WHITE PAPER

Building HIPAA Compliant Chat

Twilio & Virgil Security

1. INTRODUCTION

Twilio is a cloud communications platform delivered via easy-to-use APIs available for most platforms and languages. Twilio provides Voice, Video, Messaging, and Authentication APIs.

Virgil Security's easy-to-use cryptographic software and key management APIs enable enhanced privacy and security across any platform, programming language, or deployment scenario. Virgil empowers developers with minimal to no cryptographic training to meet fundamental security requirements as well as enabling multiple regulatory frameworks that mandate information security.

2. HIPAA BACKGROUND

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which was updated in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH), included provisions that required the U.S. Department of Health and Human Services ("HHS") to adopt national standards for electronic healthcare transactions. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy and security protections for individually identifiable health information. These are embodied in the Privacy Rule, Security Rule, and Breach Notification Rule.

The HIPAA Privacy Rule set national standards for the protection of Protected Health Information ("PHI"). PHI is individually identifiable health information transmitted or maintained in any form by the three types of covered entities (health plans, health care clearinghouses, and health care providers), who conduct certain health care transactions electronically, and their business associates. The Privacy Rule established a foundation of Federal protections for the privacy of PHI. The Rule does not replace Federal, State, or other law that grants individuals even greater privacy protections, and covered entities are free to retain or adopt more protective policies or practices.

The HIPAA Security Rule establishes national standards to protect individuals' electronic PHI ("ePHI") that is created, received, used, or maintained by a covered entity or their business associates. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.

The HIPAA Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI.

3. VIRGIL SECURITY'S TECHNOLOGY

The Virgil solution features ease of use and the ability to seamlessly integrate privacy, security, and authentication into your HIPAA-regulated applications. In particular, the Virgil Stack includes cryptographic libraries that operate in conjunction with a global cloud-based key management infrastructure-as-a-service that allows developers to add security to their products in hours instead of weeks or months—all without having to become security experts themselves.

These features include:

A. EPHEMERAL KEY PAIR GENERATION

- Random number generation function according to NIST Special Publication (SP) 800-901 that uses a counter-mode block-cipher-based Deterministic Random Bit Generator. This is the underlying algorithm used is AES-256 in counter mode.
- Random number generation function with a "Personalization String" parameter according to NIST SP 800-90A..
- Entropy function – provided by specific features in various operating systems and hardware configurations (although direct support not always available).

B. KEY AGREEMENT

- Key Agreement, which uses Elliptic Curve Diffie–Hellman (ECDH) for the generation of a shared secret by two parties.

C. KEY DERIVATION FUNCTION

- Key Derivation Function (KDF), which produces a set of keys from keying material and some optional parameters.
- KDF1 (A Virgil implementation of the "Key Derivation Function 1" process described in ISO-18033-2). The underlying hash function is SHA-384.

D. SYMMETRIC ENCRYPTION ALGORITHM

- A hardware-specific implementation of AES256-GCM mode is used.

E. MESSAGE AUTHENTICATION CODE (MAC)

- Message Authentication Code, which produces data used to authenticate messages.
- ARM mbed TLS implementation of HMAC-SHA384.

4. HOW DO TWILIO AND VIRGIL SUPPORT HIPAA COMPLIANCE?

The Virgil Stack provides end-to-end encryption, passwordless authentication using public/private key cryptography, and secure communications to protect ePHI and as an access control mechanism. As shown in the table below, these features can support a wide variety of HIPAA requirements.

Twilio provides a communications platform over which end-to-end encrypted information travels and can optionally be stored. As the data is encrypted the entire time it travels over or is stored on Twilio's platform and as Twilio has no ability to decrypt the data, the communications data is not considered PHI while it is on the Twilio platform. In fact, Virgil has obtained an expert opinion that that the method of encryption it uses de-identifies the data in accordance with the HIPAA Privacy Rule (See §164.514(b)(1) of the HIPAA privacy rule.) For more information, please contact Josh Marpet (jmarpet@cybergrc.com) or Dmitry Dain (ddain@virgilsecurity.com). Because the data, while on Twilio's platform, is not PHI, Twilio is not involved in the use or disclosure of PHI, and therefore Twilio is not a business associate in this context.

Third-party review of the Twilio and Virgil Security solution is available upon request from either Twilio, Inc. or Virgil Security, Inc.

5. HOW DO TWILIO AND VIRGIL SUPPORT HIPAA SECURITY RULE REQUIREMENTS

Here are some of the key mechanisms that Twilio and Virgil Security offer to address compliance with these requirements.

ADMINISTRATIVE PROCEDURES AND TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY *(See attached chart).*

> As outlined in the chart attached to this whitepaper, Twilio and Virgil provide developers with a variety of ways to support HIPAA Security Rule compliance. Secure Programmable Chat ensures that employees' communications and healthcare providers' access to patient information can be made secure. Only patients and their healthcare providers are able to access the patient information. All "at rest" data is stored encrypted. As Twilio and all other intermediary cloud and communications providers are not able to access the patient information, this helps prevent security violations thereby enabling compliance with HIPAA Security Rule Requirements.
>
> End-to-end encryption enables data security in the cloud protecting patient ePHI, health care provider communications, healthcare records, and other information classified as ePHI.

Twilio and Virgil Security make developing HIPAA Security Rule compliant applications simple for developers to implement and transparent to the end users.

6. HOW DO TWILIO AND VIRGIL SUPPORT HIPAA PRIVACY RULE REQUIREMENTS

Here are some of the key mechanisms that Twilio and Virgil Security offer to address compliance with these requirements.

NOT USE OR FURTHER DISCLOSE PHI OTHER THAN AS PERMITTED OR REQUIRED BY THE CONTRACT OR AS REQUIRED BY LAW. (164.502)

Secure Programmable Chat ensures that employee and patient/provider communications can be made secure and only authorized parties are able to view information even if a breach of the cloud infrastructure has occurred. Twilio and Virgil APIs can provide an effective way to verify user identity and assist in ensuring only those who have valid authorization to use information have access to that information. Virgil's encryption technology assists in keeping unauthorized users from gaining access to PHI thereby eliminating the healthcare provider from data at rest exposure.

USE APPROPRIATE SAFEGUARDS TO PREVENT USE OR DISCLOSURE OF THE INFORMATION OTHER THAN AS PROVIDED FOR BY ITS CONTRACT. (164.504)

The Twilio and Virgil Security APIs provide strong protections that can be utilized to assist in meeting HIPAA contractual obligations required under Business Associate Agreements (BAA). Cryptographic standards use to encrypt information conform to all aspects of NSA Suite B and are suitable for use in healthcare ePHI scenarios.

REPORT TO THE COVERED ENTITY ANY USE OR DISCLOSURE OF THE INFORMATION NOT PROVIDED FOR BY ITS CONTRACT OF WHICH IT BECOMES AWARE. (164.504)

Both Twilio and Virgil provide developers with the ability to store and access audit logs and other metadata associated with the use of the APIs.

It is important to note that the user identity string, which you define in your application, is stored by Twilio in an unencrypted fashion. Therefore, these strings should not contain any PHI. As an example, if an email address or name constitutes PHI in your particular use case, you should not use those as the user identity string. Instead you could use a randomly generated alphanumeric string.

MAKE AVAILABLE PROTECTED HEALTH INFORMATION FOR AMENDMENT AND INCORPORATE ANY AMENDMENTS TO PROTECTED HEALTH INFORMATION (AN INDIVIDUAL HAS THE RIGHT TO HAVE A COVERED ENTITY AMEND PROTECTED HEALTH INFORMATION OR A RECORD ABOUT THE INDIVIDUAL). (164.526)

> With Secure Programmable Chat neither Twilio nor Virgil have the ability to decrypt the ePHI.

MAKE AVAILABLE THE INFORMATION REQUIRED TO PROVIDE AN ACCOUNTING OF DISCLOSURES (AN INDIVIDUAL HAS A RIGHT TO RECEIVE AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION MADE BY A COVERED ENTITY IN THE SIX YEARS PRIOR TO THE DATE ON WHICH THE ACCOUNTING IS REQUESTED). (164.528)

> With Secure Programmable Chat neither Twilio nor Virgil have the ability to decrypt the ePHI.

A COVERED ENTITY MUST HAVE IN PLACE APPROPRIATE ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS TO PROTECT THE PRIVACY OF PROTECTED HEALTH INFORMATION. A COVERED ENTITY MUST REASONABLY SAFEGUARD PHI FROM ANY INTENTIONAL OR UNINTENTIONAL USE OR DISCLOSURE THAT IS IN VIOLATION OF HIPAA. (164.530)

> The Twilio Programmable Chat API and Virgil Security cryptography API and Key Management API provide developers with everything they need to fulfill the technical and physical safeguards for Protected Health Information. Twilio 2FA Authy solution and Virgil Security's encryption technology assists in protecting unauthorized users from gaining access to information.

7. HOW DOES VIRGIL SUPPORT BREACH NOTIFICATION REQUIREMENTS?

Here are some of the key mechanism that Virgil offers to address compliance with these requirements.

FOLLOWING A BREACH OF UNSECURED PROTECTED HEALTH INFORMATION, COVERED ENTITIES MUST PROVIDE NOTIFICATION OF THE BREACH TO AFFECTED INDIVIDUALS, THE SECRETARY, AND, IN CERTAIN CIRCUMSTANCES, TO THE MEDIA. IN ADDITION, BUSINESS ASSOCIATES MUST NOTIFY COVERED ENTITIES IF A BREACH OCCURS AT OR BY THE BUSINESS ASSOCIATE.

> Virgil Security provides encryption technology that meets the HHS standards providing a safe harbor exception to the breach notification rule. If ePHI is protected with a level of encryption that meets HHS standards, the loss of encrypted data does not constitute a reportable breach under HIPAA. Virgil encryption

> will assist companies in ensuring that minor security incidents that may occur do not result in reportable HIPAA breaches. All information being transmitted over Twilio communications platforms is always end-to-end encrypted using NSA Suite B cryptography.

Please note that Twilio and Virgil are providing this information only as a courtesy, and this does not constitute the provision of legal advice. This information should not be used as a substitute for obtaining legal advice from a licensed attorney with appropriate expertise and authorization to practice in your jurisdiction. Twilio and Virgil are not in a position to interpret any laws, rules, or regulations on behalf of its customers or other third parties. You should consult with your legal advisors to ensure that your use of Virgil Security and Twilio Programmable Chat is compliant with HIPAA and all other applicable laws, regulations, and requirements.

ADMINISTRATIVE SAFEGAURDS

Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	**Risk Management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.	Required 164.308(a)(1)(ii)(B)	• **Secure Programmable Chat:** Healthcare provider to patient communications are encrypted and prevent access violations • **Identity Authentication:** ensures only those who have valid authorization to use information have access to it • **Encryption technology:** protects data access from unauthorized users
Workforce Security: Implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI and to prevent those workforce members who should not have access from obtaining access to ePHI.	**Authorization and/or Supervision:** Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where ePHI might be accessed.	Addressable 164.308(a)(3)(ii)(A)	• **Identity Authentication:** ensures only those who have valid authorization to use information have access to it. Authy 2FA, Virgil Passwordless Token
Information Access Management: Implement policies and procedures for authorizing access to ePHI.	**Isolating HC Clearinghouse Functions:** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	Required 164.308(a)(4)(ii)(A)	• **Identity authentication:** ensures only those who have valid authorization to use information have access to it • **Encryption technology:** protects violations from unauthorized users
	Access Authorization: Implement policies and procedures for granting access to ePHI.	Addressable 164.308(a)(4)(ii)(B)	• **Identity authentication:** ensures only those who have valid authorization to use information have access to it
Security Incident Procedures: Implement policies and procedures to address security incidents.	**Response and Reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents; and document security incidents and their outcomes.	Required 164.308(a)(6)(ii)	• **Secure Programmable Chat:** Healthcare provider to patient communications are encrypted and prevent access violations • **Identity authentication:** ensures only those who have valid authorization to use information have access to it • **Encryption technology:** protects violations from unauthorized users
Contingency Plan: Establish policies and procedures for responding to an emergency or other occurrence that damages systems containing ePHI.	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	Required 164.308(a)(7)(ii)(C)	• **Secure Programmable Chat:** Healthcare provider to patient communications are encrypted and prevent access violations • **Identity authentication:** ensures only those who have valid authorization to use information have access to it

TECHNICAL SAFEGAURDS

Access Control: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or programs that have been granted access rights.	**Encryption and Decryption:** Implement a mechanism to encrypt and decrypt ePHI.	Addressable 164.312(a)(2)(iv)	• **Encryption technology:** protects violations from unauthorized users
Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	**None**	164.312(b)	• Access to encrypted information is controlled through encryption keys • Access and usage of the keys is logged for audit
Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction	**Mechanism to Authenticate EPHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Addressable 164.312(c)(2)	• **Secure Programmable Chat:** Healthcare provider to patient communications are encrypted and prevent access violations • **Identity authentication:** ensures only those who have valid authorization to use information have access to it • **Encryption technology:** protects violations from unauthorized users
Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Evaluate Authentication Methods and select and implement authentication options	Required 164.312(d)	• **Secure Programmable Chat:** Healthcare provider to patient communications are encrypted and prevent access violations • **Identity authentication:** ensures only those who have valid authorization to use information have access to it • **Encryption technology:** protects violations from unauthorized users
Transmission Security: Implement technical security measures to guard against unauthorized access to ePHI that is transmitted across an electronic communications network.	**Integrity Controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Addressable 164.312(e)(2)(ii)	• **Secure Programmable Chat:** Healthcare provider to patient communications are encrypted and prevent access violations • **Identity authentication:** ensures only those who have valid authorization to use information have access to it • **Encryption technology:** protects violations from unauthorized users
	Encryption: Implement a mechanism to encrypt ePHI whenever appropriate.	Addressable 164.312(e)(2)(ii)	• **Encryption technology:** protects violations from unauthorized users