Is HIPAA in Your Hip Pocket for **Virtual Health**?

by **CHRIS BOWEN**, CISSP, CCSP, CIPP/US, CIPT
ClearDATA Chief Privacy & Security Officer and Founder

ClearDATA
SECURE · HEALTHCARE · CLOUD

A **ClearDATA** eBook

It used to be a mobile app or smart watch was enough to deliver remote patient care.

The cloud has allowed us to evolve past a mobile app to the use of remote IoT and the medical internet of things, which allows us to do things like connect providers, payers and patients via chat from home devices, monitor a patient's glucose levels in real time and alert them or their caregivers on their phones if action is needed, or understand rhythms of the heart with remote heart monitoring devices.

Some innovative companies are even using AI for sentiment analysis to detect significant changes in facial expression that denote depression and can send messages to the provider to alert them to reach out to the patient and explore whether the proper medication plan is in place.

In this eBook, we'll take a look at the anatomy of Remote IoT, because sometimes the simpler technology seems on the user side of the interface, the more complex the back end is.

IN THIS eBOOK

- ✔ The complexity and risks associated with today's Remote IoT
- ✔ Why ensuring privacy, security and compliance is baked in on an ongoing basis
- ✔ How best practices, automation and tooling can reduce security and compliance risk in Remote IoT

2020 What a year in healthcare news!

Covid-19 changed everything. We saw providers and payers forced to pivot on a moment's notice to chat functionality and video conferencing on multiple devices. A surge in remote health monitoring also occurred. Payers and providers were forced to meet the patients where the patients were—in their homes—to reduce the spread of the virus.

In the wave of new telehealth, new privacy, security and compliance questions came into play.

The Office for Civil Rights (OCR) eased some HIPAA restrictions and declared they would not impose penalties for noncompliance against providers during the COVID-19 pandemic if they leveraged telehealth platforms—even if they may not comply with the privacy or security rules. For the first time in history, healthcare providers we allowed to use popular apps to deliver telehealth care. Apple FaceTime, Facebook Messenger, Google Hangouts, Zoom, Skype, and other similar services were no longer restricted by HIPAA rules.

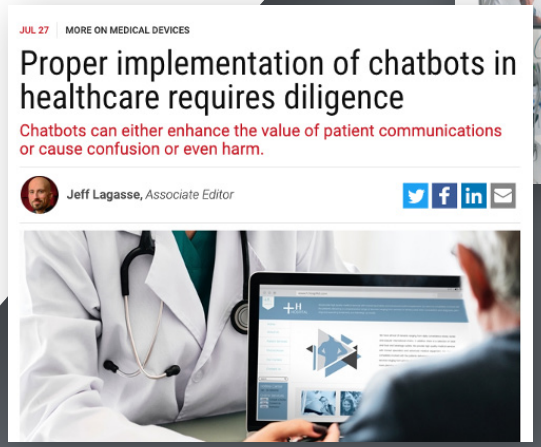
Did these COVID-induced changes mean we're no longer required to enforce the same protections on patient privacy as we did pre-pandemic?

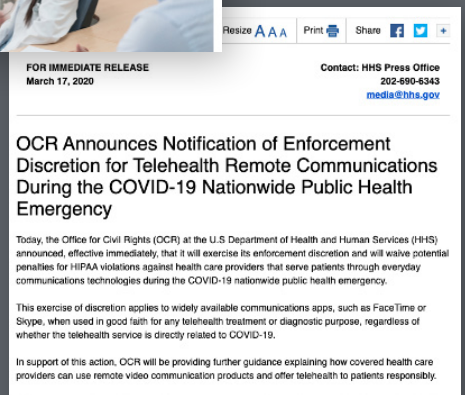
No is the short answer. This does not mean safety and compliance are the most recent victims of this sweeping virus. **HIPAA has in no way been weakened by this decision, and still applies to everything that provider or a payer or medical device company does with the information they get from that patient.**

As expected, the bad guys don't take a break when we are under attack from a virus. They see it as a vulnerability they can exploit, and have been targeting healthcare as never before. With so many rushing to the cloud and to mobile and remote IoT, the vulnerabilities and security by design best practices were often overlooked, potentially leaving your organization vulnerable to attack.

GO DEEPER

- What a 9,000% Increase in Telehealth Use Tells Us about HIPAA
- TeleHealth, Remote Communications, and HIPAA

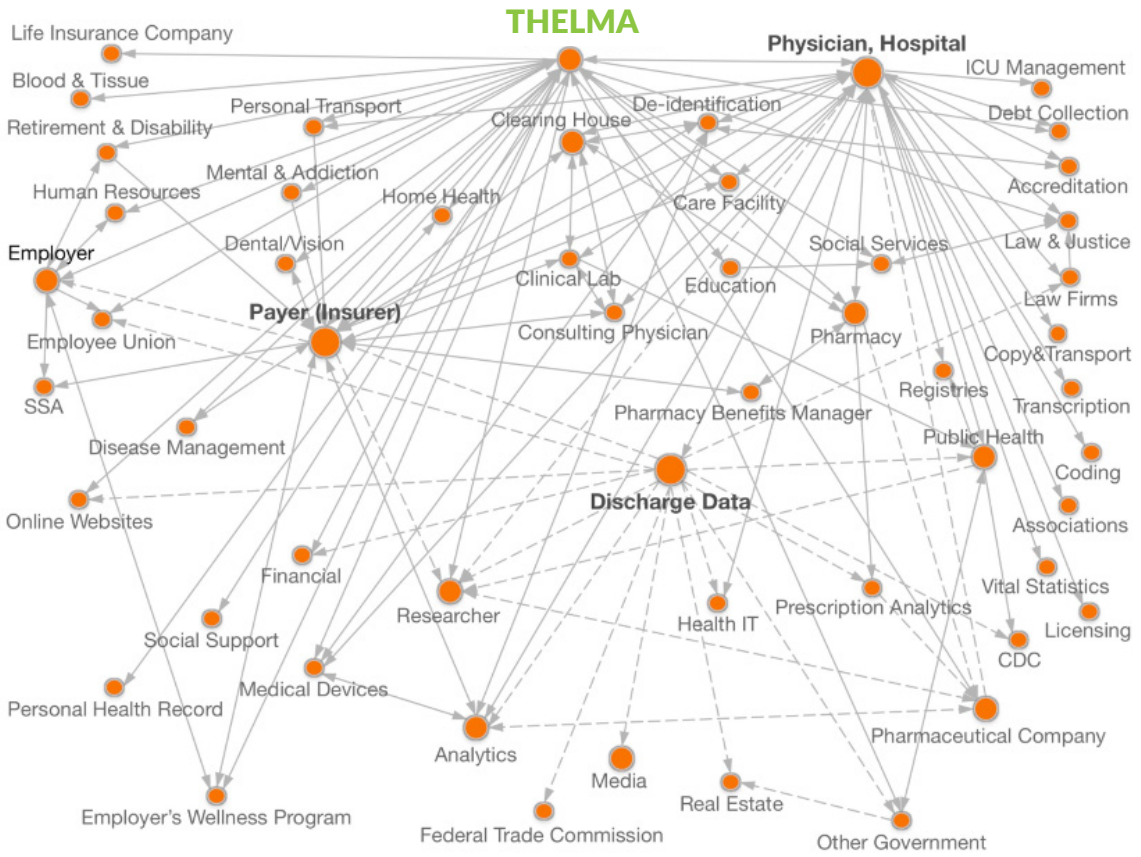




Meet Thelma*...

Being prudent and cautious, Thelma knows that her age places her in a higher-risk demographic. She uses her phone for telehealth visits when she doesn't need to see a provider in person. Unfortunately for Thelma, she unknowingly faces a risky landscape brought on by **software bugs, bad or no security patches, and device loss or theft**.

To further complicate matters, while Thelma thinks she is having a linear one-on-one conversation with her provider, her data is on a much more complex journey...



Mapping Healthcare Data — TheDataMap.org — A Harvard University Project
A single interaction between a doctor and patient can send patient data hundreds of directions, and the data sprawl is only getting worse with remote and mobile devices.

GO DEEPER

WIRED

A Legion of Bugs Puts Hundreds of Millions of IoT Devices at Risk

7 SAN DIEGO

Data Shows Cell Phones Are Being Stolen at Alarming Rate

ChannelProNetwork

Mobile Device Security: Startling Statistics on Data Loss and Data Breaches

* Of course, her name isn't really Thelma. *We protect patient privacy.* This woman is a model. You get the idea.

HIPAA Eligible v. HIPAA Compliant

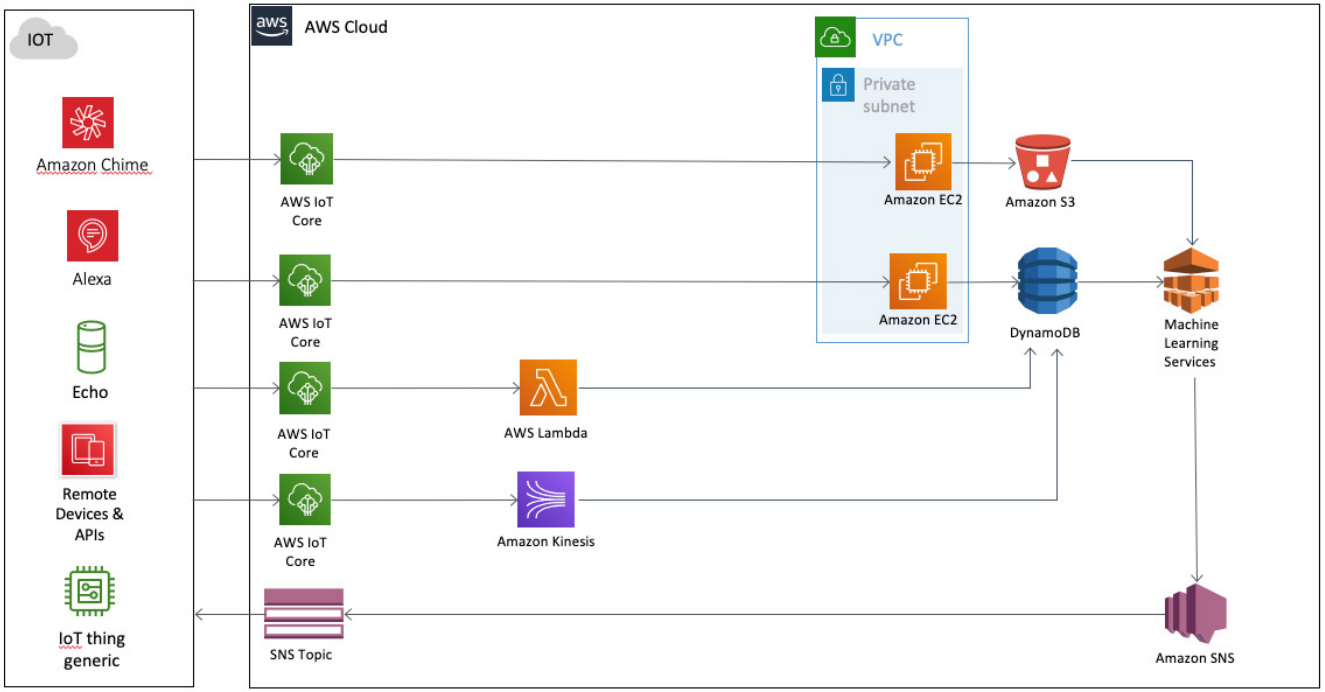
The Difference Has Big Implications

The public clouds are doing a wonderful job of deploying hundreds of new services every month, and many of these are being made HIPAA eligible.

HIPAA eligible means the service can be configured to be used within HIPAA compliance regulations, but it isn't automatically HIPAA compliant — you must know how to configure your environment for compliance and keep it that way. Just because a cloud has provided the building block doesn't mean the block is in the right place. And the concerns are not just at deployment, you have to maintain HIPAA compliance.

Healthcare and cloud expertise are vital. Your developer is probably not familiar with the complicated regulatory framework of healthcare, nor may that developer know how to translate HIPAA regulations into the necessary automated safeguards and technical controls that will keep your organization off the OCR's breach portal listing.

The Anatomy of Remote IoT in the Cloud



This reference architecture shows how data moves from devices on the left side, where patients and payers engage, through a complex ecosystem of cloud technologies. AWS is shown as an example, but all three major clouds have similar—but distinct—anatomies. Each stop through this ecosystem presents security risks.

Remember Thelma? — She may use Amazon Chime to consult with her doctor in Phoenix from the comfort of her home in South Dakota. But what's going on behind the scenes?

Consider the use cases on the left side. Supporting each of those in the cloud is complicated and if not done correctly, your organization is prone to risk. **And so is Thelma.** Your organization must be concerned with protecting Thelma as her PHI makes this journey.

An Example Scenario with Thelma

What was once science fiction is now reality, but there are serious security considerations in each of these steps. **How does one mitigate security risks in this instance?** Read On...

As a developer, you start with an application called AWS IoT Core, which allows connection to literally billions of devices that can pull information and push it through a data pipe called Amazon Kinesis.

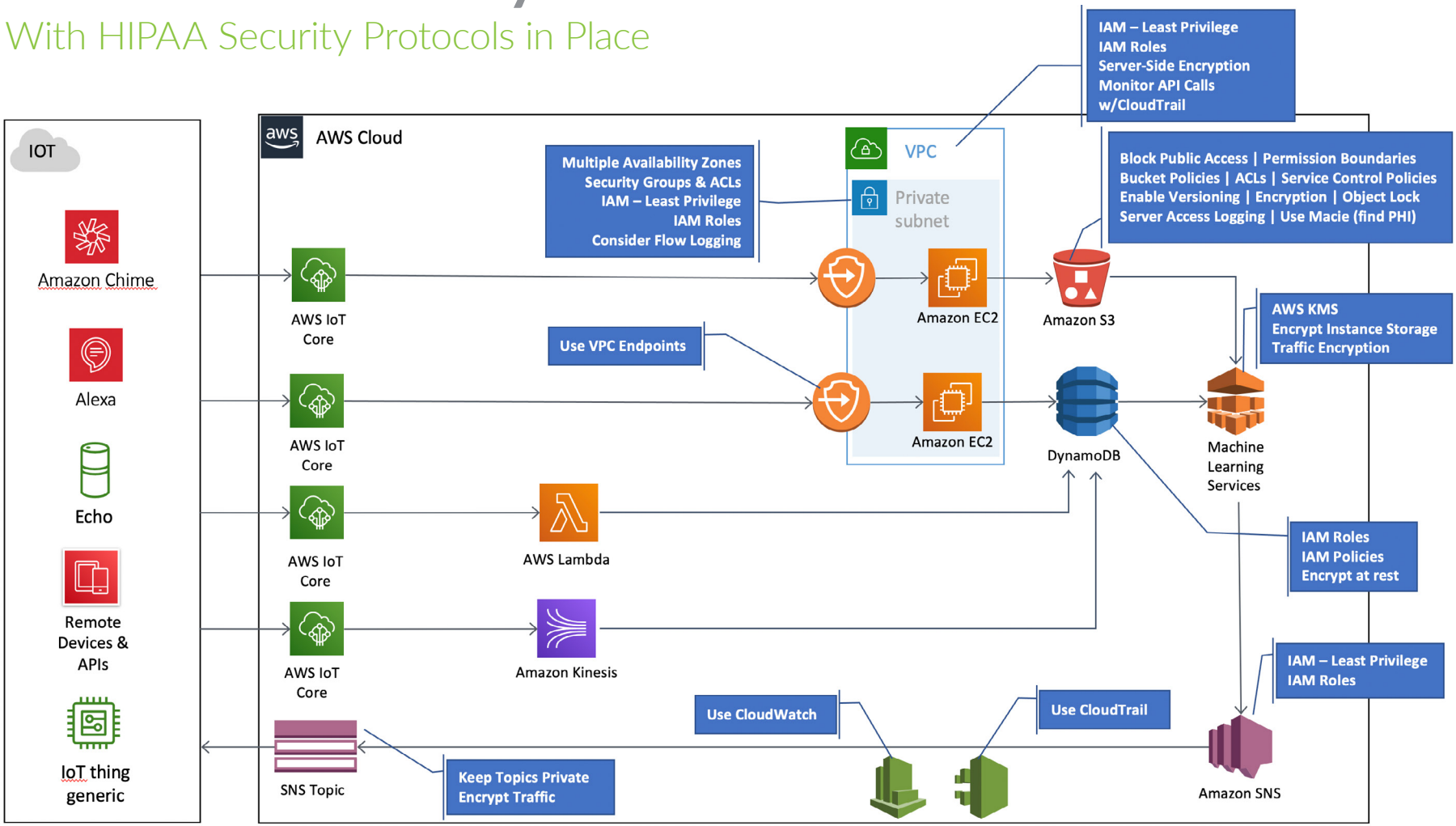
From there your cloud certified solution architect (or your third party partner if you don't have an architect on your staff) could configure AWS Lambda, which allows you to send commands to a remote machine.

Looking at sentiment analysis, the information can be pushed into a Dynamo DB table, a Database as a Service from Amazon, and then pushed into a machine learning service, in the Amazon world, called Sagemaker.

Finally, that info can flow back to the provider, using Amazon Simple Notification Service (SNS). Thelma's doctor can look at her sentiment analysis and realize she may be having a challenge with her medication, and personally reach out to see how she's doing.

The Same IoT Anatomy

With HIPAA Security Protocols in Place



WHAT'S HAPPENING IN THIS DIAGRAM?

- ✔ Secure ingress to privately connect multiple VPCs
- ✔ Block public access
- ✔ Encrypt each bucket
- ✔ Audit logging enabled
- ✔ Encrypt data at rest
- ✔ Identity management with roles and access/policies for each

If this looks complex, it's because it is. Cloud data security is not as simple as cobbling together the services — you must do it in a way that that adheres to HIPAA as well as standard frameworks for security such as the HITRUST Common Security Framework or the NIST Cybersecurity Framework.

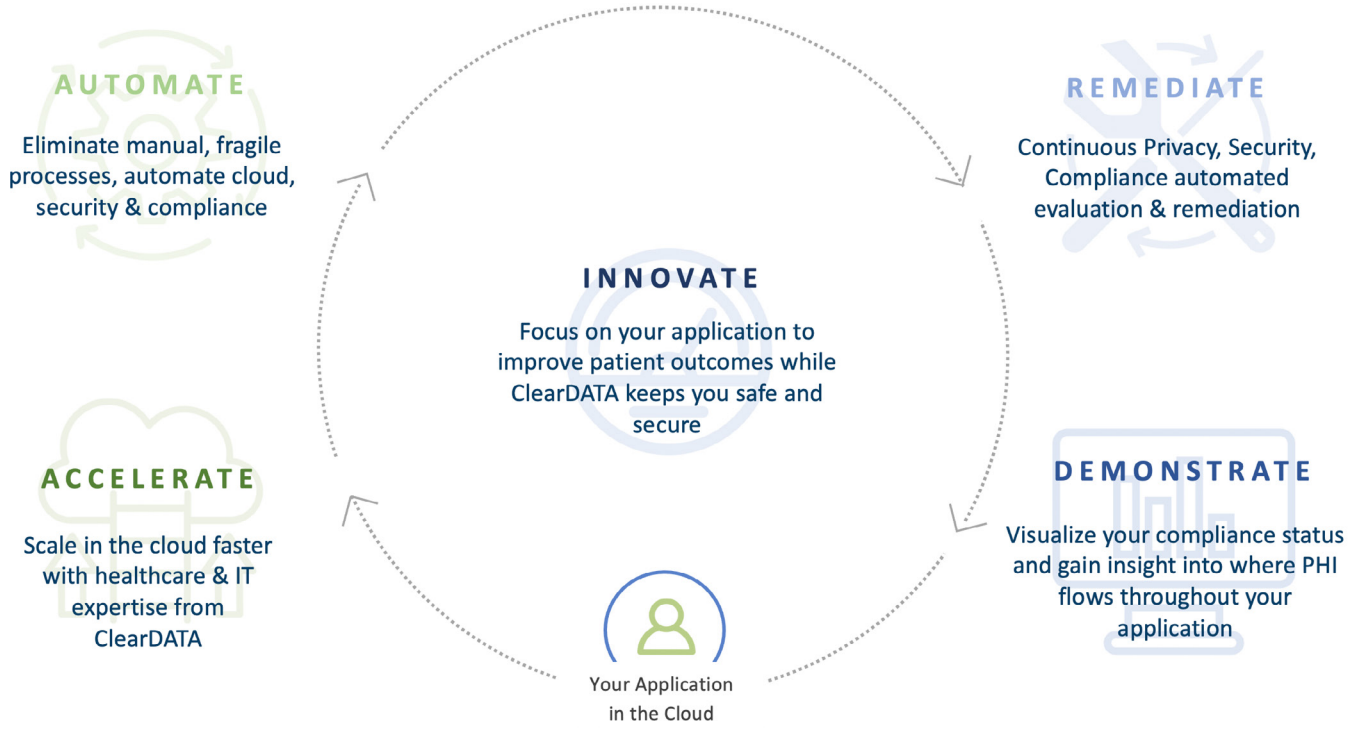
This is crucial for an agile development lifecycle — get the technology out there quickly and use CI/CD (continuous integration, continuous deployment) to push updates, **with no room for mistakes that could result in a breach**.

The ClearDATA Cycle of Innovation

We Help You Transform and Innovate in a Secure, Compliant Cloud

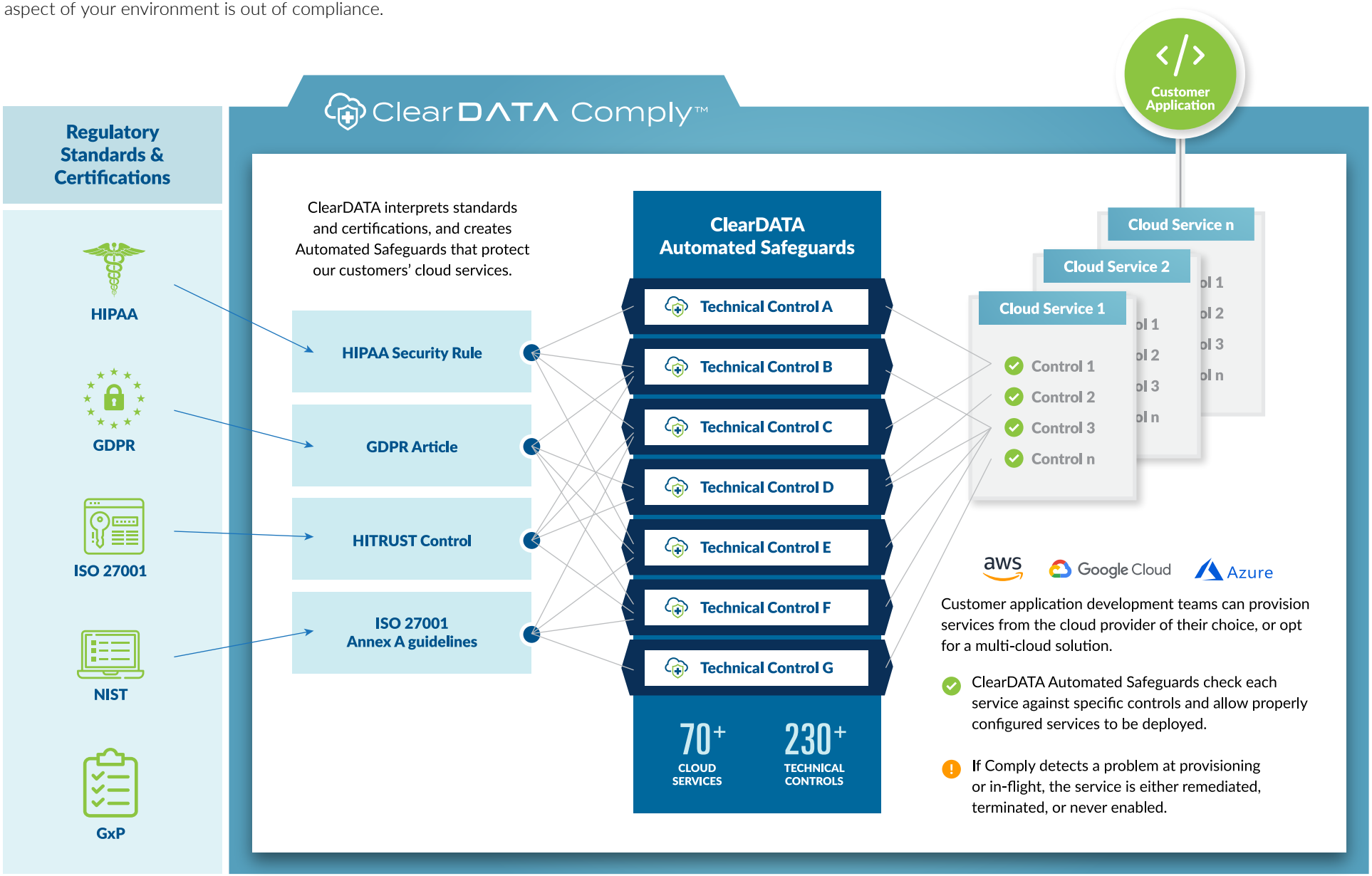
At ClearDATA we are HITRUST certified and healthcare exclusive, and because of that focus and expertise **we bring our customers peace of mind** knowing we are the leaders in providing security, privacy and compliance in the public cloud. Among the things we provide to give our customers peace of mind are:

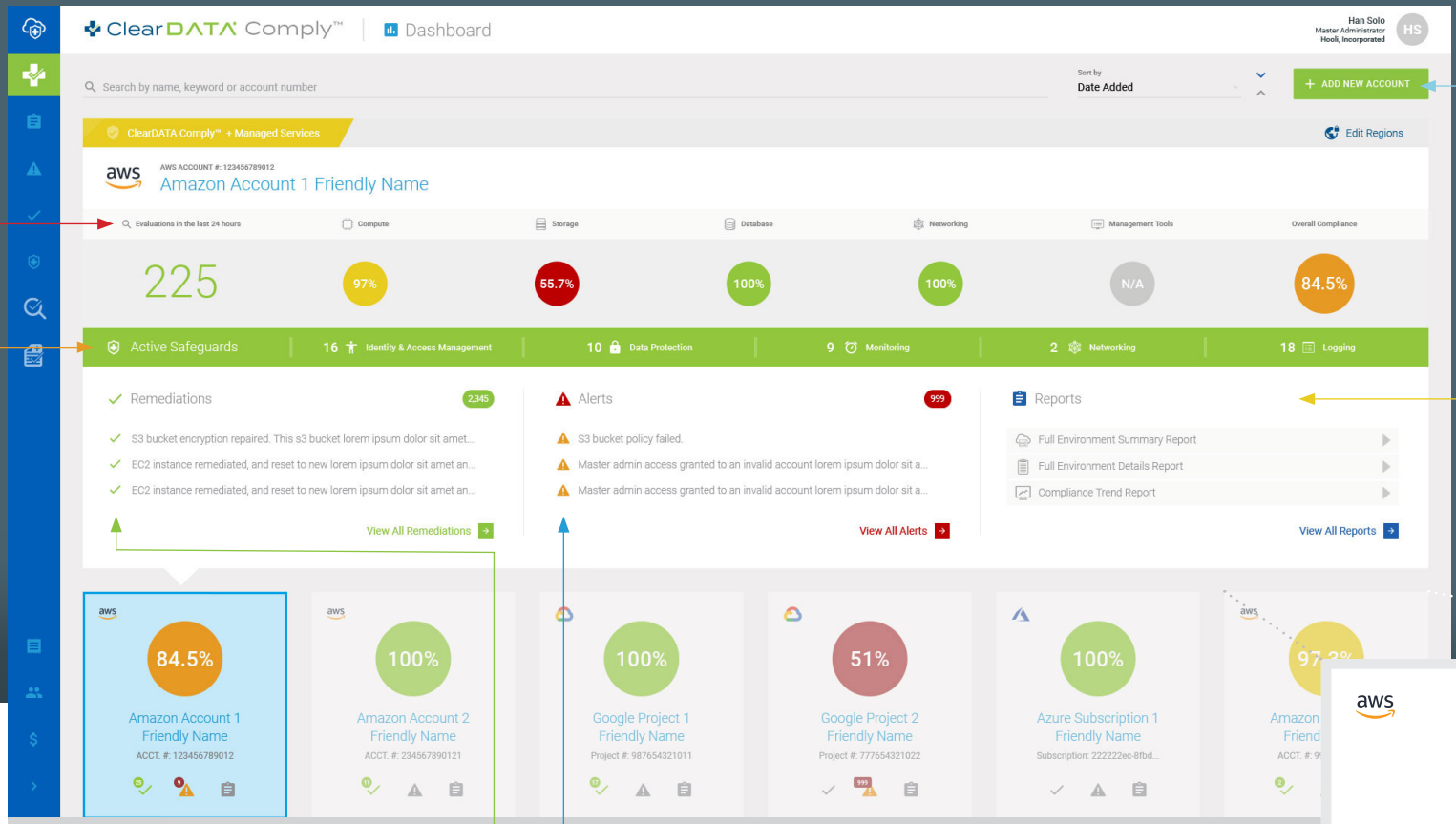
1. We have turned those HIPAA eligible services into HIPAA compliant configured services so you can accelerate your business and scale.
2. We ensure security and compliance from Day 1 for the life of the app, and automatically remediate if you drift out of compliance.
3. We demonstrate your compliance posture for you via our SaaS solution and dashboards backed by expert managed and professional services, so you know you are safe 24/7.



Develop Boldly. We interpret regulations so you don't have to.

ClearDATA has done the heavy lifting for you. We understand how regulations, both old and new, apply to the latest cloud technologies, connecting the dots between regulations like HIPAA and GDPR, standards organizations like NIST and ISO, and more than 230 controls across Azure, AWS and GCP. ClearDATA provides hardened images based upon CIS benchmarks — patched nightly and released monthly. **This mapping architecture works in real-time** and lets you know immediately if any aspect of your environment is out of compliance.



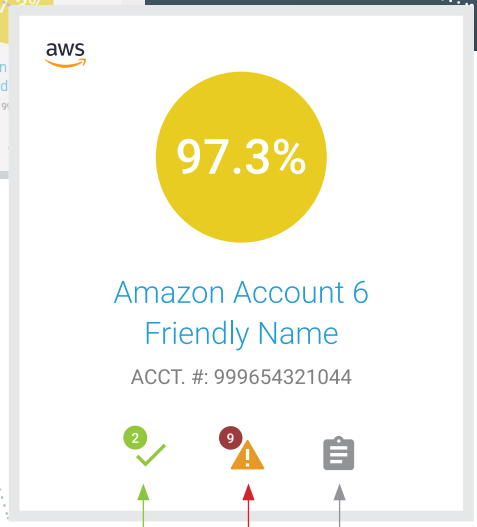


ClearDATA Comply™

Your window into the security and compliance status of your cloud environment

Add New Accounts On Your Own

Compliance Reports
View auditable reports across multiple accounts, projects and subscriptions



Comply Dashboard Features

Automated Safeguards
Technical controls automatically configured to keep PHI/PII secure, compliant, and protected

Evaluations
Triggered by a creation or change event to assess your compliance status

Alerts from the Past 24 Hours
Filter or search by severity, date range, etc. Alerts are events that may require attention or action. Severity is based on CIS guidelines

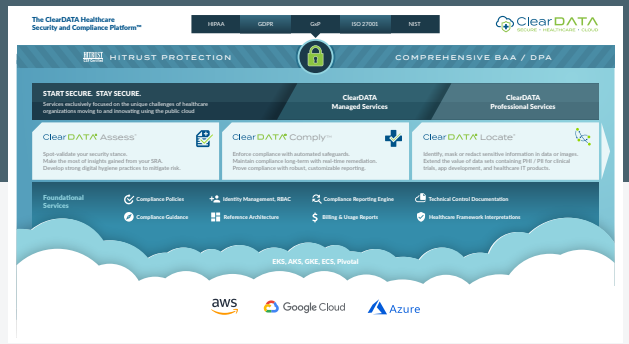
Real-Time Remediation
See what resources were remediated and when

Number of remediations in the past 24 hours

Number of alerts in the past 24 hours

Shortcut to reports for this account

How to get started with Comply



Learn more about the ClearDATA Platform

Comply Software Only

Deploy Comply to enforce compliance and access dashboards, audit reports, as well as ClearDATA Hardened Images, while managing your own environment and BAA.

Comply + Managed Services

Our certified cloud experts work with your team to manage security as your cloud journey expands and scales. As a trusted advisor, we can also help with custom architectures, cloud environment optimization, and international deployment of apps that handle sensitive data, maintaining compliance within global privacy frameworks.

Professional Services

ClearDATA can help you accelerate your cloud journey for even your most sensitive data sets through our healthcare IT consulting and professional services. Develop your cloud strategy based on a culture of compliance from the very beginning with ClearDATA experts, and know that sensitive healthcare data is safe, secure, and compliant.

What else does ClearDATA offer?

Comply is part of our complete solution called **The ClearDATA Healthcare Security and Compliance Platform™**— our comprehensive answer to securing sensitive data in the cloud. Built exclusively for healthcare by cloud experts, our platform not only keeps your sensitive data safe, but unlocks the tremendous, untapped value of data analysis and usage.

About ClearDATA

CORPORATE HEADQUARTERS
835 West 6th Street
Austin, Texas 78703

HITRUST
CSF Certified

aws Google Cloud Azure

Last updated: October 2020
2020-10-Rev.A

WE ARE
HEALTHCARE-FOCUSED

ClearDATA was conceived and designed from the ground up to serve the mission-critical system needs and regulatory requirements of healthcare organizations. Our founders drew upon their own experience, as well as that of the top engineers, systems architects, and visionaries from the healthcare IT and cloud computing industries, to create the most robust, secure, reliable, and HIPAA-compliant cloud computing solution in the industry.

As a HITRUST certified organization and the market leader for healthcare cloud computing and information security services for providers, life sciences, payers, and healthcare technology organizations, our solutions enable our customers to fully automate, protect, and securely manage healthcare applications, data, and IT infrastructure in the cloud.

Learn how ClearDATA can help accelerate your cloud strategy

Schedule a Live Demo of ClearDATA's Solutions

or call us directly at **(833) 99-CLEAR**