BROWN & TOLAND PHYSICIANS

Confidentiality & Accountability Information Security Attestation

Sign and return by **Dec. 31, 2020** to ***cybersecurity@btmg.com*, *with a copy to* *compliance@btmg.com***

SCOPE

This agreement applies to all physician practice workforce members, including any individual on the payroll, contractors, interns, third-party employees, volunteers, trainees, and other persons whose work for the practice is under the direct control and supervision of the practice, whether or not they are paid by the practice.

DEFINITIONS

Confidential Information includes, but is not limited to the follow categories:

- **Protected Health Information (PHI)** – any information about an individual maintained by an organization, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, mother's maiden name, or biometric records; and (2) any information that is linked to an individual, such as medical, educational, financial, and employment information.
- **Personally Identifiable Information (PII)** – means any individually identifiable information that is a subset of health information including demographic information that: identifies or could be used to identify an individual; is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and relates to the past, present or future physical or mental health or condition of an individual (both electronically or written).
- **Sensitive Information (SEI)** - any information classified by Brown and Toland as confidential, PII, PHI, proprietary or restricted.

PURPOSE

Brown and Toland Physicians (BTP) has a responsibility to safeguard and protect the confidentiality, integrity, and availability of all BTP's Enterprise Information Systems (EIS) and data.

EXPECTATIONS & GUIDANCE

This agreement establishes the expectations for the practice and all workforce members (previously identified) regarding the access, use, and disclosure of confidential information.

The practice is responsible for the following:

Information Security Training and Communication

- Providing information privacy and information security education to all new employees upon hire, and annual refresher training for all workforce members.
- Periodically communicate information privacy and information security reminders.
- Communicating the Workforce Member Expectations to all members of the practice workforce

Maintaining Computer System and Physical Protections

- Maintaining computer system and physical protections
- Devices provided by the practice and used for connecting to BTP's systems, applications, and data. Devices must have system protections which include:
    - Antivirus software
    - Encryption
    - Endpoint protection software (recommended)
- It is expected practice owned devices connecting to BTP's systems, applications, and data will be inventoried and kept up to date with operating system and antivirus software.
- Physical security controls to data and network closets will be restricted and maintained as appropriate.

Managing User Access for its Workforce members

- Managing user access for its workforce
- The practice is responsible for requesting all workforce members are issued their own unique user ID and password to access BTP systems, applications, and data.
- User access must be authorized by a designated practice leader.
- User access must be limited to the minimum necessary for individuals to perform their assigned duties.
- User Access should be rescinded promptly when a user no longer needs access.
- If the practice contracts with a third-party for services requiring access to BTP's systems, applications, and data the practice must notify BTP prior to entering into the agreement and obtain approval for the third-party to have access to BTP's systems, applications and data.
- All third-party arrangements involving offshore staff or staff working temporarily offshore who will have access to BTP's systems, applications, or data need to secure BTP approval before sharing any access or data with the offshore vendor.

Workforce Member Expectations:

It is expected the following expectations will be communicated by the practice to all workforce members.

- ***Comply with all applicable laws pertaining to the privacy and security of PHI, PII, and SEI***.
- Follow all privacy and security policies and procedures.
- ***Not disclose or share any system or application credentials (user ID and password) with anyone for any reason.***
- Users will be held accountable and responsible for all activity conducted with their assigned user ID and password.
- Users shall also agree not to use the credentials of another individual to gain access to BTPs' systems, applications or data.
- Confidential data will only be stored on approved encrypted devices or appropriate network folders.
- Local storage will not be used to store any confidential information.
- Personal devices and removable storage devices, such as USBs will not be used to access or store BTP applications, systems and data.
- Emails containing confidential information will not be forwarded to an external personal email account without appropriate encryption.
- Personal email accounts will not be used to conduct practice or BTP business.
- Posting confidential or proprietary information from the practice or BTP on social media sites is strictly forbidden unless authorized to do so as part of assigned job duties.
- Text messaging PHI, PII, SEI or proprietary information will only be done according to approved secure methods and in accordance with the guidance provided by Information Technology and the practice.
- Safeguards shall be exercised when copying, faxing, printing or disposing of confidential information.
- Securing BTP approval before using systems to access PHI while working outside of the United States.
- BTP has the right to restrict and block the access of any device that poses a security risk to the BTP network.
- Users must acknowledge computer audit logs of user activity will be maintained and BTP has the right to audit and/or monitor access and use of BTP applications and data.
- ***Report known or suspected instances of unauthorized access, use or disclosure of PHI, PII, and sensitive information.***

BROWN & TOLAND PHYSICIANS

System Access & Connectivity True-Up Opportunity

As BTP continues to evolve, we are offering a one-time opportunity to notify Information Technology (IT) of any security deficiencies before November 30, 2020 and work with the IT staff to resolve deficiencies and identify a corrective action plan. Examples of areas to disclose, but are not limited to the following:

- Sharing of credentials among workforce members.
- Notifying IT of third-party vendors who have access to PHI, PII, and sensitive information.
- Notifying IT of offshore staff and/or vendors who have access to PHI, PII, and sensitive information.
- Unencrypted devices which may house PHI, PII and sensitive information.

Please disclose these types of deficiencies in the box below.

Acknowledgement of the Confidentiality & Accountability Information Security Attestation is required by December 31, 2020. Please have an authorized practice leader complete and return to: cybersecurity@btmg.com, with a copy to compliance@btmg.com

If you have questions, please contact cybersecurity@btmg.com

Official Practice Name	Office Phone Number	
Mailing Address		
City	State	Zip Code
Name of Person Completing	Date Completed	
Title of Person Completing		
Disclosures to be made to BTP		