hippo™ WHITE PAPER

Compliance + Data Security Standards

FOR VIRTUAL CARE

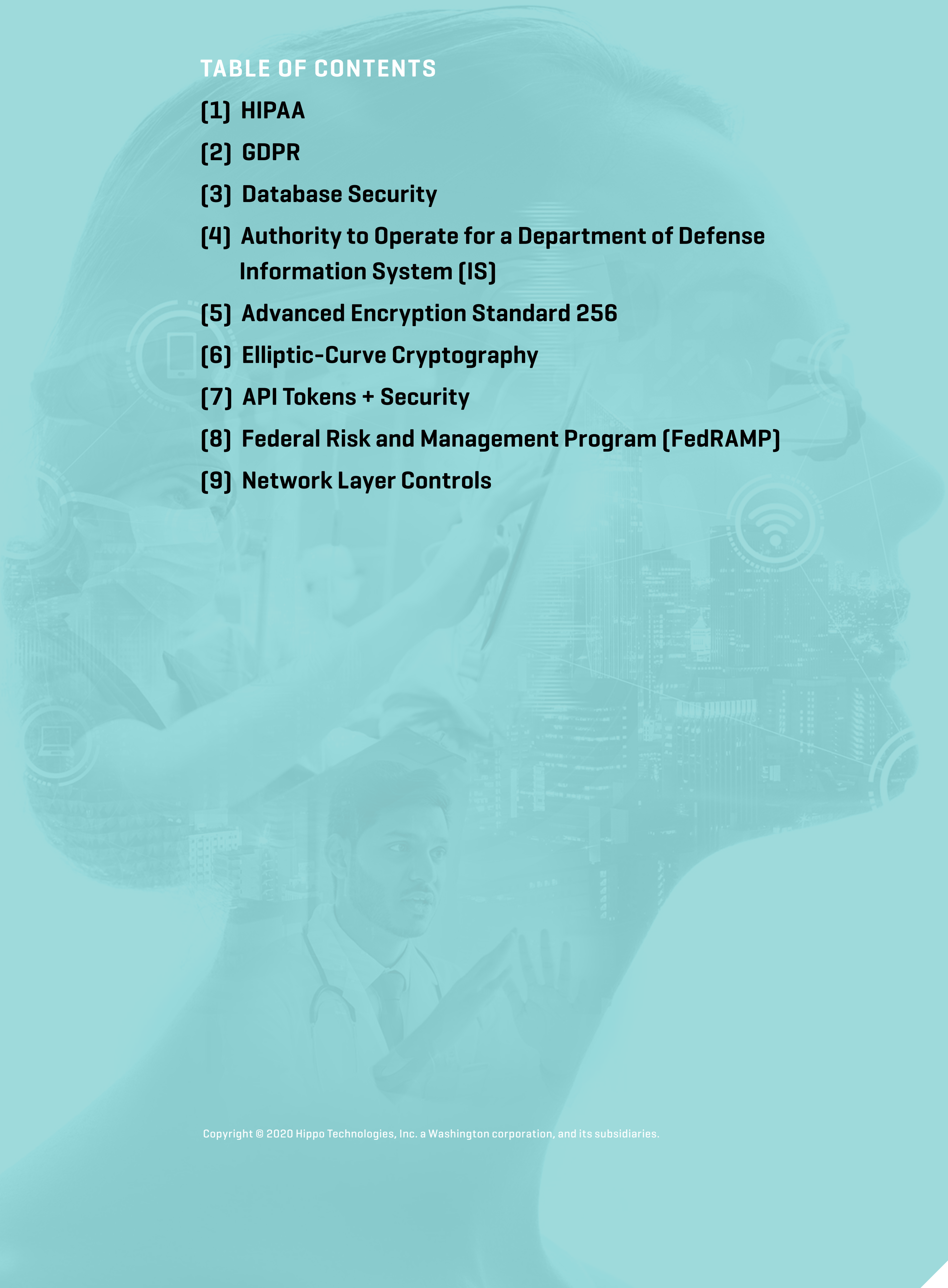


TABLE OF CONTENTS

Copyright © 2020 Hippo Technologies, Inc. a Washington corporation, and its subsidiaries.

> “The global pandemic has effectively opened the floodgates to a wave of new telehealth solutions. Against this background of unprecedented deregulation, it’s more critical than ever that we cast a spotlight on compliance and data security in this new era of Virtual Care.”
>
> **Patrick Quinlan, MD**
> CEO, Hippo Technologies Inc.

INTRODUCTION

Back in early January 2020, most Americans barely paid attention to COVID-19. In those early months it was merely something newsworthy that was happening in China.

However, shortly thereafter, things got real for the rest of the world, and they got real in a hurry as suddenly the impact of the pandemic was felt worldwide.

There is an old saying that “necessity is the mother of invention” – meaning that when the need for something becomes critical, we as humans are forced to figure out how to do it.

In the case of COVID-19, these uncertain times have created opportunities for innovation as industries have been forced to change extremely quickly. This includes healthcare and being able to provide on-demand virtual care, distance-based learning and clinical support in a world where physical separation is encouraged, if not mandated.

Ever since the beginning of the pandemic, Virtual Care went from a “nice to have” to a “must have” almost overnight as institutions needed technological solutions to help them survive and thrive during these unprecedented times. Despite the sudden rush to apply technology to Virtual Care, one theme remains critical for Virtual Care to both proliferate and succeed – and that is the need for compliance, data security and safeguarding patient privacy.

This sudden move to Virtual Care, along with changes in standards put these topics at the top of the agenda in terms of mission critical tasks that institutions must focus on. In healthcare, compliance standards such as GDPR and HIPAA are keeping a watchful eye to ensure that institutions are addressing compliance, data security and patient privacy as they innovate at breakneck pace.

So, the question is – what does this mean for you and your organization and how can you keep on track and up to date?

The answer is two-fold:

(1) Become as educated as possible on the subject matter; and

(2) Make sure that you are aligned with the proper technology tools.

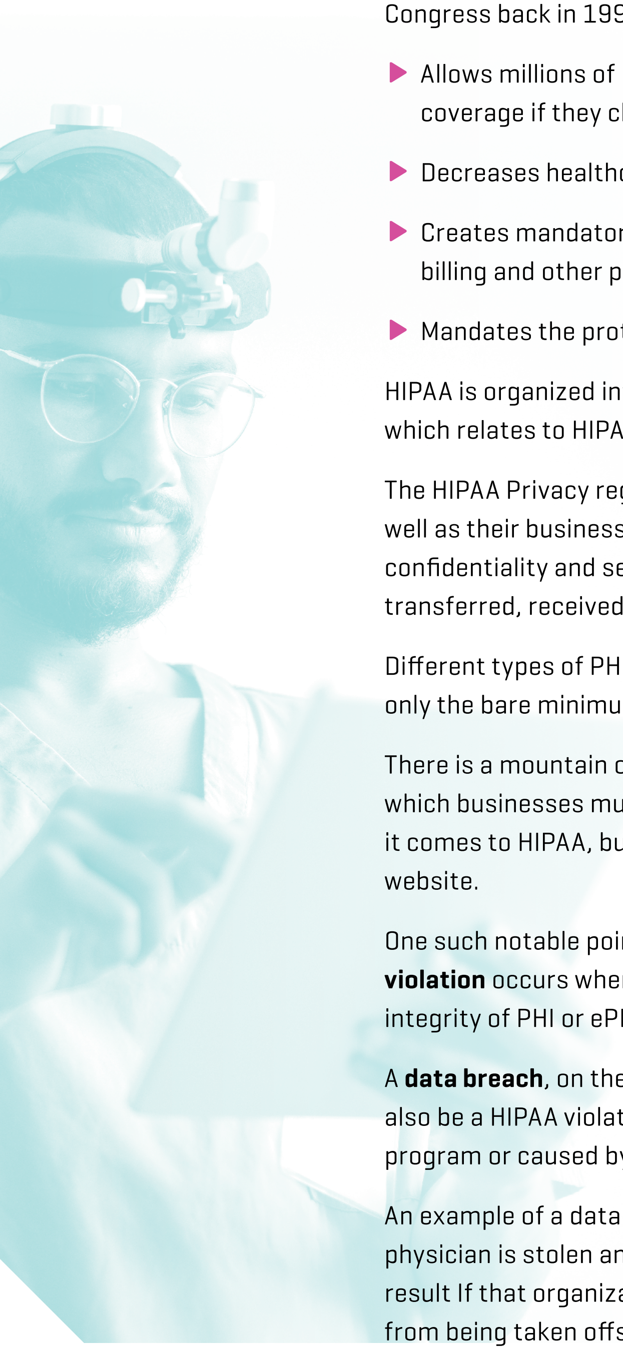
Let’s begin with education by learning more about some of the best-in-class Compliance and Data Security Standards in healthcare by looking at what they mean and why they are important as it relates to the rapidly expanding world of Virtual Care.

1
HIPAA
Health Insurance Portability and Accountability Act

WHAT DOES IT MEAN?

HIPAA stands for the Health Insurance Portability and Accountability Act which was passed by Congress back in 1996. It does the following:

- Allows millions of US workers and their families to transfer and continue health insurance coverage if they change or lose their jobs;
- Decreases healthcare fraud and abuse;
- Creates mandatory industry-wide standards for healthcare information regarding electronic billing and other processes; and
- Mandates the protection and confidential handling of protected health information.



HIPAA is organized into two different “Titles”; the one we will be focusing on in this paper is the latter which relates to HIPAA Privacy or ***Protection and Confidential Handling of Health Information.***

The HIPAA Privacy regulations mandate that both healthcare providers and organizations, as well as their business associates, must create and adhere to procedures which ensure both the confidentiality and security of protected health information (PHI) at all times – meaning when it is transferred, received, handled, and shared.

Different types of PHI that fall into this category include paper, oral, and electronic form. In addition, only the bare minimum of health information required to conduct business may be used or shared.

There is a mountain of information which must be digested when it comes to HIPAA guidelines which businesses must follow to be compliant. We will review a few of the more notable points when it comes to HIPAA, but for specific guidelines, we recommend that you consult the official HIPAA website.

One such notable point is the difference between a HIPAA violation and a data breach. A **HIPAA violation** occurs when there is a breach of an organization’s compliance program in which the integrity of PHI or ePHI becomes compromised.

A **data breach**, on the other hand, is different from a violation. While it is possible for a breach to also be a HIPAA violation, this only occurs if it is the result of a breakdown in the HIPPA compliance program or caused by a specific violation of the institution’s HIPAA policies.

An example of a data breach would be if a Head-mounted Device (HMD) belonging to an organization’s physician is stolen and that device has access to unencrypted medical records. A violation would result If that organization did not have a policy that stated HMDs and Smart Glasses were prohibited from being taken offsite.

WHY IS IT IMPORTANT?

- While there are many reasons why HIPAA is important, there are a few takeaways that are critical:
  - It helps ensure both privacy and confidentiality;
  - Gives patients access to their healthcare data; and
  - Decreases fraudulent activity while improving data systems.
- For healthcare institutions, HIPAA creates a valuable framework which safeguards who can access and view specific healthcare data while restricting access to whom that information is shared with.
- Furthermore, any organization that deals with PHI is required to also put into place physical, technical, and administrative safeguards to be compliant. This also includes subcontractors and other business associates.
- While HIPAA exists to safeguard individuals and to make sure everyone has access to a copy of their medical records, it also requires data protection for those who create, store, transmit or use health information that is individually identifiable.
- Those healthcare businesses and entities that handle, store, maintain, or transmit PHI are required to be in total compliance with the Security Rule of the HIPAA law.
- By following required HIPAA Rules, institutions will avoid liability associated with incorrectly managed security risks.

HIPAA + HIPPO

Hippo Virtual Care is fully HIPAA compliant; regular audits are conducted to identify possible risks for data. Hippo certifies each client installation post customization. The platform has been deployed on the AWS GovCloud for the US Department of Defense and Department of Veteran Affairs and is on-premises for the US Navy. Hippo Virtual Care and has also gone through a larger certification process for Authority to Operate (ATO) involving the implementation of 1,500-3,000 security controls.

2

GDPR
General Data Protection Regulation

WHAT DOES IT MEAN?

GDPR stands for General Data Protection Regulation and is a regulation in the EU which was adopted in April 2016 which replaced an obsolete data protection directive from 1995. It includes provisions that mandate businesses to protect the privacy and personal data of citizens of the EU which take place within EU member states. It also includes the transfer of personal data which occurs outside of the EU and European Economic Area. The GDPR is widely known as the most robust security and privacy law in the world.

The provisions of the GDPR are uniform across all 28 of the EU member states, which means that companies are required to meet a universal standard within the EU. That will include the UK post-Brexit, with the he UK Government confirming that it plans to continue GDPR post the transition period (December 31, 2020).

The GDPR protects a multitude of privacy data, including[3]:

- Information related to basic identity such as name, address and ID numbers
- Internet data such as IP address, location, cookie data, and RFID tags
- Health data
- Genetic data
- Biometric data
- Racial and ethnic data
- Political opinions
- Sexual orientation

Third-party processors should take note that GDPR places equal liability on those who own the data (data controllers) and external organizations who help manage the data (data processors). This means that when a third party data processor is not compliant, your organization is also considered not compliant.

What this essentially means is that each existing contract with data processors must spell out key responsibilities as well as define consistent processes which outline how data is to be managed and shared and how you will report breaches.

Failure to comply with GDPR may result in harsh penalties of up to €20 million or 4% of global annual turnover, whichever is higher.

However, a majority of the fines issued thus far have been relatively minor. Most of the fines levied to date have been in the low thousands and tens of thousands of euros range. The largest fine levied was against Google, for €50 million, which was issued due to lack of transparency and valid consent.

WHY IS IT IMPORTANT?

- There is a substantial public concern with respect to privacy in the EU. According to an RSA Data Privacy & Security Survey 2019 for which RSA surveyed 6,387 consumers in France, Germany, the UK and the US, 78% of consumers said lost banking and financial data is a top concern. Lost security information (e.g. passwords) was cited by 75% as a concern and identity information (e.g., passports or driving license) was cited as a concern of 70% of the respondents.[11]
- Another alarming stat coming from the same RSA report is that 64% of US respondents to the survey said they would blame the institution for their lost data in a breach rather than the hacker. The takeaway here is that as they become better educated, customers want more transparency and responsiveness from those who handle their data.
- Lastly, the report stated that "60% of all consumers surveyed on average find wearables intrusive. However, early adopters love them for their ability to help optimize diet, fitness, productivity, and other goals."[11]. This means that being GDPR compliant is absolutely critical in the virtual care space.

2

GDPR + HIPPO

Hippo Virtual Care is fully GDPR compliant. Regular audits are conducted to identify possible risks for data breaches or privacy violations. The certification is associated with each installation post customization. Hippo certifies each client installation post customization. The platform has been deployed on the AWS GovCloud for the US Department of Defense and Department of Veteran Affairs and is on-premises for the US Navy. Hippo Virtual Care and has also gone through a larger certification process for Authority to Operate (ATO) involving the implementation of 1,500-3,000 security controls.

3

Database Security

WHAT DOES IT MEAN?

Database security is comprised of a multitude of measures that organizations take which protect their databases from both external and internal threats. It includes the protection of that database itself, the data which it contains, the DBMS (database management system), as well as all of the applications which access the database.

It also refers to the various tools, controls and metrics which are used to establish and maintain the confidentiality, integrity and availability of the database.

Database security is a complex and demanding endeavor that incorporates many aspects of information security technologies and practices. Naturally, it is also at odds with database usability. The more usable and accessible a database is, the more it is vulnerable to security threats; and the more invulnerable it is to threats, the harder it is to access and use. You may have heard this paradox referred to as Andersons's Rule.

WHY IS IT IMPORTANT?

A data breach, defined as a failure to uphold the confidentiality of data in a database, can inflict many types of harm on an organization:

- **Intellectual property compromised** – Much of your competitive advantage may be tied to your intellectual property and if your information is stolen or exposed, it may be a challenge to maintain or recover that competitive advantage.
- **Brand reputation damaged** – Clients or partners may no longer want to do business with you if they feel they can no longer trust you with their data.
- **Business continuity** – Many businesses cannot resume operations until a breach is resolved.
- **Fines or penalties** – As we saw above, non-compliance with HIPAA and GDPR regulations can carry hefty and devastating fines.
- **Financial cost of repairing breaches/notifying customers** – In addition to the cost of communicating the breach with a customer, a breached institution must compensate for activities such as forensic and investigative processes, crisis management, repairing of affected systems etc.

3

DATABASE SECURITY + HIPPO

Hippo Virtual Care ensures security at all levels and we follow a "Zero Trust" policy for our server configurations. Security controls are implemented both at the application layer as well as at the network layer. All network access to the server is protected by a multi-layered firewall operating in a deny-all mode. Internet access is only permitted on explicitly opened ports for only a subset of specified virtual hosts.

4 Authority to Operate for a Department of Defense Information System (IS)

WHAT DOES IT MEAN?

A DoD ATO enables an organization to process, store, or transmit information on cybersecurity control standards of the DAA (Designated Accrediting Authority). It refers to Automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

WHY IS IT IMPORTANT?

Medical devices that are wirelessly connected to a system are a potential target for intrusion from hackers. The DoD is reducing cybersecurity risk by complying with strict Department of Defense cybersecurity standards. Compliance with these standards enables organizations to continue leveraging advanced interoperable medical technologies on maximum security level.

4

DOD ATO + HIPPO

Hippo Virtual Care has been granted ATO certification in compliance with the DoD's RMF Assessment & Authorization (A&A) process. The platform has been deployed on the AWS GovCloud for the US Department of Defense and Department of Veteran Affairs and is on-premises for the US Navy. Hippo Virtual Care has also gone through a larger certification process for Authority to Operate (ATO) involving the implementation of 1,500-3,000 security controls.

Advanced Encryption Standard 256

WHAT DOES IT MEAN?

AES is the first and only publicly accessible cipher approved by the US National Security Agency (NSA) for protecting top secret information. AES-256 supports the largest bit size and is practically unbreakable by brute force based on current computing power, making it the strongest encryption standard.

AES was created in response to the needs of the US government. Back in 1977, federal agencies used the Data Encryption Standard as their encryption algorithm. However, after being used successfully for almost 20 years, it became apparent that the DES was no longer adequately secure against brute force attacks. This meant that a much more sophisticated and robust encryption standard was needed.

To fill this need, the government created a public competition with the goal of finding a replacement system. After five years, 15 entries were pared down to five finalists, and a winner was eventually chosen.

In the end, something called the Rijndael cipher came out on top. A symmetric-key block cipher similar to DES but much more sophisticated, Rijndael was developed by—and named after—two Belgian cryptographers, Vincent Rijmen and Joan Daemen. In 2002, it was renamed the Advanced Encryption Standard and published by the US National Institute of Standards and Technology (NIST).[6]

The NSA approved the AES algorithm to handle top secret information not long after and soon the entire technology world took note. Since then, AES has become the gold standard for encryption with its open nature meaning that AES software is able to be used for public and private, as well as commercial and noncommercial implementations.

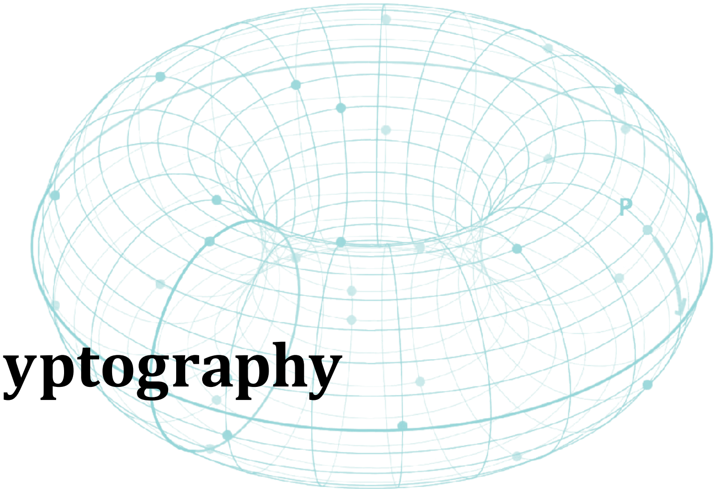
WHY IS IT IMPORTANT?

- AES 256 is basically impenetrable to those using brute-force methods. Where a 56-bit key can be cracked in less than 24 hours, it would take hackers billions of years to break AES using today's computing technology.
- Maximum secure encryption allows you to securely protect data from users that are not authorized.
- It helps protect private information, sensitive data, and can enhance the security of communication between client apps and servers.

AES-256 + HIPPO

Hippo Virtual Care provides secure messaging with AES 256 encryption and ECC (Elliptic Curve Cryptography) and is in compliance with security standards (HIPAA) in Healthcare for protecting sensitive patient data and personal health information (PHI). All data communication to/from servers is fully encrypted, both in transit as well as at rest.

Elliptic Curve Cryptography



WHAT DOES IT MEAN?

Elliptic curve cryptography (ECC) generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

ECC leverages the mathematical properties of elliptic curves to create a public key cryptographic system. As with all public key cryptography, ECC is built upon mathematical functions that are easy to compute in one direction, but much harder in reverse. According to SSL.com, "In the case of ECC, this difficulty resides in the infeasibility of computing the discrete logarithm of a random elliptic curve element with respect to a publicly known base point, or the 'elliptic curve discrete logarithm problem' (ECDLP). The Elliptic Curve Digital Signature Algorithm (ECDSA) is a widely-used signing algorithm for public key cryptography that uses ECC."[7]

The main difference in ECC from earlier cryptosystems is related to the key size in comparison with the cryptographic resistance. Interestingly, ECC provides the same cryptographic strength as the RSA system, but with much smaller keys. For example, a 256-bit ECC key is the same as a 3072-bit RSA key (which is 50% longer than the 2048-bit keys used today).

WHY IS IT IMPORTANT?

- ECC's smaller sizes result in stronger encryption being achieved with much less computing power, which is very advantageous for increasingly ubiquitous devices such as low-powered mobile and Internet of Things (IoT) devices.
- ECCs can be used to create faster, smaller, and more efficient cryptographic keys.
- ECCs provide a significantly more secure foundation than first-generation public key cryptography systems.
- ECCs help to establish equivalent security with lower computing power and battery resource usage; it is becoming widely used for mobile applications.

ELLIPTIC-CURVE CRYPTOGRAPHY + HIPPO

Hippo Virtual Care provides secure messaging with AES 256 encryption and ECC and is in compliance with security standards (HIPAA) in Healthcare for protecting sensitive patient data and personal health information (PHI). All data communication to/from servers is fully encrypted, both in transit as well as at rest.

API Tokens + Security

WHAT DOES IT MEAN?

An API is a tool set – a software intermediary used by programmers that allows two applications to talk to each other. To authorize access to those APIs, a request must include an access token or key.

WHY IS IT IMPORTANT?

- It is important to secure the API because businesses use it to connect services and to transfer data. Broken, exposed, or hacked APIs have resulted in major data breaches.
- As we saw earlier, those organizations who suffer a data breach can be faced with significant damage to their reputation as well as a public relations nightmare. And with HIPAA and GDPR, large fines can also be added to the consequences. Therefore, protecting against those types of attacks must be top of mind when it comes to API security.
- The major goal of API security is to prevent unauthorized access, which, in turn, may result in data breaches and business disruption.

API TOKENS AND SECURITY + HIPPO

Hippo Virtual Care takes advantage of advanced API Token security to protect Application Programming Interfaces. As the API provider, we can customize system-to-system access to meet your specific requirements

Federal Risk and Management Programs

HIPAA Security Risk Assessment and FedRAMP

WHAT DOES IT MEAN?

FedRAMP stands for the Federal Risk and Authorization Management Program, which is a cyber security risk management program for the purchase and use of cloud products and services used by US federal agencies.

More specifically, it is a government-wide program which creates a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. Similarly, the NIST Cybersecurity Framework provides a HIPAA Security Rule crosswalk. This standardized approach has cloud security solutions assessed once, with that assessment then used across multiple agencies.

FedRAMP revolves around NIST SP800-53, which is the best-practice standard for security control frameworks. More critically, FedRAMP allows for a clear and consistent means for cloud service providers, as well as customers across all industries, to measure security on an ongoing basis, and not only at a single point in time.

This movement to capitalize on the advantages of the cloud is not limited to federal agencies — far from it. FedRAMP was built to catalyze adoption within the federal government, but non-federal organizations are starting to reap its benefits as well, including critical infrastructure and business entities.

WHY IS IT IMPORTANT?

- Trustworthiness – having a third party verify that an organization has implemented various security features and functions creates a sense of trustworthiness.
- Demonstrates a commitment – satisfying the security requirements of both private and public sector organizations also shows a commitment to security.

FEDRAMP + HIPPO

For federal businesses, the HVC platform is hosted in the AWS.gov cloud and has been granted ATO and certified with FedRAMP for its standardized approach to security assessment. There are several requirements Hippo has completed to obtain a FedRAMP ATO:

- **Completion of FedRAMP documentation including the FedRAMP SSP**
- **Completion of a HIPAA Security Risk Assessment, as supported by the NIST Framework**
- **Implementation of controls that comply with FIPS 199 categorization**
- **Commercial cloud offerings are assessed by a FedRAMP Third Party Assessment Organization (3PAO)**
- **Development of a Plan of Action and Milestones (POA&M)**
- **Obtain Joint Authorization Board (JAB) Provisional ATO (P-ATO) or Agency ATO**
- **Implementation of a Continuous Monitoring (ConMon) program including monthly vulnerability scans**

9 Network Layer Controls

WHAT DOES IT MEAN?

The role of the Network Layer is to enable any two open systems to exchange data with one another, irrespective of the types of network the two systems are attached to and the means of interconnecting those two networks. It also controls the operation of the subnets.

WHY IS IT IMPORTANT?

Activating the various security characteristics included in this equipment is important for preventing unauthorized control of it. Use of strong passwords and correct configuration of management protocols through encrypted connections are some of the measures that can be taken to protect this.

9 NETWORK LAYER CONTROLS + HIPPO

Hippo Virtual Care provides high-level Network Layer Control mechanisms, for example in combination with its cloud service. Additionally, HVC performs Role-based Access Control (RBAC) to restrict network access based on individual roles.

10

Conclusion

As mentioned in the introduction, these rapidly changing times have created opportunities for innovation as healthcare organizations and the industries that support them have been required to pivot and move extremely quickly.

On the other hand, moving so quickly can open these organizations – particularly in the Virtual Care space – up to vulnerabilities when it comes to the need for compliance, data security and safeguarding patient privacy.

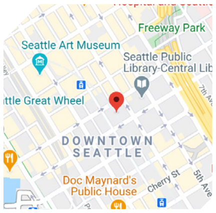
That's why having the right partner to accompany you in your Virtual Care journey is so critical. And as you have seen in each of the nine standards detailed above, Hippo goes above and beyond to ensure that when it comes to compliance, data security and safeguarding patient privacy, you are in the safest of hands.

▶ For further information on Hippo Technologies' Virtual Care solutions and our compliance and data security standards, contact **engage@myhippo.life**

hippo™ WHITE PAPER

Compliance + Data Security Standards

FOR VIRTUAL CARE

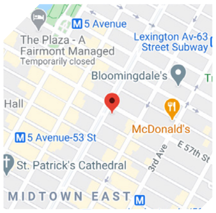


SEATTLE

1001 4th Avenue,
Suite 3200

Seattle, WA 98154

United States



NEW YORK

445 Park Avenue,
Suite 900

New York, New York 10022

United States

Hippo Technologies is delivering GDPR and HIPAA-compliant military grade solutions for virtual care and medical education. We are a clinician-led company bringing a combination of global medical practice and next generation technologies to transcend conventional boundaries of distance, time and training to serve patients and those who care for them.

1-877-HIPPO4U | 1-877-447-7648 | myhippo.life

REFERENCES

1 https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx

2 https://www.absolute.com/blog/what-is-hipaa-compliance-and-why-is-it-important-to-healthcare-security/

3 https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html?page=2

4 https://www.ibm.com/cloud/learn/database-security

5 https://smallbusiness.chron.com/authorization-operate-ato-81858.html

6 https://www.solarwindsmsp.com/blog/aes-256-encryption-algorithm

7 https://www.ssl.com/faqs/what-is-elliptic-curve-cryptography-ecc/

8 https://www.pingidentity.com/en/company/blog/posts/2019/advanced-api-security-4-lessons-to-protect-against-data-breaches.html

9 https://www.darkreading.com/cloud/why-fedramp-matters-to-non-federal-organizations/a/d-id/1334849v

10 https://www.welivesecurity.com/2015/06/30/strengthening-the-different-layers-of-it-networks/

11 https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf