CONFIDENTIALITY, NON-DISCLOSURE & APPROPRIATE USE AGREEMENT

In all aspects of our operations, Triangle Area Network (TAN) has a legal responsibility to safeguard the confidentiality and security of our patients' protected health information ("PHI"), as well as operational, proprietary, and student and employee information (collectively "TAN Confidential Information"). This information may include, but is not limited to, technology information, insurance carrier contract terms, inventions of processes or devices or programs, services provided to particular patients, patient lists, all information pertaining to patients which is protected by HIPAA and any other state or federal law, or regulation, strategic or operational planning information, patient care research, fundraising plans and resources, other financial resources and related terms, TAN contracts, fee schedules, costs and expenses charged or incurred by TAN, financial obligations and arrangements, marketing and planning, business affairs, staff rosters, legal matters, process information, or any nonpublic information particular to the business of TAN that is ascertained by employment or professional affiliation or association with TAN. TAN Confidential Information may also include data where loss or unauthorized disclosure would impair the functions of TAN, cause significant financial or reputational loss, or lead to likely legal liability (e.g., financial information, salary information, policies, research work in progress, and copyrighted or trademarked material). Confidential Information may exist in any form, including electronic, video, spoken, or written.

This Agreement does not, however, restrict use of information that is public knowledge that is generally known in the profession, or that the person learned independent of work with the TAN. This Agreement also does not prohibit employees of TAN from appropriately exchanging information to the extent protected by the National Labor Relations Act. However, sensitive employee data, such as employee medical information, family health information, dates of birth, Social Security numbers, and similar information, is considered Confidential Information. TAN Confidential Information also includes data in any format collected, developed, maintained, or managed by or on behalf of TAN, or within the scope of TAN's activities, that are subject to specific protections under federal or state law or regulations or under applicable contracts (e.g.,

medical records, private family information, Social Security numbers, credit card numbers, driver license numbers).

This Agreement applies to all persons providing services to TAN patients, including, but not limited to, employees, volunteers, students, board members, physicians, and third parties, whether temporary or permanent, paid or not paid, visiting, or designated as affiliates or associates, who are employed by, contracted with, or under the direct control of TAN. This Agreement also applies to all persons granted access to PHI of TAN patients or other confidential TAN information. Further, this Agreement applies to all users who are granted access to TAN-issued computing and technology resources (e.g., desktops, laptops, tablets, mobile phones, printers, etc.), application systems or access to the TAN network, whether the user is affiliated with TAN or not, and whether access to or use of the information systems occurs locally or from remote locations. Access to protected information is conditioned upon the receiving party's agreement to comply with the confidentiality protections set forth in this Agreement, as well as the requirements of HIPAA and other federal and state trade secret protection laws, including the Defend Trade Secrets Act and the Texas Uniform Trade Secrets Act.

I understand that TAN relies on me to maintain the confidentiality of the protected information at all times, even after my employment or other association with TAN ends, regardless of the reason for the separation. I hereby agree as follows:

- I will maintain patient privacy and protect and safeguard the confidentiality and security of PHI and TAN Confidential Information in accordance with state and federal laws and TAN policies and procedures. TAN has provided me with the U.S. Department of Health & Human Services Summary of the HIPAA Privacy Rule, and I have read it to confirm that I am familiar with all aspects of HIPAA privacy requirements that apply to my position or role. If I am involved in electronic transfer of PHI, I will also comply with all data security procedures implemented by TAN.
- I understand that access to health information created, received, or maintained by TAN or its affiliates is limited to those who have a valid business, medical, or professional need to know the information. I understand that TAN has implemented administrative, technical, and physical safeguards to protect the confidentiality and security of PHI, and I agree not to bypass or disable these safeguards.
- I will not disclose any PHI or other Confidential Information to any individual or third party, except as specifically authorized by TAN policies and procedures, and upon receiving a written authorization from the affected patient (where required by applicable law), and then only on a need-to-know basis. If I have any doubt about whether any disclosure is appropriate, I will ask for clarification and approval before any disclosure.
- I will not use any PHI or other Confidential Information in an inappropriate, unethical, detrimental or unauthorized manner.

- I will not discuss any information regarding TAN Confidential Information or patients in an area where unauthorized individuals may overhear such information, including waiting rooms, hallways, elevators and other public areas. I understand that it is strictly prohibited to discuss any TAN Confidential Information or PHI in public areas, even if a patient's name is not used.
- I understand that I will be given a unique User ID and password to access electronic health, operational, proprietary, student, employee, or other Confidential Information. I understand that my User ID and password are confidential, may only be used by me, that I am responsible for the safekeeping of my password, that I am also responsible for any activity initiated by my User ID and password, and that in certain circumstances, my User ID and password may be equivalent to my legal signature. If I suspect that my User ID or password has been compromised, I should immediately contact the Operations Manager or Compliance Officer..
- I have no expectation of privacy when using TAN information systems or electronic devices. TAN shall have the right to record, audit, log, and/or monitor all access to or use of its information systems, even if I consider the communications, internet access, or otherwise to be "personal" in nature. I agree to practice good workstation security measures on any computing device that uses or accesses a TAN information system. Good security measures include, but are not limited to, maintaining physical security of electronic devices, never leaving a device unattended while in use, and adequately shielding the screen from unauthorized viewing by others.
- I understand that only encrypted and password protected devices may be used to transport PHI or other Confidential Information.
- I understand that smartphones and other mobile devices used to access TAN information systems must be configured to encrypt any Confidential Information, including photographs and videos, in persistent storage.
- I understand that I may access and/or use PHI and other TAN Confidential Information only as necessary to perform my job-related duties and that I may disclose (i.e., share) TAN Confidential Information only to authorized individuals with a need to know that information in connection with the performance of their job functions or professional duties for or in association with TAN.
- I will only use my personal phone, computer(s), or other electronic devices, or those of any third parties, to receive, transmit, store, or otherwise serve as a conduit or repository of protected TAN information upon receiving specific advance authorization from my immediate supervisor or another authorized TAN representative, and I will follow all procedures applicable to use of electronic devices for the protection of the Confidential Information.
- I will not remove PHI or other TAN Confidential Information, in any form, from the premises of TAN without advance approval from an authorized member of the TAN

management team. This prohibition includes, but is not limited to, electronic forwards, downloads, or other transfers.

- I understand that upon termination of my employment/affiliation/association with TAN, I will immediately return or destroy, as appropriate, any TAN Confidential Information under my control or in my possession.
- I understand that my confidentiality obligations under this Agreement will continue after the termination of this Agreement and after termination of my employment, affiliation or association with TAN. I will not retain any TAN information, nor will I provide such information to any other person for retention on my behalf or any other use. If I have any protected TAN information on my personal phone, computer(s), or other electronic devices, I will cooperate fully with TAN requests to promptly delete all iterations of that information and to demonstrate to the satisfaction of TAN that I have done so.
- I agree to immediately report any known or suspected violation of the confidentiality of TAN Confidential Information or of the security of PHI of patients of TAN to TAN's Compliance Officer or Operations Manager.
- If I have any questions about whether any use of any information is authorized, in fact involves use of confidential information, or otherwise, I will obtain clarification from a TAN officer before disclosing, retaining, or making any use of the information.
- I understand that violations of this Agreement may result in revocation of my user privileges and/or disciplinary action, up to and including termination of my employment, affiliation, or association with TAN and that TAN may seek any civil or criminal recourse and/or equitable relief.
- All trade secrets and other proprietary or otherwise confidential information and all patents, copyrights, trademarks, and other related rights are at all times the sole property of TAN.

An individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that—(A) is made—(i) in confidence to a federal, state or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual—(A) files any document containing the trade secret under seal; and (B) does not disclose the trade secret, except pursuant to court order.

By signing this Agreement, I acknowledge that I have read the Confidentiality, Non-Disclosure and Appropriate Use policy and agree to comply with the terms and conditions stated above.

_____

Signature of Employee

_____

Today's Date