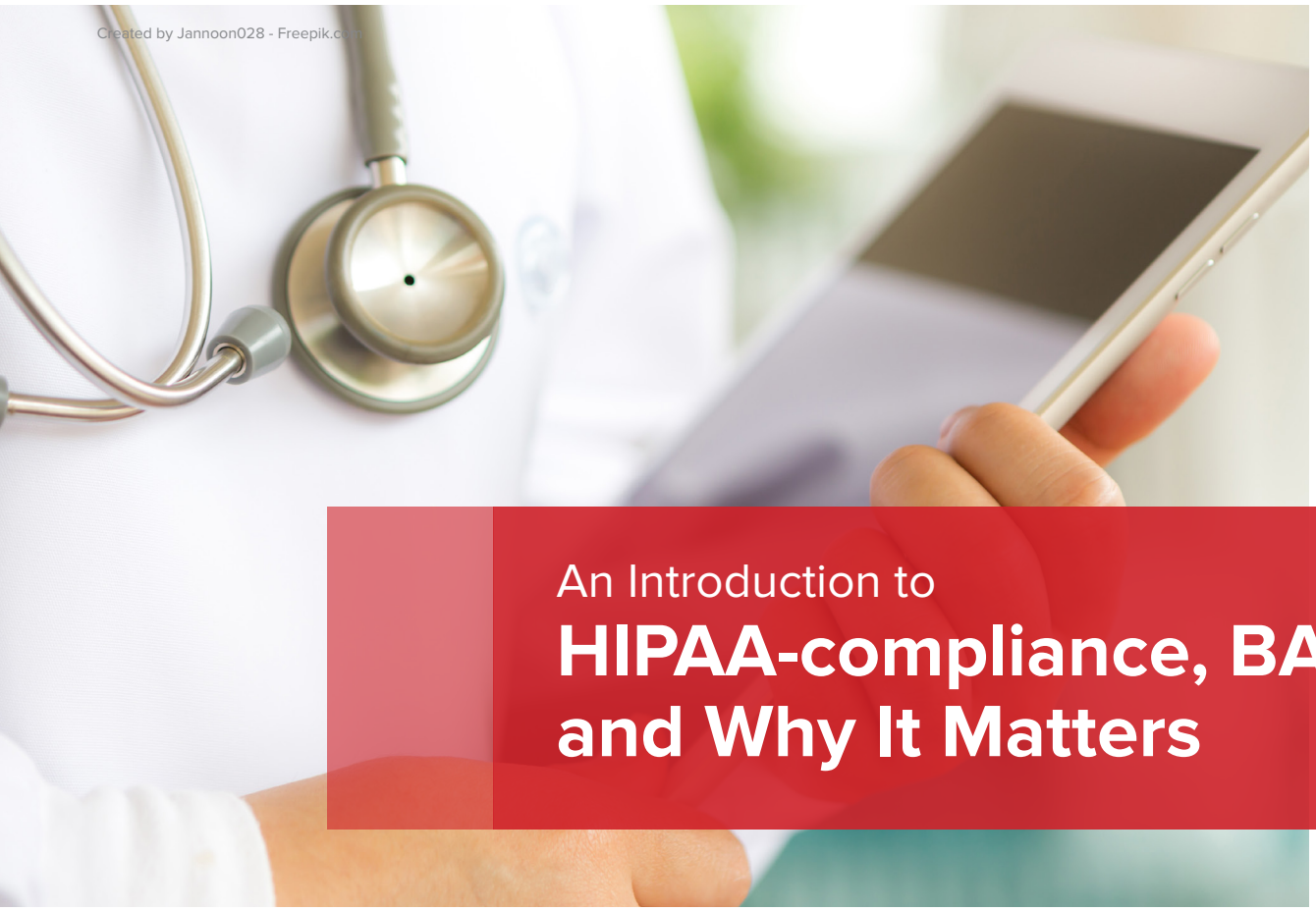
PubNub

SO YOU'RE BUILDING A HIPAA-COMPLIANT APP. . .



An Introduction to

HIPAA-compliance, BAAs and Why It Matters

PubNub

INTRODUCTION

So you're looking to enter the healthcare market with a new, innovative app to transform an industry ripe for disruption? Well, you've come to the right place.

Building and launching healthcare applications is different from other industries. Why? Compliance and security. Any app that handles electronic Protected Health Information (ePHI), in any way, is highly regulated, and for good reason.

Healthcare data breaches continue to grow, which can lead to lawsuits, revenue loss, and brand damage. It seems there are new fines being announced each month - Cottage Health was fined $2 million in October 2017 for violations which included failure to encrypt data[1], Metro Community Provider Network was fined $5.5 million for poor record keeping and not having processes such as audit logs, access reports, and security incident tracking reports[2]. Whether it's healthcare organizations themselves, or a third-party app integrated into their organization, all are vulnerable. In fact, according to the 2016 Web Applications Security Statistics Report, 50% of healthcare organizations' applications were rated "always vulnerable."

And with this guide, he hope to set you up for success to ensure you're not in the 50% "always vulnerable" group. HIPAA-compliance is a great place to start, and that's what we'll be covering in this ebook.

We assume in building your application, you won't be building everything from scratch, but rather utilizing a number of different APIs, IaaS, PaaS, and SaaS products and vendors.

1 http://www.healthcarefinancenews.com/news/health-system-fined-2-million-making-patient-data-public-online-twice

2 https://healthitsecurity.com/news/2017-ocr-hipaa-settlements-focus-on-risk-analyses-safeguards

WHAT WE'LL COVER

HEALTHCARE TERMINOLOGY

Before we set in, lets define the terms we'll use throughout this ebook.

Created by Pressfoto - Freepik.com

HIPAA

HIPAA, an acronym for, **Health Insurance Portability and Accountability Act**, is a law passed by US Congress in 1996 with two main purposes: one, to enable American workers to retain health insurance coverage when changing or losing their job (the portability part), and two, to ensure the protection and confidentiality of health information (the accountability part).

To achieve accountability among healthcare providers (e.g. doctors, dentists, etc.), health plan and health insurance organizations, and their associates (e.g. clearinghouses and cloud billing/storage providers), HIPAA defines four key rules[3]:

- The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"[4]) gives patients important rights regarding their ePHI, and identifies proper use and disclosure of PHI for patient care and other purposes.

- The Security Standards for the Protection of Electronic Protected Health Information ("Security Rule[5]") outlines the necessary physical, technical, and administrative safeguards for securing ePHI. As such, it is extremely relevant to data stream networks and will be the primary focus of this post.

- The Enforcement Rule[6] is, as the name implies, concerned with enforcing HIPAA. It deals with compliance, investigations, penalties for violations, and procedures for hearings.

- The Breach Notification Rule[7] requires "HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information."

3 The text of these rules are located at 45 CFR Part 160 and Subparts A and E of Part 164.
4 https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
5 https://www.hhs.gov/hipaa/for-professionals/security/index.html
6 https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html
7 https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

ePHI

Any PHI data that is created, transmitted, received, or stored electronically is referred to as **Electronic PHI** (ePHI) and must be handled with the appropriate security controls in compliance with HIPAA Security Rule requirements.

Unauthorized use or disclosure of PHI or ePHI by Covered Entities (e.g. hospitals, doctors, health insurance companies) and Business Associates (third-parties such as cloud billing services) brings the risk of severe civil and criminal penalties.

For reference, the 18 types of information that are classified as ePHI are:

1. Name
2. Address
3. Dates (of appointments, payments, etc.)
4. Telephone number
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan / insurance beneficiary number
10. Account number
11. Certificate / license number
12. Any vehicle identifiers (e.g. license plate number)
13. Device identifiers and serial numbers
14. Web URLs (Links)
15. Internet Protocol (IP) address
16. Biometric identifiers (finger / retinal / voice)
17. Photographic images
18. Any other characteristic that may be used to uniquely identify the individual

BAA

BAA (**Business Associate Agreement**) is a contract between a HIPAA-covered entity (the organization who is delivering the product), and HIPAA business associates (the organization or vendor working with the entity to store, transmit, or process PHI). It's basically an agreement between you (the entity) and the technology and services (the business associate) you choose to power your app.

The BAA is a legal contract that outlines the ways that the business associate complies with HIPAA, and responsibilities and risks that the business associate is taking on. BAAs include:

- Services the business associate provides
- Types of data they are interacting with

HIPAA AND WHY IT MATTERS

In a nutshell, HIPAA helps ensure that your PHI is protected, and holds those handling it liable. HIPAA sets rigorous and comprehensive guidelines for how PHI should be handled, to ensure privacy and fend off malicious parties.

Equally important, in choosing services and vendors that strictly adhere to HIPAA, you can focus on building a world class healthcare product rather than spending substantial engineering resources on HIPAA. It follows the classic build vs. buy calculation: why do it yourself when there's a number of solid vendors out there whose job is to do it for you?

HOW HIPAA FITS IN INFRASTRUCTURE AND THE APPLICATION ITSELF

Whether you're looking to build a HIPAA-compliant product using vendors and services, or you're building a HIPAA-compliant service of your own, you need to understand and implement controls on both the infrastructure and application levels. In this section, we'll discuss the controls that need to be in place for each level, as well as areas to implement these controls.

CONTROLS TO IMPLEMENT

- End-to-end encryption with TLS for in/outbound packets and AES for packets.
- Support fine-grained, token-based access control. Token-based access control allows you to grant and revoke access to any messaging channel.
- Purchase a TLS certificate; Distribute and manage certificate securely.
- Protect channels and topics (not covered by TLS).
- Build an authorization system for users.
- Consider AES and/or RSA encryption for payloads (not covered by TLS).

Now that you have a better idea of the controls necessary to comply with HIPAA, we'll look at the different levels, and where HIPAA fits in.

INFRASTRUCTURE

Infrastructure vendors need to implement reliability and security controls across their organzations. Here are the most important controls to achieve compliance:

- Twelve factor methodology.
- Secure provisioning for multiple environments (like a Kubernetes).
- Set up service management, system monitoring, and ops alerting.
- Create a load balancing scheme (like Nginx or HAProxy).
- Segment data by channels or topics with encryption.
- Find a store-and-forward solution for signal recovery, i.e. in-memory caching.
- Implement a method to detect which data center and port to connect a client to.
- Figure out which channels/topics to send/receive for a given client.
- Decide which platforms and languages you'll support.
- Create universal data serialization (JSON).
- Detect data uplink that works across device types.
- Determine Quality of Service and level of loss. Develop a data recovery scheme (or settle for "fire and forget").
- Decide APIs and capabilities you'll need, then build them (i.e. presence detection).

As you can see, ensuring HIPAA-compliance at the infrastructure level is a challenge that requires both expertise and significant maintenance. This is why many entities choose business associates to handle the infrastructure layer, rather than manage it themselves.

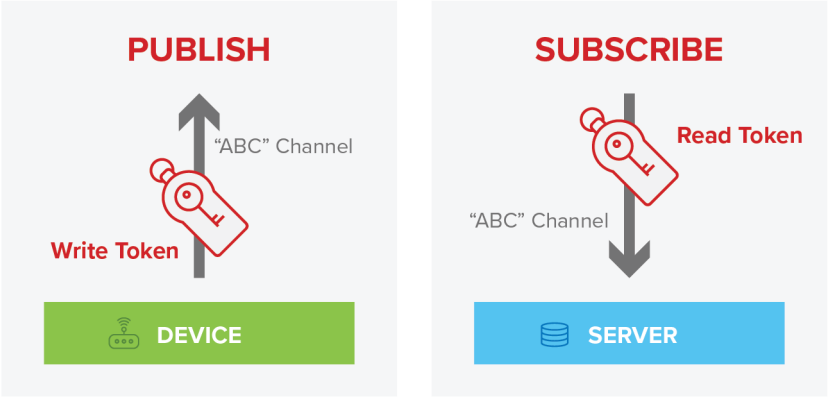
APPLICATION

At the application level, the entity and business associate may more likely share responsibility for achieiving compliance. Compliance on the application level is all about how the **entity architects and builds the app to interface with their end user**, rather than the infrastructure behind the scenes powering the app.

More robust HIPAA-compliant infrastructures will often provide APIs and SDKs, as well as professional services to help entities architect their applications to comply with HIPAA.

ACCESS MANAGEMENT AND AUTHORIZATION SCHEMES

Token-based access control is essential at the application level. It allows you to handle the end users and devices of your application, as well as the channels they're communicating over. Access management delivers fine-grained access control over who and what can transmit and receive data.



For example, take a publish/subscribe paradigm. The app can distribute tokens that grant either read or write access to specific data channels. This approach enables fine-grained control over which tokens are created, which devices receive those tokens, and to which data those tokens grant access. It also enables

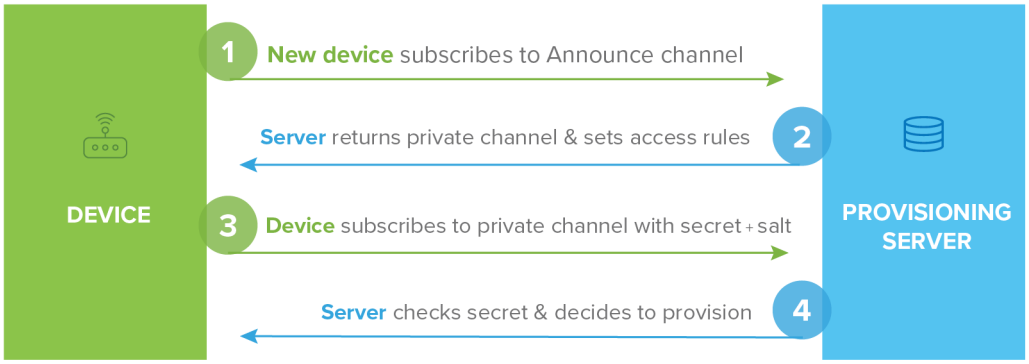
centralized control over when and how tokens are revoked, cutting off data stream access from non-paying customers, or invalid users.

In doing so, the network effectively serves as a traffic cop, both authorizing device access and managing which devices can speak and listen on the network based on the tokens the network distributes.

SECURE PROVISIONING

When devices running your application first start up, they'll need a process to securely provision software and firmware upgrades. This keeps your entire system immunized from exploits as they're patched out.

One common but unexpected security vulnerability: many users never install updates if the app seems to function well when it's initially set up. Often, users only opt to install firmware updates if something goes wrong. This leaves them vulnerable to security exploits, even if a fix is available.



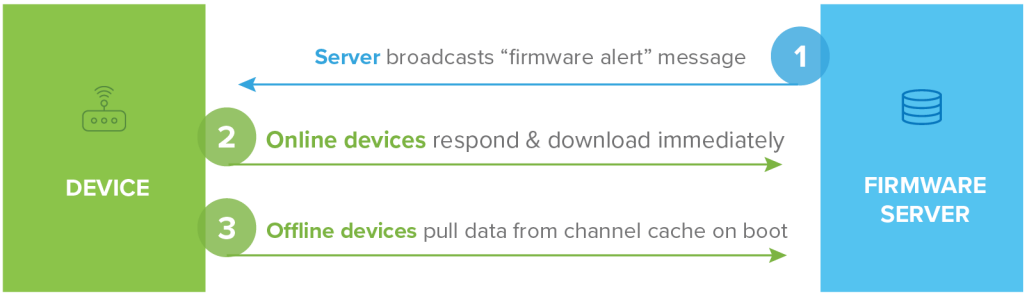
A publish/subscribe paradigm that uses the standard outbound ports 80 and 443 makes it easy to securely set up and provision healthcare apps. For example, when an app is active, it can subscribe to a designated Announce channel, and announce itself to the data delivery network. The server would return a private channel on which the device and server can communicate. The server can then set access rules on the channel, and provision from there. All of this happens immediately, retaining the consumer's expected plug-and-play experience.

SECURE FIRMWARE UPDATES

Once an app is set up and provisioned, it's also important to implement a way to securely and automatically update firmware for that app. If consumers have responsibility for downloading and installing firmware updates, there's a chance they will not download critical updates.

Without a secure channel, users may be vulnerable to malicious updates from unauthorized sources. To counter this eventuality, organizations should use the device's secure publish/subscribe channels to instruct the app to download and install firmware updates when they become available.

The design model for realtime firmware updates in the field begins with the server broadcasting a firmware alert message on a channel that all devices can read securely. The master server then instructs the devices how to access and install the update:



CONSIDERATIONS FOR CHOOSING THE RIGHT VENDORS AND TECHNOLOGIES

Before you begin researching the wide variety of services, frameworks, and vendors, ask yourself a couple questions. These will help you decide how much you want to build, and how much you want to buy.

- Do you run your own service, or do you utilize a hosted service?
- How much does it cost upfront? How much will it eventually cost at scale?
- Is the hosted service reliable, secure, and scalable?
- How mission critical is uptime to my application?
- Who on my team will maintain the infrastructure? Do they have the skills to make it scalable and secure?
- Where does the service store the data, and who has access to it?

These considerations expose just how many resources are required to operate an in-house solution. This extends beyond headcount, factoring in time commitment to building, maintaining, and orchestrating the infrastructure. Building the infrastructure in-house may work for smaller projects and POCs, but once you begin to scale, a hosted-solution is the way to go.

If price in the early stages is a concern, most hosted-solution providers also allow a free-forever sandbox pricing tier, where you can develop your app without paying. Once you've grown to a certain size, you pay as you grow. For those companies looking to move fast, and don't want to worry about all the intricacies of networking and infrastructure, hosted-solutions are the way to go.

BAAs

As defined in our earlier terminology section, a BAA an agreement between you (the entity) and the technology and services (the business associate) you choose to power your app. And BAAs are required for HIPAA-compliance, so ensuring that the technologies you use to power your app can sign the BAA is paramount.

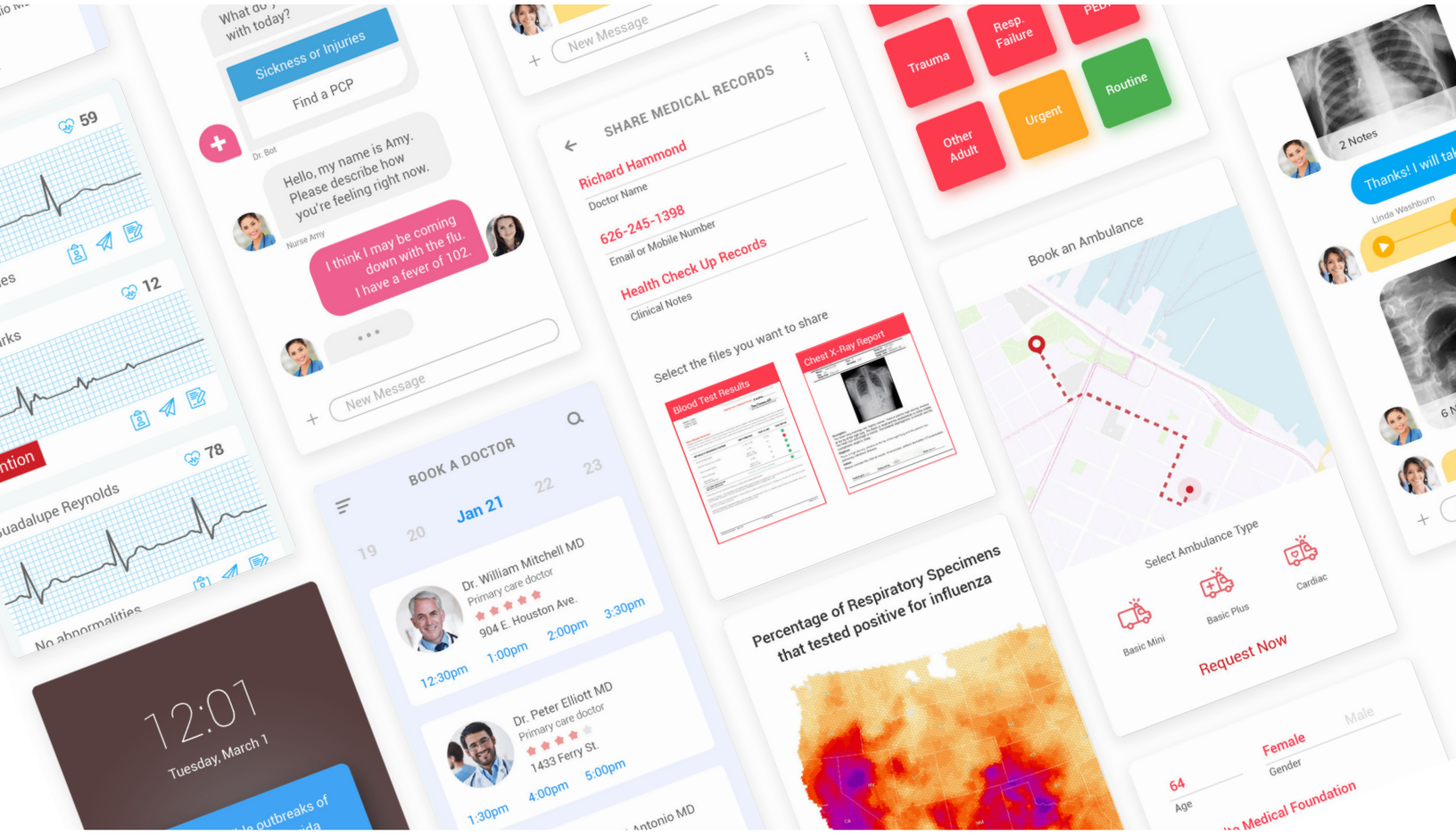
Why?

Any company can claim they're HIPAA-compliant. But signing a BAA puts it in writing that your third-party contractors are handling the sensitive information. These agreements establish the security expectations between you and the vendor(s). If a vendor isn't willing to sign a BAA, they aren't confident in their ability to maintain HIPAA compliance.

PubNub
AND HEALTHCARE

Read the Overview →

PubNub provides APIs and infrastructure to power realtime messaging to help you modernize your health and safety applications with robust and secure realtime messaging capabilities. Whether it's enabling HIPAA-compliant chat, sending and receiving PHI with confidence, or signaling and dispatching emergency response, PubNub provides the infrastructure and APIs to power it all.



We've built a realtime programmable network so developers can focus on what they'd rather do - innovate their applications - without having to worry about the 'plumbing:' whether or not the infrastructure is secure, scalable, and reliable. We've also worked hard to ensure that our network is HIPAA-compliant, so applications handling sensitive health information can safely use PubNub as their realtime infrastructure.

BEYOND HIPAA COMPLIANCE

PubNub has been HIPAA-compliant since 2015, and is the only HIPAA-compliant realtime network. We have many customers in the healthcare industry, such as New York Presbyterian, AthenaHealth and OneDrop, who have chosen PubNub for their realtime needs.

Outside of HIPAA, PubNub has taken additional strategies to ensure compliance with other data privacy laws:

E.U. ONLY DATA STORAGE

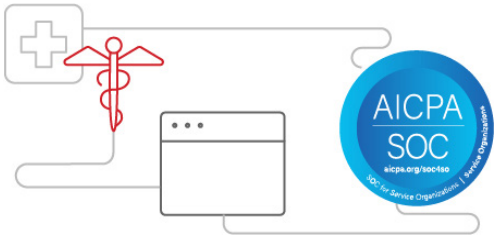
PubNub provides an option for any keyset to persist its data only in (at least two) E.U. Hosted data centers. Without this setting, by default, the customer's data is persisted and replicated to multi-regional (multinational) data centers.

MODEL CLAUSES

By request from any PubNub customer on a large scale plan, PubNub will enter into standard contractual clauses as provided by Articles 25 and 26 of the EU Data Privacy Directive 95/46/EC (known as "Model Clauses") to allow for lawful transfer of personal data from the EU to the United States. PubNub has secured reciprocal Model Clauses agreements from all its hosting providers.

EU-US PRIVACY SHIELD

PubNub has self-certified its participation in the EU-US Privacy Shield.



SOC2

We've completed the SOC 2 Type II audit, meeting the security, availability, confidentiality, and privacy standards set by American Institute of CPAs (AICPA).

GENERAL DATA PROTECTION REGULATION (GDPR)

PubNub has engineered its services and code to be compliant with European data privacy regulations.

Privacy Shield
Framework

CONCLUSION: WHAT'S NEXT?

Want to get building with PubNub? Here's a couple ways to get started:

1. Building HIPAA chat? Check out our PubNub Chat SDKs, which make it easy to build reliable, secure chat for web and mobile.
2. Dashboards and monitoring? Check out EON, our framework for building dashboards.
3. Want to talk to somebody? Our awesome success team and architects are ready for you. Contact us here.