disclosed to that which is the "minimum necessary" to accomplish the purpose.
        - Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes
- **Safeguarding Patient Information:**
    - Covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures.
    - Covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic PHI.
- **HIPAA Applies Only to Covered Entities and Business Associates:**
    - The HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity's or business associate's workforce.
    - Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more covered health care transactions electronically, such as transmitting health care claims to a health plan.
    - Business associates generally are persons or entities (other than members of the workforce of a covered entity and inclusive of subcontractors) that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI
    - The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered entities or business associates.
    - A business associate of a covered entity may make disclosures permitted by the Privacy Rule.

For more information please go to the following website:
https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf
https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf

National Institute of Standards and Technology (NIST) Telework Security

- **Enterprise Telework and Remote Access Security:**
    - All components of telework and remote access solutions, including client devices, remote access servers, and internal servers accessed through remote access, should be secured against a variety of threats.
    - Before designing and deploying telework and remote access solutions, organizations should develop system threat models for the remote access servers and the resources that are accessed through remote access.
    - Organizations should assume that client devices will be acquired by malicious parties who will either attempt to recover sensitive data from the devices or leverage the devices to gain access to the enterprise network.
    - Organizations should plan their remote access security on the assumption that the networks between the telework client device and the organization cannot be trusted.
    - Organizations should assume that client devices will become infected with malware and plan their security controls accordingly.
    - Organizations should carefully consider the balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources.
    - Organizations should ensure that any internal resources they choose to make available through remote access are hardened appropriately.
    - Organizations considering permitting BYOD devices within the enterprise should strongly consider establishing a separate, external, dedicated network for BYOD use within enterprise facilities
- **Remote Access Solution Security**
    - Remote access servers should be kept fully patched, operated using an organization-defined security configuration baseline, and only managed from trusted hosts by authorized administrators.
    - Organizations should carefully consider the security of any remote access solutions that involve running a remote access server on the same host as other services and applications.
    - Organizations should consider several major factors when determining where to place a remote access server, including device performance, traffic examination, unprotected traffic, and NAT.
    - Organizations should place remote access servers at the network perimeter unless there are compelling reasons to do otherwise.
    - Remote access servers should authenticate each teleworker before granting any access to the organization’s resources, and then use authorization technologies to ensure that only the necessary resources can be used.
    - Any sensitive information from remote access communications passing over the Internet, wireless networks, and other untrusted networks should have its confidentiality and integrity preserved through use of cryptography.
    - Organizations should carefully plan how remote access client software security will be maintained and managed before selecting and deploying a remote access solution.

- Organizations should also plan how the telework client devices that they provide to teleworkers will be managed and supported.

- Organizations should ensure that remote management is properly secured, particularly encrypting network communications and performing mutual authentication of endpoints.

- Organizations with higher security needs or with particularly high risks against their remote access communications should use thick remote access clients whenever possible to reduce the risk of compromise

- **Telework Client Device Security:**

  - Telework client devices should be secured properly and have their security maintained regularly.

  - Telework client devices should have the same local security controls as other client devices in the enterprise.

  - Sensitive information, such as certain types of PII (e.g., personnel records, medical records, financial records), that is stored on or sent to or from telework devices should be protected so that malicious parties cannot access or alter it.

  - An organization should have a policy of encrypting all sensitive data when it is at rest on the device and on removable media used by the device.

  - For telework mobile devices, organizations should take advantage of centralized security management capabilities whenever available.

- **Security Considerations for the Telework and Remote Access Life Cycle:**

  - A telework security policy should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, the type of access each type of teleworker is granted, and how user account provisioning should be handled
  - Each organization should make its own risk-based decisions about what levels of remote access should be permitted from which types of telework client devices.

  - Organizations should periodically reassess their policies for telework devices and consider changing which types of client devices are permitted and what levels of access they may be granted.

  - Organizations should document the security aspects of the telework and remote access solution design in the system security plan.

  - An organization should implement and test a prototype of the design and evaluate it, including its connectivity, traffic protection, authentication, management, logging, performance, implementation security, and interference with applications.

  - Organizations should regularly perform operational processes to maintain telework and remote access security, such as deploying updates, verifying clock synchronization, and reconfiguring access control.

  - Organizations should also periodically perform assessments to confirm that the organization's remote access policies, processes, and procedures are being followed properly.

  - Before disposing of a telework client device or remote access server, the organization should remove any sensitive data from it.

For more information please go to the following website:
NIST**:** https://content.govdelivery.com/accounts/USNIST/bulletins/2822a2f

COVID-19 Phishing Emails Guidance

Phishing is the most common type of cyber-attack that affects organizations like DHHS.

- Phishing attacks can take many forms.
    - Goal - Getting you to share confidential information such as health information, login credentials, credit card information, or bank account details.
- **Types of Attacks:**
    - Phishing - Hackers impersonate a real company to obtain your login credentials,
    - Spear Phishing - More sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source,
        - Hackers may use your name and phone number and refer to DHHS in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.
    - Whaling - A popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real DHHS executive.
        - Using a fake domain that appears like ours, they look like normal emails from a high-level official and ask you for sensitive information (including usernames and passwords).
    - Shared Document Phishing - You may receive an e-mail that appears to come from file-sharing site like SharePoint or DocuSign alerting you that a document has been shared.
        - The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your credentials.
- **What You Can Do To avoid these phishing schemes, please observe the following email best practices:**
    - Do not click on links or attachments from senders that you do not recognize,
    - Do not provide sensitive personal information (like usernames and passwords) over email,
    - Watch for email senders that use suspicious or misleading domain names,
    - Inspect URLs carefully to make sure they’re legitimate and not imposter sites,
    - Do not try to open any shared document that you’re not expecting to receive,
    - Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

Teleworking with FTI data

On March 19th, 2020 the IRS Office of Safeguards issued a Security and Privacy Alert providing teleworking with Federal Tax Information (FTI). Publication1075 provides requirements for the proper handling and protection of FTI at telework locations.

- **Publication 1075 Telework Requirements:** All physical safeguards required for computers, electronic devices and media, shall apply to telework locations. To prevent unauthorized disclosure and protection of systems, the following base requirements must be provided:
    - Any remote access where FTI is accessed over a remote connection must be performed using multifactor authentication (MFA). More information on MFA can be found at the North Carolina Statewide Information Security Policy. https://it.nc.gov/resources/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies
    - FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore-outside of the United States territories.
    - FTI may not be received, processed, stored, transmitted, accessed by or through, and/or disposed of by IT systems located offshore.
- **NC DHHS Mandated Laptop Requirements:** NC DHHS agency laptops must be used with NC DHHS VPN. The VPN must be configured to the following technical capabilities:
    - Monitor and control remote access methods.
    - Implement cryptographic mechanisms to protect confidentiality and integrity of remote access sessions that transmit FTI over the remote connection.
    - Route all remote accesses through a limited number of managed network access control points.
- **Telework Best Practices for Protecting FTI data:**
    - Do not place systems in front of windows or areas that promote shoulder surfing.
    - Establish VPN tunnels using FIPS 140 algorithms before accessing FTI systems.
    - Implement session lock on agency laptop.
    - Create strong passwords and restrict access to employee-managed networks to only devices you know.
    - Do not include FTI email transmissions outside of the agency's internal network.
    - Ensure Access controls include password security, audit trail, encryption, virus detection, and data overwriting capabilities.

For more information please go to the following website: https://www.irs.gov/pub/irs-pdf/p1075.pdf

COVID-19 AND FERPA DATA

On March 2020, The United States Department of Education issued Frequently Asked Questions regarding the Family Educational Rights and Privacy Act (FERPA) and the COVID-19 National Public Health Emergency. Below are high level summary points of this notification.

- **FERPA:** Federal Law that protects the privacy of student education records. It applies to all educational agencies and institutions that receive funds under any program administered by the Secretary of Education.
    - School Districts, Public Schools, Private post-secondary schools.

- **Use Case:** Enable information sharing and coordination between educational institutions and public health departments.

- **Sharing of personally identifiable information (PII) with Agencies:** School officials may disclose PII from student education records as necessary with State and local public health officials without prior written consent.

- **Sharing of PII with parents or students other than the afflicted student:** Only de-identifiable information can be shared with parents or students without prior written consent regarding any student in attendance who is out sick due to the COVID-19 virus.

- **Sharing of PII with the afflicted student's parents:** An educational agency or institution may disclose eligible student's PII to the parent without obtaining the student's consent whether or not the parent claims the student as an dependent under section 152 of the IRS Code 1986 when in connection with a health or safety emergency.

For more information please go to the following websites:
U.S. Department of Education: https://www.ed.gov/coronavirus
https://studentprivacy.ed.gov/

Telehealth and 42 CFR Part 2 Guidance
Substance Abuse and Mental Health Services Administration (SAMHSA)

In response to the Public Health Emergency on COVID-19, SAMHSA has provided guidance to ensure that substance use disorder treatment services are uninterrupted.

- **Use and Disclosure of 42 CFR Part 2 Data:** Obtaining written patient consent for disclosure of substance use disorder records may not be possible. Under these circumstances, prohibition on use of disclosure of patient identifying information under 42 CFR Part 2 would not apply to the extent that the provider determines that a medical emergency exists.
    - **42 CFR Section 2.51** permits disclosure by a part 2 program or other lawful holder to medical personnel without patient consent in order to meet a medical emergency when the patient's prior informed consent cannot be obtained.
- **Redisclosure:** Information disclosed to medical personnel who are providing treatment during a medical emergency may re-disclose for treatment purposes as needed.
- **Record Documentation:** Part 2 requires programs to document certain information in their records after a disclosure is made pursuant to the medial emergency exception.

For more information please go to the following websites:
SAMHSA: https://www.samhsa.gov/sites/default/files/covid-19-42-cfr-part-2-guidance-03192020.pdf