Trinity Health

Trinity Health Acceptable Use Acknowledgement

Background/Applicability

The following requirements apply to all non-public patient, colleague, and business information, including patient information (protected health information **("PHI")**) ("Confidential Information"). The requirements apply to Confidential Information in electronic, paper, and oral forms (any form). Confidential Information includes information of Trinity Health and all its affiliated and controlled healthcare organizations. The requirements apply to all computer systems, networks, or applications to which an authorized user has access, and which are used for Trinity Health activities. This includes third parties' and Trinity Health's computer systems, networks, and applications (collectively, the "Information Systems").

You must acknowledge agree to the following requirements as a condition of employment and/or being permitted to have access to (and logon credentials for) Information Systems. You are required to acknowledge that you understand the requirements. You also are required to agree that you are accountable to comply with Trinity Health's Acceptable Use Procedure.

Section 1: General Rules

- You agree to act in the best interest of Trinity Health. You agree to support compliance with federal and state laws and regulatory requirements including, but not limited to Health Insurance Portability and Accountability Act Laws and Regulations and updates and additions ("HIPAA").
- You agree to comply with the Trinity Health Acceptable Use Procedure.
- Trinity Health reserves the right to access, monitor, or disclose the information within its Information System and/or on its network as it deems necessary. Trinity Health may disclose your activity to law enforcement officials and Trinity Health management without your consent or prior notice to you.
- Trinity Health, in its sole discretion, has the absolute right to terminate your access and use of Confidential Information and/or Information Systems at any time. Trinity Health may terminate your access and use, with or without notice, for any reason or no reason, without any liability to you.
- You agree to maintain a current contact phone number, text accessible cell phone number and personal email in Trinity Health identity data storage. Trinity Health may use your phone number if necessary for user identification. Trinity Health may contact you by text or voicemail to any phone number associated with your identity, including cell phone numbers, which could result in charges to you.

Section 2: Information Security

Use of Trinity Health Computer Systems/Devices:

- Immediately report to the TIS Service Desk at 888-667-3003, including:
  - Suspected security events;
  - Security policy violations (such as improper/unauthorized access to Trinity Health's Computer System);
  - Possible improper use or disclosure of Confidential Information (in electronic, paper, or oral forms); and
  - Lost or stolen devices with access to Trinity Health's Information System or Confidential Information.

- Use Trinity Health devices only for purposes permitted by Trinity Health:
  - If in doubt about use of a Trinity Health device contact your supervisor or the TIS Service Desk.
- Care for and use Trinity Health devices in a secure and confidential manner:
  - Assure physical security for the devices;
  - Assure confidential storage of the devices; and
  - Assure secure disclosure and access to Confidential and PHI Confidential Information.

Only use Trinity Health computer systems/devices while traveling outside of the United States of America in accordance with the International Travel Policy.

Acceptable Use of Email, Network, and Internet

- Download, configure and use the approved security applications (currently Microsoft Authenticator) with your mobile device for secure remote access to the Trinity Health network.
- Encrypt Confidential Information when transmitted across non-Trinity Health networks.
- Use Trinity Health's email and other Information System resources only to perform job functions.
- In an emergency or unplanned situation, Trinity Health may suspend or terminate your access without advance warning to protect its Information System.
- Do not use Trinity Health's Information System or other network resources to harm, expose, or create legal liabilities by inappropriate use.

Password Use and Security

- Create, protect and use strong passwords, as described in Trinity Health's Acceptable Use Procedure.
- Use only your personally assigned user credentials and do not share your user credentials (e.g., login IDs, passwords, PINs, access codes, badges) with others for any reason.

Appropriate Software Use:

- Do not download non-Trinity Health sanctioned software/programs to Trinity Health devices.
- Use only Trinity Health approved software to conduct Trinity Health business and store Confidential Information.
- Do not make any changes to Trinity Health's Information Systems or devices without Trinity Health's prior written approval.

Information Protection

- Secure your workstation by locking screen or logging-off workstation when the device is not in use.
- Secure physical documents containing Confidential Information in a locked location when not in use.

Section 3: Legal and Privacy

Permitted and Required Access, Use and Disclosure of Confidential Information- You agree to:

- Access, display, store, use or disclose PHI only for legitimate purposes of diagnosis, treatment, or obtaining payment for patient care or for healthcare operations. You agree to actions only as appropriate to your employment/role.
- Protect all Confidential Information to which you have access, or which you otherwise acquire, from loss, misuse, alteration, modification, or unauthorized disclosure or access.
- Appropriately dispose of Confidential Information in a manner that will prevent viewing or use of the information. You agree never to discard paper documents or other materials containing Confidential Information in the trash unless they have been shredded.

Trinity Health

Prohibited Access, Use and Disclosure of Confidential Information Requirements:

- Do not access, display, store, use or disclose Confidential Information in any form for personal reasons, or for any purpose not permitted by Trinity Health policies and procedures. This prohibition includes information about co-workers, family members, friends, neighbors, celebrities, or yourself. (**NOTE:** You must follow the required procedures at each applicable Ministry regarding gaining access to your own PHI in medical and other records.)
- Do not use another person's login ID, password, badges, or other method that enables access to the Information Systems or Confidential Information.
- When your employment or association with Trinity Health ends:
  - Do not subsequently access any non-public Information Systems (other than as directed by Trinity Health for communication purposes);
  - Do not access, use, or disclose any Trinity Health Confidential Information;
  - Promptly return any devices and other Trinity Health property; and
  - Appropriately dispose of Confidential Information.
- Do not distribute, sell, market, or commercialize Trinity Health Confidential Information for personal gain.
- If your role requires distributing information outside of Trinity Health, do not send bulk emails (more than five) revealing the identity of the recipients (use 'blind copy' functionality).
- Do not access, disclose, or reproduce Trinity Health's Confidential Information outside of your job function/role.
- Do not access any Information Systems when located outside of the United States, except in accordance with the Trinity Health International Travel Policy.

Acknowledgement

- By typing or signing your name below, you hereby agree that: you have read this Acceptable Use Acknowledgement and Trinity Health's Acceptable Use Procedure and agree to abide by the requirements,
- you acknowledge that violation of Trinity Health's Acceptable Use Procedure or these requirements may lead to disciplinary action, up to and including termination, and
- you acknowledge that your access may be suspended or terminated and/or you may be personally liable for failure to comply and are subject to substantial civil damages and/or criminal penalties for any violation of these requirements.

If there are any items in these requirements that you do not understand, you agree to promptly ask your supervisor, employer, or sponsor for clarification.

USER SIGNATURE

Signature of individual to be given access: _____

Print Name: _____ Date: _____

EMPLOYER/EXTERNAL SPONSOR SIGNATURE

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

Signature of employer/external sponsor for the individual to be given access: _____

Print Name: _____ Date: _____