Confidentiality and Information Security Agreement

The following rules for Confidentiality and Information Security apply to all non-public patient and business information ("Confidential Information") of Trinity Health and all of its affiliated and controlled healthcare organizations. The rules also apply to the non-public and business information of joint ventures, and other entities and persons collaborating with Trinity Health, to which an authorized user has access to Trinity Health's computer system, network or application ("Computer System") containing Confidential Information.

As a condition of being permitted to have access to Confidential Information on Trinity Health's Computer System which is relevant to my job function or role, I agree to comply with Trinity Health's posted policies and procedures, including the following rules:

1. **Permitted and Required Access, Use and Disclosure of Confidential Information:**
   - I will access, display, store, use or disclose confidential Protected Health Information (PHI) only for legitimate purposes of diagnosis, treatment, or obtaining payment for patient care or for healthcare operations permitted by HIPAA.
   - I will access, use or disclose Confidential Information only for legitimate business purposes of Trinity Health.
   - I will disclose confidential information only to individuals who have a need to know to fulfill their job responsibilities and business obligations (e.g., co-workers, business associate).
   - I will only access, use or disclose the minimum necessary amount of confidential information needed to carry out my job responsibilities or role.
   - I will protect all confidential information to which I have access, or which I otherwise acquire, from loss, misuse, alteration, a modification or unauthorized disclosure and access including, but not limited to, the following:
     - making sure that paper records are not left unattended in unsecure areas where unauthorized people may view them;
     - using password protection, screensavers, automatic time-outs and/or other appropriate security measures to ensure that no unauthorized person may access confidential information from my workstation or other device;
     - appropriately disposing of confidential information in a manner that will prevent a breach of confidentiality and never discard paper documents or other materials containing confidential information in the trash unless they have been shredded;
     - safeguarding and protecting workstations and portable electronic devices containing confidential information including laptops, smartphones, tablets, CDs, USB thumb drives, etc.; and
     - Ensure physical security of workstations.
   - I will ensure that any confidential information that is transmitted using the Internet or other public networks is sent over a secure connection like VPN (That is, do not access, use or disclose confidential information at a hotel, Panera Bread, etc.).
   - I agree to remove or delete confidential information when it is no longer needed.
   - I understand that my access to Trinity Health's computer system is a privilege and not an absolute individual right.
   - I will comply with Trinity Health's Enterprise Information Security and Privacy policies and procedures.

2. **Prohibited Access, Use and Disclosure of Confidential Information:**
   - I will not access, display, store, use or disclose confidential information in electronic, paper or oral forms for personal reasons, or for any purpose not permitted by Trinity Health policies and procedures, including information about co-workers, family members, friends, neighbors, celebrities, or myself**.

** NOTE: I will follow the required procedures at each applicable Ministry Organization regarding gaining access to my own PHI in medical and other records.

- I will not engage in any activity that attempts to circumvent or avoid information security controls.
- I will not share / disclose my own login ID, password, or other security device with any other person, including but not limited to, co- workers, supervisors, subordinates, family members, friends, etc. for any reason.
- I will not use another person's login ID, password, other security device or other information that enables access to Trinity Health's Computer System.
- If my employment or association with Trinity Health ends, I will not subsequently access, use or disclose any Trinity Health confidential information and will promptly return any security devices and other Trinity Health property.
- I will not at any time or in any manner, either directly or indirectly, access confidential information for purposes of distributing, selling, marketing or commercializing Trinity Health confidential information for personal gain.
- I will not engage in any personal use of Trinity Health's Computer Systems that inhibits or interferes with the productivity of colleagues or others associated within Trinity Health's business operations, or that is intended for personal gain.
- I will not at any time or in any manner use by access to create derivative products or applications based on Trinity Health's confidential information.
- I will not utilize the Trinity Health computer system to access Internet sites that contain content that is inconsistent with the mission, values, policies, and procedures of Trinity Health.
- I will not misuse or attempt to alter Trinity Health's Computer System in any way.
- I will not carelessly utilize an Internet capability that may negatively impact Trinity Health's Computer System normal performance or unduly jeopardize network computing capabilities and resources, including causing them to malfunction regardless of location or duration.
- I understand that scanning of the network is prohibited when it is not within the scope of your job function or role.
- I understand that sharing network and/or application accounts (including work email accounts) is not permitted.
- I will not willfully introduce a computer virus or other destructive program into Trinity Health's Computer System, including vendor/supplier computer systems and networks.
- I will not automatically forward email to an external destination (i.e., personal email accounts) not specifically approved by Trinity Health policy, procedure, administration, or department management.
- I will not use Trinity Health's Computer System or email for solicitation or for non-Trinity Health commercial endeavors not specifically approved by Trinity Health policy, procedure, administration, or department management.
- I will not send unsolicited mass email messages, including the sending of "junk mail" or other advertising material (e.g., email spam), over Trinity Health's computer system.
- I will not send bulk emails to non-Trinity Health recipients revealing the identity of the recipients (e.g., instead I will use 'blind copy' functionality)
- While utilizing Trinity Health's Computer System, I will not engage in the transmission of information which is demeaning, defaming, harassing (including sexually) or disparaging to others based on race, national origin, sex, sexual orientation, age, disability or religion, or which is otherwise offensive, inappropriate and/or in violation of the mission, values, policies or procedures of Trinity Health.
- I will not access, display, store or distribute any offensive, discriminatory, or pornographic materials on Trinity Health's Computer System.
- I will not use Trinity Health's Computer System to create an intimidating or hostile work environment.
- I will not use Trinity Health's Computer System to commit fraud or use it unethically. Examples of fraud and unethical use include, but is not limited to, the following:
    - misrepresenting oneself, or inappropriately representing Trinity Health;
    - any misrepresentation / fraud to gain unauthorized access to a Computer System;
    - unauthorized decrypting or attempting to decrypt the Computer System;
    - using an account of another individual without the latter's express permission or proxy.
    - solicitation that is not specifically approved by Trinity Health policy, procedure, administration, or department manager; and

- participating in non-Trinity Health sponsored contests, games, or on-line gambling.

3. Use of Trinity Health Computer Systems/Devices:

- I understand that I am accountable for my use of Trinity Health's Computer System, including, but not limited to, my content, emails and Internet use.
- I will immediately notify the Trinity Health's Security Official or Privacy Official if I believe that there has been improper/unauthorized access to Trinity Health's Computer System or improper use or disclosure of confidential information in electronic, paper or oral forms.
- I understand that I am required to immediately report lost or stolen devices containing Trinity Health Confidential Information to TIS Service Desk at 888-667-3003 I understand that if I violate any of the requirements of this agreement, I may be subject to disciplinary action, my access may be suspended or terminated and/or I may be liable for breach of contract and subject to substantial civil damages and/or criminal penalties.

4. Trinity Health Monitoring and Disclosure to Third Parties / Law Enforcement:

- I understand that Trinity Health has the right to access and will Monitor my access to, and my activity within, Trinity Health's Computer System.
- I understand that I have no rightful expectation of privacy regarding my access or activity within Trinity Health's Computer System, including, but not limited to, any and all email messages sent or received from the same (e.g., personal email accounts).
- I understand that Trinity Health may disclose, as it deems necessary, my activity and any of my content on Trinity Health's Computer System to law enforcement officials and to management without my consent / authorization or prior notice to me.
- I understand that if I violate any of the requirements of this agreement, I may be subject to disciplinary action, my access may be suspended or terminated and/or I may be liable for breach of contract and subject to substantial civil damages and/or criminal penalties.

5. Appropriate Software Use:

- I agree to use only Trinity Health approved software to conduct Trinity Health business.
- I understand that my use of the software on Trinity Health's Computer System is governed by the terms of separate license agreements between Trinity Health and the vendors of that software.
- I agree to use such software only to provide services to benefit Trinity Health.
- I will not attempt to download, copy or install the software on any computer or other Trinity Health device.
- I will not make any change to any of Trinity Health's computer systems without Trinity Health's prior express written approval.
- I will not make any unauthorized reproduction of information system software.
- I agree not to violate any copyright or intellectual property rights laws.

6. Appropriate Network Use:

- I understand that access to Trinity Health's Computer System is "as is", with no warranties and all warranties are disclaimed by Trinity Health.
- I understand that Trinity Health may suspend or discontinue access to protect the Computer System or to accommodate necessary down time.
- I understand that in an emergency or unplanned situation, Trinity Health may suspend or terminate access without advance warning.

7. Termination of User's Access to Trinity Health's Computer System:

- Trinity Health, in its sole discretion, has the absolute right to terminate this agreement and the user's access and use of confidential information at any time, with or without notice, for any reason or no reason without any damages or liability to you.

8. **Employer Acceptance of Responsibility for an Individual with Access to Trinity Health's Computer System containing Confidential Information*:***

(Applies to physicians/physician practices; other individual or facility providers; a business associates; vendors; payers; any other unaffiliated organizations).

- I accept responsibility for all actions and/or omissions by my employees and/or agents.
- I agree to notify the TIS Service Desk at 888-667-3003 within 5 business days if any of my employees or agents no longer need or are eligible for access due to leaving my practice/company, changing their job duties or for any other reason.
- I agree to complete an annual review of all employees and agents in an effort to identify individuals who no longer need access.
- I agree to report any actual or suspected privacy or security violations made by my employees and/or agents to Trinity Health's Privacy Official or Security Official.
- I understand that Trinity Health may terminate my employee and/or agent's access, with or without prior notice to anyone, at any time.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

SIGNATURE PAGE / RELATIONSHIP TO TRINITY HEALTH / MINISTRY ORGANIZATION

I am a: (*Please check all that apply to you*)

Direct relationships with (MacNeal Hospital)

___Colleague (employee) at (MINISTRY Name)
___Physician Credentialed on (MINISTRY Name) Medical Staff
___Volunteer at a (MINISTRY Name) Facility
___Temporary/Contractor at a (MINISTRY Name)/ Facility: (name of agency)
☐ Student at MacNeal Hospital, From:

Employed by or Associated with a (MINISTRY Name) Credentialed Medical Staff Member

___Medical Staff Member's Employee or Temp Staff (name of practice) _____
___Medical Staff Member's Vendor's Employee (name of vendor)_____

Vendor Providing Goods or Services to (MINISTRY Name)

___Employee/Temp Staff of (MINISTRY Name)'s clinical services vendor: (name of vendor)
___Employee/Temp Staff of (MINISTRY Name)'s business services vendor: (name of vendor)
___Employee/Temp Staff of (MINISTRY Name)'s IT services vendor: (name of vendor)

(MINISTRY Name)'s Joint Venture or a Facility Managed by (MINISTRY Name)

___Employee of a (MINISTRY Name)'s Joint Venture (name of joint venture:) _____
___Employee of a Hospital/Other Facility Managed by (MINISTRY Name) (name of facility):_____
___Credentialed Physician on Medical Staff of a Hospital/Other Facility Managed by (MINISTRY Name):
(Name of facility):_____
__ Employee or Temp Staff of a Credentialed Physician on the Medical Staff of a Hospital/Other Facility Managed by (MINISTRY Name): (name of physician's practice)

Other

☐ Unaffiliated (non-credentialed) Physician/Other Provider: _____
___Unaffiliated Physician or Facility: (name of practice or facility) _____
___Employee of a Payer :(name of payer)
___Researcher (Research study name):_____
___Other (name of employer) _____

USER SIGNATURE

If there are any items in this agreement that I do not understand, I will ask my supervisor or other appropriate (MacNeal Hospital) contact person for clarification. My signature below acknowledges that I have read, understand and accept this agreement and realize it is a condition of my employment or association with Trinity Health. I also acknowledge that I have received a copy of this Confidentiality and Network Access Agreement.

Print Name:

Signature of individual to be given access: Date:

EMPLOYER SIGNATURE- Completed by MacNeal Hospital

(**Required** when user is an employee or agent of: a physician/physician practice; other individual or facility provider; a vendor that is not a business associate; any other organization unaffiliated with (MacNeal Hospital) or Trinity Health.
My signature below acknowledges that I have read, understand and accept my responsibilities as the employer or the sponsor of the user who has signed this agreement above.

Print Name:

Signature of employer of the individual to be given access: Date: