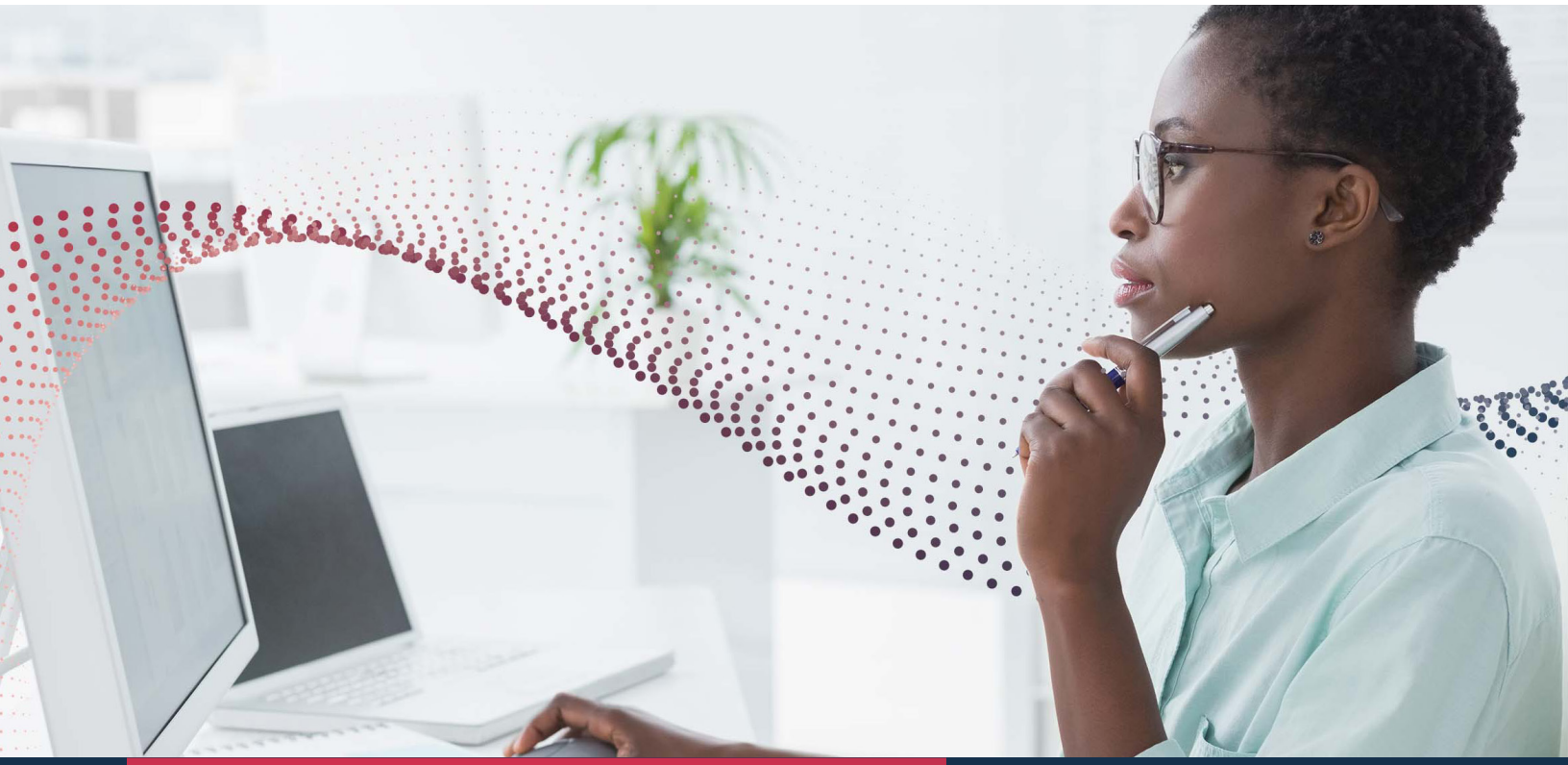
AKASA™



AKASA Information Security and Privacy

Information Data Collection and Security Overview

How AKASA collects information and keeps it safe.

Data is critical for healthcare systems because it's so much more than just data. It's your patients' health records, it's your financial information, it's sensitive information on your employees and community — it's everything.

We understand the importance of this data, and the concern and caution that comes with an ask to share any of it. This data needs to be protected and secure, so we make sure our process is as minimally invasive as possible.

Why AKASA Needs Access to Data

Data plays a vital role in the work we do at AKASA. Without it, we can't provide the world-class automation that allows you to streamline your revenue cycle process.

Before automating your revenue cycle, we embark on a three-step process that helps things go smoothly and safely.

01

Observe

We remotely install our proprietary software that analyzes how your team works, helping us determine where we can make the most significant impact with our automation.

02

Learn

With the help of our in-house revenue cycle experts, we build and deploy AI-based automation that's tailored to your systems and workflows.

03

Perform

Once the AI-based automation is in place, it conducts persistent performance monitoring, triaging unknown tasks to our internal experts-in-the-loop for resolution and further ML algorithm training, as well as identifying improvements to drive additional efficiency.

Once we've completed our core three steps, we continually measure performance to ensure you're always getting the most out of your automation. If we can improve, we will

Now, let's take a look at how we go about actually collecting this information.

How AKASA Collects Data

We collect numerous pieces of data to make our automation as effective as possible — while staying compliant with security requirements for your organization. To keep our process as safe as possible, we split our data collection into three categories.

Historical Learning

To understand how our platform can improve your workflow, we need to understand where you've been. To do this, we safely collect and analyze Word and Excel files around your SOP, org charts, and pre-AKASA productivity benchmarks. These files all play an essential role in training the machine learning. We also analyze a year's worth of EDI files (837s and 835s) to understand historical denial and payment patterns, and payor response times.

As part of the historical learning process, we also look at billing claim volume (Word and Excel documents) and aged receivables summaries (also Word and Excel documents) to set both baseline claim volume and baseline outstanding claim volume.

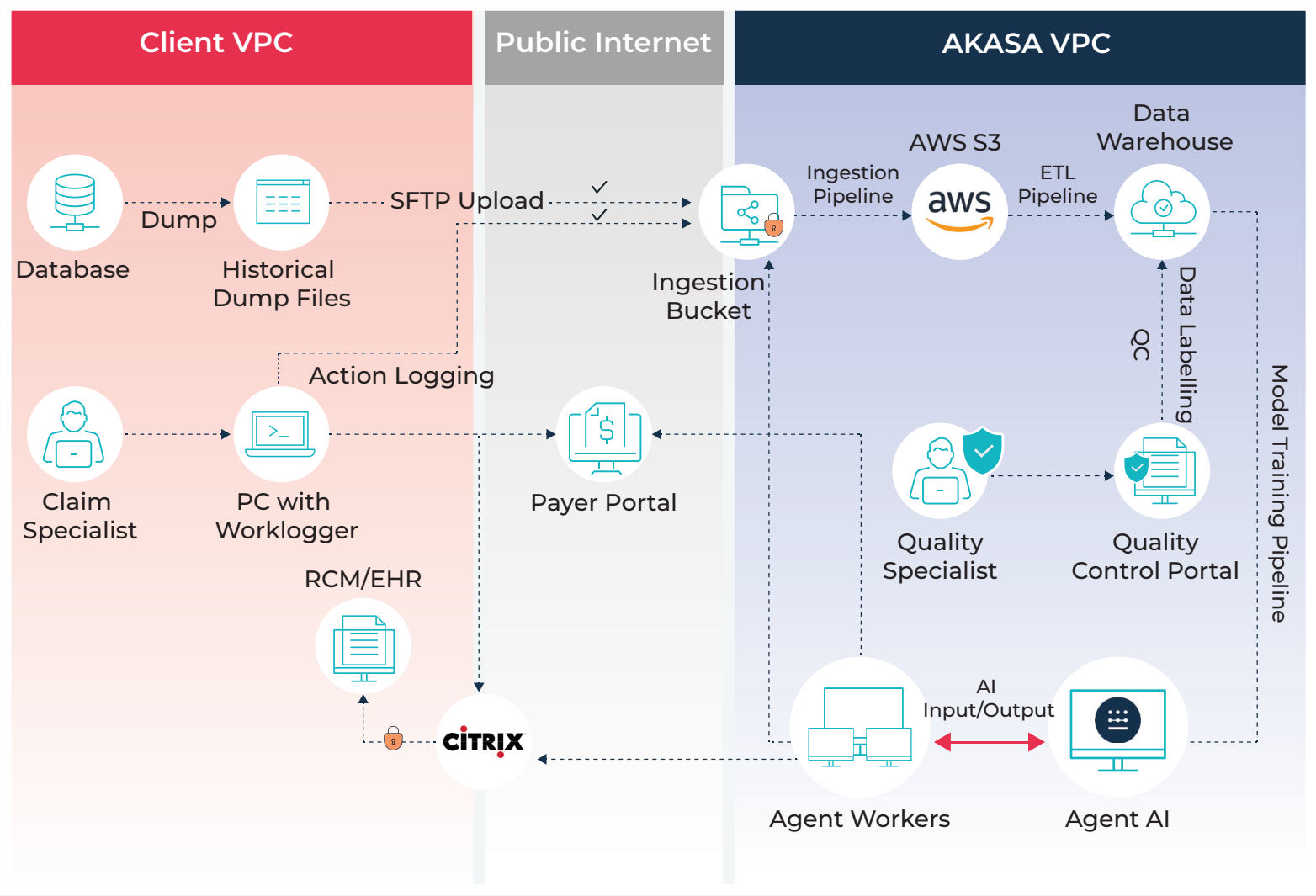
Real-time Learning

To see how your team operates, we remotely shadow your staff using teleops and our proprietary work-logging software as well. We also review recordings of patient access, mid-cycle, and business office tasks performed by your staff.

System Access

We look at standard employee onboarding, including billing application accounts and payor logins.

AKASA Technology Infrastructure



VISIT AKASA.COM

Safety Measures in Place

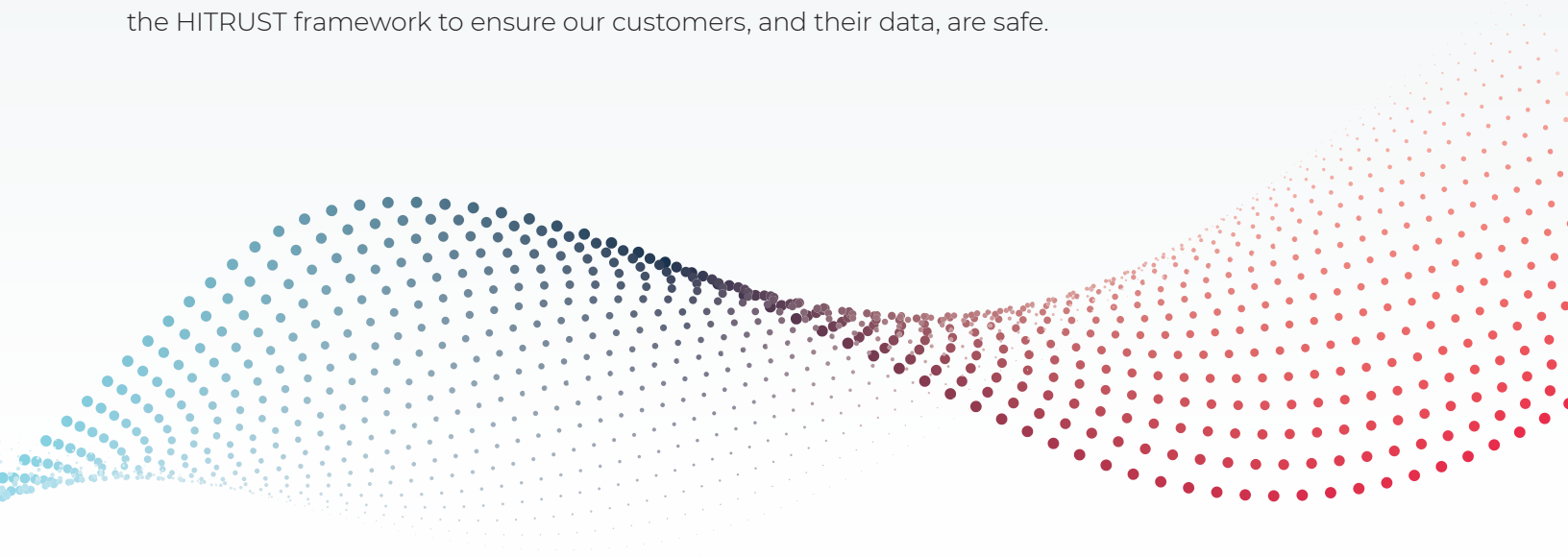
The safety of your data is paramount to you — and to us. This is why our security infrastructure is built upon certified security standards like NIST 800-53, HITRUST, and CIS. We have prioritized keeping your information safe through:

- **Amazon Web Service (AWS) Identity and Access Management (IAM):** AKASA utilizes strict authorization and authentication controls, which force 2FA, minimum password complexity, password expiration, and more. The AWS services robust security infrastructure is built upon certified security standards, including NIST 800-53, SOC Type 1 & 2 and ISO.
- **Data Encryption:** AKASA employs ZeroTrust VPN and FIPS 140-2 compliant data-at-rest and data-in-transit encryption protocols and keys, which are employed with complete user lockdown and privilege controls.
- **Protected Transfers:** All transmitted data is protected using SFTP or VPN and in some cases encrypted email.
- **Patch and Vulnerability Management:** AKASA scans and remediates the infrastructure in accordance with the published timelines from Homeland Security (i.e. critical vulnerabilities are patched within 15 days).
- **Audit Trails:** Any access to PHI data is logged with detailed information. In the event of a suspected breach we have documented security protocols we quickly put into place.
- **Versioning:** Original content is retained upon any data object changes.
- **Alerts/Monitoring:** We monitor our automation 24/7, with strict access monitoring metrics established. Any deviation for our automation or relating to access results in immediate alerts being triggered.

- **CIS Benchmarks:** AKASA utilizes CIS Level 1 hardening standards and Industry Best Practices within our AWS infrastructure. CIS benchmarks are accepted in business, industry, and government use, and require strict adherence to safety.

- **Data Destruction:** We destroy all sensitive data after termination of a customer contract, or during an engagement based on our customer's preferred retention schedules.

All of the above are backed by our administrative, physical, and technical safeguards that meet or exceed all HIPAA regulatory mandates and implementation specifications. We also align ourselves with the HITRUST framework to ensure our customers, and their data, are safe.



Safe, Secure, Simple. AKASA.

Automation requires data. There's no getting around that. But, unlike many other vendors in the automation space, we require only one lightweight installation, and we have experts-in-the-loop available in the event assistance is needed.

With AKASA, you can rest easy knowing your data is still in your control and being handled as little as possible — by those who put security first.

AKASA™

If you have any additional questions, **contact info@akasa.com**