Information Security Questionnaire

For each item, please check the box if the security control is in place. For unchecked items, please attach pages as necessary describing (a) reason for not fulfilling (b) plans for fulfilling, and/or (c) alternate technologies or procedures used as compensating security controls.

Organization Name:

Organization Type:

Completed By:

Position:

Contact Name:

Contact Phone Number:

Contact Email Address:

Date:

General Security Controls

✓	
	UTSW reserves the right to perform external vulnerability scans without prior notice to ensure compliance with these standards. Results of your performed security audits may also be requested.
	Provide a proposed architecture document that includes a full network diagram of where there are integration points with UTSW. Illustrate the relationship between the environment and any other relevant networks (include ports/protocols), with a full data flowchart that details where UTSW data resides (include backup processes) and what data will be processed and collected (data inventory).
	Service involves PHI (BAA to be in place) or other protected information.
	All administrators and users can be individually identified (no generic accounts).
	In the event of a security breach, UTSW will be notified within 10 days of discovery of the breach or per HIPAA BAA.
	Organization was involved in a breach in the last 3 years where customers had to be notified.
	Security Penetration Testing is completed annually for public facing services.
	There is an employee Security and Privacy awareness training program.
	There is a technology risk assessment and risk management program in place.

	There is a senior level Information Security Officer responsible for your security program.
	Multi-Factor Authentication is required on public facing services (e.g., remote access, email).
	UTSW users are authenticated through centralized account administration (e.g., UTSW Active Directory).

Physical Security

	The data center is in a secure, environmentally controlled and protected facility with a locked cage-type rack environment.
	There are policies and procedures in place to log and limit personnel access to data and technology systems on a need to know role basis.

Network Security

	UTSW data is segmented from any other customer that you may have. This means the UTSW service environment is using separate hosts or separate infrastructure, or other appropriate security controls to maintain segmentation.
	Firewall technology is in place to control resource, data and service access.
	There are 24/7 monitored Intrusion Prevention and Detection systems in place.
	There are incident response processes.
	All authentication and data transmissions are encrypted using current best practices.

Host Security

	Hosts/devices comprising your infrastructure have been hardened against attack and are reviewed for potential security enhancements on a scheduled basis.
	There is a configuration management, security vulnerability and patch management program in place. Security patches are typically applied within 30 days.
	All software is on vendor supported versions (e.g., no end-of-life software).
	Anti-Virus software will be monitored and up to date for all supported systems.
	The infrastructure is monitored for integrity and availability.
	Accounts include strong password and account controls, and account disabling/termination processes when no longer needed. NIST guidelines are often utilized.

	Media containing UTSW data will be secured during transport (e.g., encrypted backups, secure tape vaulting).
	Media containing UTSW data is securely cleaned, degaussed or destroyed prior to disposal.
	All devices used for business have hard drive encryption (e.g., laptops, desktops, mobile devices, USB storage).

Web Security

	Security architecture has been validated through testing of authentication, authorization and accounting functions.
	Code reviews and web vulnerability assessments are performed for the explicit purposes of finding and remediating security vulnerabilities (e.g., OWASP 10, XSS, Injection).

Cryptography

	Connections that transmit sensitive information use current cryptographic technologies such as IPSec, TLS, SSH/SCP and systems are protected from Brute Force attacks.
	If in scope, Site to Site VPN will use Cisco IKEv2/IKEv1, AES256, SHA256/SHA1.

Technology Resiliency

	System redundancy, backup procedures and Incident Response plans are in place and tested at least annually.

Comments:

Signature: _____ Title: _____ Date: _____