MedTunnel HIPAA Compliance Matrix

Administrative Safegaurds	Implementation Specification *(R) = Required (A) = Addressable*	Description	MedTunnel Fulfilment
Security Management Process 164.308(a)(1)	Risk analysis (R)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	MedTunnel's applications are designed to protect private health information (PHI). We continuously review our internal and external security protocols and procedures.
	Risk management (R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	MedTunnel's applications are built around security. We continuously implement the latest security measures specifically to protect patient data.
	Sanction policy (R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	MedTunnel's infrastructure is such that no workforce member even at the CEO level can inadvertently or on with intent access any patient data.
	Information system activity review (R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	MedTunnel monitors the general activity on its servers and it has designed a detailed audit and logging report for its customers.
Assigned Security Responsibility 164.308(a)(2)	Security Official (R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Kishore Tipirneni MD, our CEO, is also in charge of security and has designed and implement many other HIPAA-compliant software applications that are used throughout the medical industry on a daily basis.
Workforce security 164.308(a)(3)	Authorization and/or supervision (A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	MedTunnel's infrastructure is such that no workforce member even at the CEO level can inadvertently or on with intent access any patient data.
	Workforce clearance procedure (A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	MedTunnel's infrastructure is such that no workforce member even at the CEO level can inadvertently or on with intent access any patient data.
	Termination procedure (A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3) (ii)(B) of this section.	Since no MedTunnel employee can access PHI, there is no need to terminate access upon the end of employment of a workforce member.
Information access management 164.308(a)(4)	Isolating healthcare clearinghouse function (R)	If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearing- house from unauthorized access by the larger organization.	MedTunnel has no clearinghouse functions.
	Access authorization (A)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	As MedTunnel does not permanently store PHI, the control of this function is at the level of the administrator for that account or group.

	Access establishment and modification (A)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	As MedTunnel does not permanently store PHI, the control of this function is at the level of the administrator for that account or group.
Security awareness and training 164.308(a)(5)	Security reminders (A)	Procedures for guarding against, detecting, and reporting malicious software.	At MedTunnel, we are intently focused on security and implement new security features on a regular basis.
	Protection from malicious software (A)	Procedures for guarding against, detecting, and reporting malicious software.	As MedTunnel only provides secure messaging applications, there is no threat of any malicious software or viruses affecting our closed system.
	Log-in monitoring (A)	Procedures for monitoring log-in attempts and reporting discrepancies.	At MedTunnel, we provide the tools so that the administrator for an account or group can set this policy.
	Password management (A)	Procedures for creating, changing, and safeguarding passwords.	At MedTunnel, we provide the tools so that the administrator for that account or group can set this policy.
Security incident procedures 164.308(a)(6)	Response and reporting (R)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	At MedTunnel, security is our primary focus and expertise. We have implemented a distributed solution that virtually eliminates risk of a potential breach while minimizing its impact. If there were to be a breach, appropriate reports would be made.
Contingency plan 164.308(a)(7)	Data back-up plan (R)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Since MedTunnel does not permanently store PHI and only acts as a secure conduit for PHI, all data should be backed up by the sender of the data.
	Disaster recovery plan (R)	Establish (and implement as needed) procedures to restore any loss of data.	Since MedTunnel does not permanently store PHI and only acts as a secure conduit for PHI, all data should be backed up by the sender of the data and the sender should have procedures to restore any loss of data.
	Emergency mode operation plan (R)	Establish (and implement as needed) procedures to enable the continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	As all data that passes through our MedTunnel servers is secure, we do not need to make any operational changes for an emergency.
	Testing and revision procedure (A)	Implement procedures for periodic testing and revision of contingency plans.	MedTunnel has a continuous process to improve the availability of our service.
	Applications and data criticality analysis (A)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	MedTunnel provides secure messaging applications. We constantly assess various components of the system and make contingency plans.
Evaluation 164.308(a)(8)	Technical and non-technical evaluation (R	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	At MedTunnel, security is our primary focus and expertise. We are constantly evaluating all security procedures.

Business associate contracts and other arrangements 164.308(b)(1)	Written contract or other arrangement (R)	Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	As MedTunnel is strictly a **conduit** and we do not even access the information that passes through our servers on a random or infrequent basis, we do not even meet the minimum requirements (as noted in the Federal Register, Vol. 75, No. 134, p. 40873) to be considered a Business Associate.
Facility access controls 164.310(a)(1)	Contingency operations (A)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	At MedTunnel, our cloud servers are under an SSAE-16 Compliant cloud service provider.
	Facility security plan (A)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	MedTunnel does not keep or store PHI in our office. All data is securely routed and passes directly through our SSAE-16 Compliant cloud servers.
	Access control and validation procedures (A)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Since there are no paper or digital PHI records stored in the MedTunnel office, we do not need to enforce these stringent policies; front desk based controls are implemented. Data Center access controls follow SSAE-16 standards and procedures as well as industry best practices.
	Maintenance records (A)	Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).	Since there are no paper or digital PHI records stored in the MedTunnel office, this standard does not apply to us.
Workstation use 164.310(b)	Function and attributes (R)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	At MedTunnel, we only provide the application and not the hardware so this standard does not apply to us.
Workstation security 164.310(c)	Restrict access (R)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	At MedTunnel, we provide the tools so that the administrator for that account or group can implement appropriate password protection and automatic system logoff.
Device and media controls 164.310(d)(1)	Disposal (R)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	As MedTunnel does not permanently store PHI, this standard does not apply to us.

	Media re-use (R)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	As MedTunnel does not permanently store PHI, this standard does not apply to us. However, we are able to advise our customers on how to do this.
	Unique user identification (R)	Assign a unique name and/or number for identifying and tracking user identity.	MedTunnel's secure messaging applications assign a unique MedTunnel ID to each user so that they are the only ones who can decrypt the messages received.
	Emergency access procedure (R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	MedTunnel's secure messaging applications are realtime and allows users to access data no matter where they are located as long as there is network connectivity.
	Automatic log-off (A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	MedTunnel's secure messaging applications the end user to set the auto-logoff settings.
	Encryption and decryption (A)	Implement a mechanism to encrypt and decrypt electronic protected health information.	MedTunnel's secure messaging applications provide true end-to-end encryption. Message traffic is encrypted with 2048 bit RSA keys as wells as with a 256 bit AES-CBC. The sender encrypts the message and only the intended receiver can decrypt the message.
Audit controls 164.312(b)	(R)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	At MedTunnel, we provide the tools so that the account owner or group administrator can monitor system usage.
Integrity 164.312(b)	Mechanism to authenticate electronic protected health information (A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	As MedTunnel does not have access to PHI, this standard does not apply to us.
Person or entity authentication 164.312(d)	(R)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	At MedTunnel, we provide the tools so that the account owner or administrator for a group can control access to the PHI.
Transmission security 164.312(e)(1)	Integrity controls (A)	Implement security measure to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	The integrity of the PHI transmitted within our secure messages is automatically maintained due to their end-to-end encryption.
	Encryption (A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	All data sent using a MedTunnel application is end-to-end encrypted and uses SSL/TLS between the client and our cloud server.