WHITEPAPER AND EXPERT OPINION

HOW TO BUILD HIPAA-COMPLIANT HEALTHCARE CHAT APPS WITH FIREBASE

Firebase + VIRGIL SECURITY

INTRODUCTION

Firebase gives developers the tools to develop high-quality apps, grow their user base and earn more money. The Firebase platform covers the essentials so developers can monetize their business and focus on their users.

The booming of the health & fitness tech industry made Firebase a strong choice for building health & fitness apps fast from the ground. Given the nature of the healthcare market, health & fitness apps implement in-app chat where doctors/caregivers and patients can connect with each other. While Firebase offers a fast & simple solution for building in-app chat, it lacks HIPAA compliancy, which forces healthcare app developers choose other platforms.

Virgil Security built an End-to-End Encryption SDK that's been used by many Twilio and Parse/Back4App customers world-wide to make their in-app chat functionality meet HIPAA requirements, despite their service providers not being HIPAA-compliant.

This whitepaper outlines an approach developers can take to build HIPAA-compliant chat apps using Firebase. In addition, it enables developers to start up fast with an Android, iOS and JavaScript chat app sample that's ready to use. For legal departments, the Appendix sections include details about the solution's HIPAA technical safeguards and an expert opinion that can be used for HIPAA audits.

The iOS and Android HIPAA-compliant Firebase Chat open source sample apps are available as part of the signup flow at https://VirgilSecurity.com/getstarted or on GitHub:

- iOS: https://github.com/VirgilSecurity/demo-firebase-ios
- Android: https://github.com/VirgilSecurity/demo-firebase-android
- JavaScript: coming soon

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.

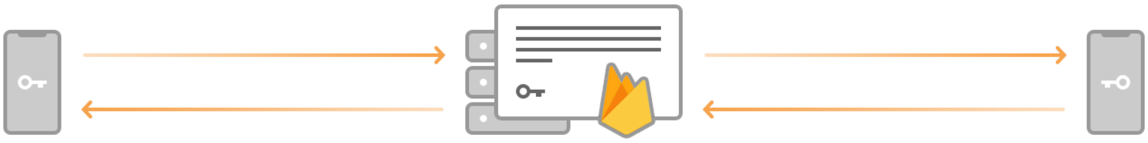
VIRGIL SECURITY'S TECHNOLOGY

Virgil's SDK features ease of use and the ability to seamlessly integrate privacy, security, and authentication into your HIPAA-regulated applications. The Virgil Stack includes cryptographic libraries across all major client platforms that operate in conjunction with a global cloud-based key management infrastructure-as-a-service that allows developers to add client-side encryption & End-to-End Security to their products in hours instead of months—all without having to become security experts themselves.

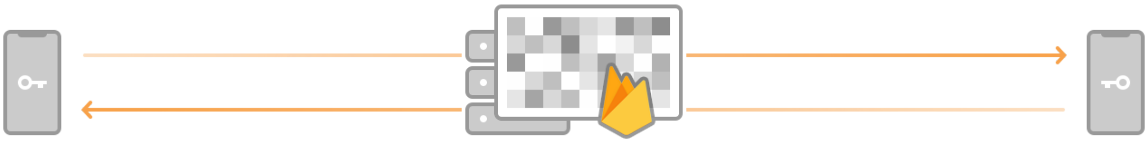
HOW DOES THE FIREBASE + VIRGIL CHAT APP SUPPORT HIPAA COMPLIANCE?

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 Appendix A, these features can support a wide variety of HIPAA requirements.

Firebase provides the platform over which end-to-end encrypted information travels between users. Chat messages are encrypted on user devices with keys that live exclusively on the device. As messages are encrypted the entire time they travel between users or while queued in Firestore for delivery, Firebase/Google/Virgil has no ability to decrypt the PHI data.



Standard app security: HTTPS + Data-at-Rest Encryption



End-to-End Encryption

Even though this technique ensures the perfect de-identification of PHI data and thus the inability to recognize even the nature of the encrypted data, HIPAA doesn't recognize it as one that exempts a vendor from complying with HIPAA (i.e. from signing a Business Associate Agreement). In order to make the solution comply with HIPAA, a second technique is applied: as soon as a chat message has been successfully delivered to the end-user, it's deleted from the Firestore server instance. This immediate and permanent, unrecoverable deletion (message redaction) enables the solution to meet HIPAA's Conduit Exception rule, which declares your in-app chat as a "courier" of health data. As per HIPAA's guidelines, the Conduit Exception rule exempts the entity from HIPAA (in the same way as UPS and other courier companies are exempt, too).

The combination of these 2 techniques ensure that patient data is end-to-end secured, is de-identified and not visible to any parties involved other than the appropriate end-users. Because of the message redaction implementation, the solution meets HIPAA's Conduit exception. This setup legally enables Google/Firebase/Virgil to not be involved in the use or disclosure of PHI, and therefore they're not a business associate in this context.

HOW DO FIREBASE AND VIRGIL SUPPORT HIPAA'S SECURITY RULE REQUIREMENTS?

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

Administrative procedures and technical security services to guard data integrity, confidentiality, and availability.

> As outlined in Appendix A, Firebase and Virgil provide developers with a variety of ways to support HIPAA's Security Rule compliance. The solution 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 Firebase 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's 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.
>
> Firebase and Virgil Security make developing HIPAA Security Rule compliant applications simple for developers to implement and transparent to the end users.

HOW DO FIREBASE AND VIRGIL SUPPORT HIPAA PRIVACY RULE REQUIREMENTS?

Here are some of the key mechanisms that Firebase 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)

> The solution 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. Firebase 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 Firebase 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 used 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 Firebase 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 Firebase in an unencrypted fashion. Therefore, these strings should not contain any PHI (such as the patient's name or email address). Instead, we recommend the use of a unique username that doesn't translate to the user's personal details.

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 the solution, neither Firebase 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 the solution, neither Firebase 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 Firebase SDK/APIs and Virgil Security's cryptography and Key Management SDKs provide developers with everything they need to fulfill the technical and physical safeguards for Protected Health Information. Firebase's 2FA solution and Virgil Security's encryption technology assists in protecting unauthorized users from gaining access to information.

HOW DOES VIRGIL SUPPORT BREACH NOTIFICATION REQUIREMENTS?

Here are some of the key mechanisms 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 by providing an expert determination method 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's 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 Firebase communications platforms is always end-to- end encrypted using NSA Suite B cryptography.

Please note that Firebase 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. Firebase 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 Firebase IP Messaging is compliant with HIPAA and all other applicable laws, regulations, and requirements.*

APPENDIX A: TECHNICAL SAFEGUARDS

CATEGORY	TOPIC	POSITION	SOLUTION
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 Messaging**: 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. Firebase 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
	Identity authentication: ensures only those who have valid authorization to use information have access to it • Encryption technology: protects violations from unauthorized users	*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 messaging**: 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	**Emergency Mode Operation Plan**: Establish and implement procedures	*Required 164.308(a)(7)(ii)(C)*	**Secure messaging**: Healthcare provider to patient communications are encrypted and prevent access violations

to an emergency or other occurrence that damages systems containing ePHI.	to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.		**Identity authentication**: ensures only those who have valid authorization to use information have access to it
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 messaging**: 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 messaging**: 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 messaging**: 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

APPENDIX B: DATA PRIVACY EXPERT OPINION

Virgil Security, working with Twilio, Google Firebase, and other vendors, has designed a methodology and functionality for an end-to-end encrypted messaging system. This messaging system can be utilized for many different functions, from a simple chat app, to an enterprise grade messaging ecosystem. This document is the data privacy expert's opinion on how the Virgil Security-integrated End-to-End Encrypted Firebase medical chat app satisfies HIPAA's (Health Insurance Portability and Accountability Act of 1996) requirements for medical use-cases, using the combination of the following 3 implementations:

1. Data security using End-to-End Encryption to ensure that patient data isn't available to 3rd-parties (not even to the vendor who's hosting the medical app)

2. How End-to-End Encryption fits within HIPAA's data de-identification standards

3. How the solution implements the Conduit exception, which ensures that even End-to-End Encrypted data isn't stored after it's been delivered and therefore, makes the solution exempt of HIPAA requirements.

The combination of these 3 features enable the medical chat solution to be HIPAA-compliant by taking advantage of the exemption that the Conduit exception grants.

DATA SECURITY USING END-TO-END ENCRYPTION

In the various iterations of Virgil Security functionality, the "keys" (elliptic curve private keys, used for decryption) are held on the individual devices operated by the end-users. The end users have physical and logical possession of the keys and therefore, they also have the responsibility for authorizing various people to utilize the data, encrypted with those keys.[1]

One of the use cases for this encrypted messaging system is medical messaging. Medical messaging is the passing of information from doctor to patient, patient to lab, lab to doctor, etc. Any medical messaging system, which does or could potentially pass ePHI (Electronic Personal Health Information), must follow standards as to the security of the health information.

While there are many parts to the HIPAA standard, the idea of "encryption in transit and at rest" is a key one for the Virgil Security Messaging System. Essentially, every message should be encrypted while in storage, or on a device (at "rest"), and should be encrypted while being transmitted and received from one device to another (in "transit").

OPINION ON ENCRYPTION ALGORITHMS USED

According to Virgil Security, AES-256 GCM encryption is used in their open source SDK to encrypt the messages in question. AES-256 GCM encryption is a fast, efficient, symmetric cipher, able to be used with mobile devices, as well as standard computing hardware. It's also transmission efficient, without bottlenecks that hinder several other types of AES. [1]

In terms of using it commercially and governmentally, NIST put AES through a battery of tests, trials, and standardizations. As NIST is responsible for developing Federal Information Processing Standards, or "FIPS", their guidelines on encryption are authoritative with regards to HIPAA and other federally regulated information security standards. [2] [3]

NIST certified AES with varying bit lengths to use for commercial applications. For governmental use, the Information Assurance Directorate, a division of the National Security Agency, certified AES-256 as accepted and encouraged for use by the federal government, as part of the Suite B algorithms, to use in encrypting information up to Top Secret. [4]

PATIENT DATA DE-IDENTIFICATION USING THE HIPAA "EXPERT DETERMINATION METHOD"

There is a formal standard around encryption of information so as to remove all individual information from the data set.[6] There are 2 methodologies to check the de-individuation listed:

1. **Methodology 1 - the "Safe Harbor" method:** with 18 categories of information that must be removed from the data in order to call the data de-identified. In the case of the Virgil Security Messaging System, while the message data is encrypted, the metadata, such as the destination address (IP address of end-user), is not encrypted. With the routing and delivery instructions/metadata (IP address of end-user) un-encrypted, the Safe Harbor method is unavailable to the Virgil Security Messaging solution.

2. **Methodology 2 - the "Expert Determination method"**: which requires an expert in information, information security, mathematics, etc, to examine sample data, and opine that no individuating data is left in the sample data, and that it is not possible to re-individuate that data.

> In §164.514(b), the Expert Determination method for de-identification is defined as follows:
>
> ○ (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
>
> ○ (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

- ○ (ii) Documents the methods and results of the analysis that justify such determination

VIRGIL SECURITY’S FIREBASE MESSAGING SOLUTION MEETS THE EXPERT DETERMINATION METHOD’S REQUIREMENTS.

AES-256 GCM is a highly secure algorithm to encrypt information so that it cannot be read or understood without the proper decryption key. As per the Information Assurance Directorate of the NSA, a properly implemented AES-256 is authorized for any type of information up to and including Top Secret. From a security perspective, ePHI is definitely within that spectrum.

From an information obscurity standpoint, a properly implemented AES-256 algorithm will encrypt cleartext, to the point that no frequency analysis, no viewing of the ciphertext, and no “eyeball” analysis of the ciphertext, will allow the extraction of any of the cleartext information from the ciphertext. A properly encrypted message will resemble random “noise”, with no meaning or understanding possible, without a proper decryption key.

While there are attacks possible on AES-256, such as a physical attack on a key6, the message itself is absolutely indistinguishable from randomly generated characters and therefore, in combination with Virgil’s user-device-stored-keys technique, it meets the Expert Determination Method’s requirements.

CONDUIT EXCEPTION USING DATA REDACTION

The use of the Conduit Exception[5] was discussed, wherein a transmission-only, no-view set of services are the only services given from the Cloud Service Provider to the covered entities or business associates.

The conduit exception applies where the *only* services provided to a covered entity or business associate customer are for transmission of ePHI that do not involve any storage of the information other than on a temporary basis incident to the transmission service.[6]

The specifics of the service provided by Firebase are a transmission-only service, with no-view capability. The data, once encrypted using a strong encryption algorithm, is de-identified, as per an expert opinion determination in the previous section.

While Google’s Firebase support confirmed in a statement that data deleted from Firestore is permanently deleted from Firebase’s servers, the service doesn’t support an automatic data/message redaction (the immediate and permanent deletion of data as soon it’s delivered). Therefore, the implementation (as in the sample code) requires a positive action, implemented in code, to immediately delete and overwrite all data from the transmission of the encrypted messages. In the current, admittedly demonstration version of the code, all encrypted data is immediately deleted via a script as soon as transmission concludes. This is appropriate and proper, and within the scope of the conduit exception. However, if the script fails, or the demonstration code is changed when put into production, then this step may be overlooked, de-prioritized, or simply changed.

To summarize, the encrypted data is definitely de-identified, both in transit and at rest. As for the Firebase system's ability to qualify for the conduit exception, while the intent of the Firebase code is to immediately delete all "left-over" data in the system, this is dependent on the code utilized in the application in question. The capability to immediately delete and overwrite the left-over data is inherently part of the Firebase codebase[7], and the Firebase Command Line Interface(CLI, a scriptable set of commands)[8].

This is not a built-in function to automatically delete all transient data, or to clearly overwrite it, thereby deleting or making unavailable, the content. This is a function that needs to be built as part of the messaging application, and verified by testing.

Effectively, and this is important, this means that every application, every usage of Firebase with Virgil Security's Messaging System, must be individually written to ensure the deletion or making the data unavailable, and must be tested individually, to certify that it does so. To be clear, the encryption of the data, and the encrypted form of the data, is absolutely de-identified, and not able to be re-individuated, or re-identified, without the private key. It is simply the transient data, pursuant to and as a result of transmission and reception of the encrypted data, that this caution applies to.

In English, this means that the development team for any application written on this Firebase/Virgil stack, must explicitly program a transient/metadata data deletion script into their application. Without this, it will not meet HIPAA Conduit Exception status. This feature is correctly implemented in the samples that are referenced in this opinion.

SUMMARY

The Firebase messaging application, as exemplified in the sample applications, meets HIPAA's data security requirements via the combination of the expert determination de-identification method and HIPAA's conduit exception.

EXPERT BACKGROUND

Joshua Marpet is an internationally recognized Information Security and Forensics Expert. He has had testimony accepted by the Turkish Supreme court, and has been Daubert tested, been deposed and testified for forensic cases in the US. Joshua has testified on Medical information, medical digital forensics, and multiple other issues. He has taught, at the university level, digital forensics, information security ethics, linux, encryption, and many other topics.

Joshua is currently the Chief Operating Officer for Red Lion, LLC, an information security consulting firm. He handles the compliance and governance issues for multiple clients, including hedge funds, family offices, governmental clients, and retail conglomerates, among others.

---

[1] For a fairly complete explanation of AES-256 GCM - https://en.wikipedia.org/wiki/Galois/Counter_Mode, or for a slightly more digestible explanation of AES in general, http://www.moserware.com/2009/09/stick- figure-guide-to-advanced.html

[2] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

[4] https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

[5] In some iterations/configurations of the Virgil System, there can be administrative key(s), which allows decryption of messages without the end user's authorization. In the iterations discussed in this opinion paper, that is not the case.

[6] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

[7] https://www.dropbox.com/s/78bqa0ddefvjhnd/Brief%20on%20Virgil%20Security%E2%80%99s%20de-identification%20practice.pdf?dl=0

[8] This is, of course, as per the current state of the art in cryptography, quantum cryptography, mathematics, and digital forensics. Any significant breakthrough in any or all of those fields could change the effectiveness of this opinion.

[9] https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Section3

[10] *ibid.*

[11] https://firebase.google.com/docs/firestore/manage-data/delete-data

[12] https://firebase.google.com/docs/cli/ - There are mentions of

“Database:remove, [which will] Delete all data at a specified location in the current project's database”, as well as” Firestore:delete[, which will] Delete documents in Cloud Firestore. With the Firebase CLI, you can use recursive deletes to delete all the documents in a collection.”