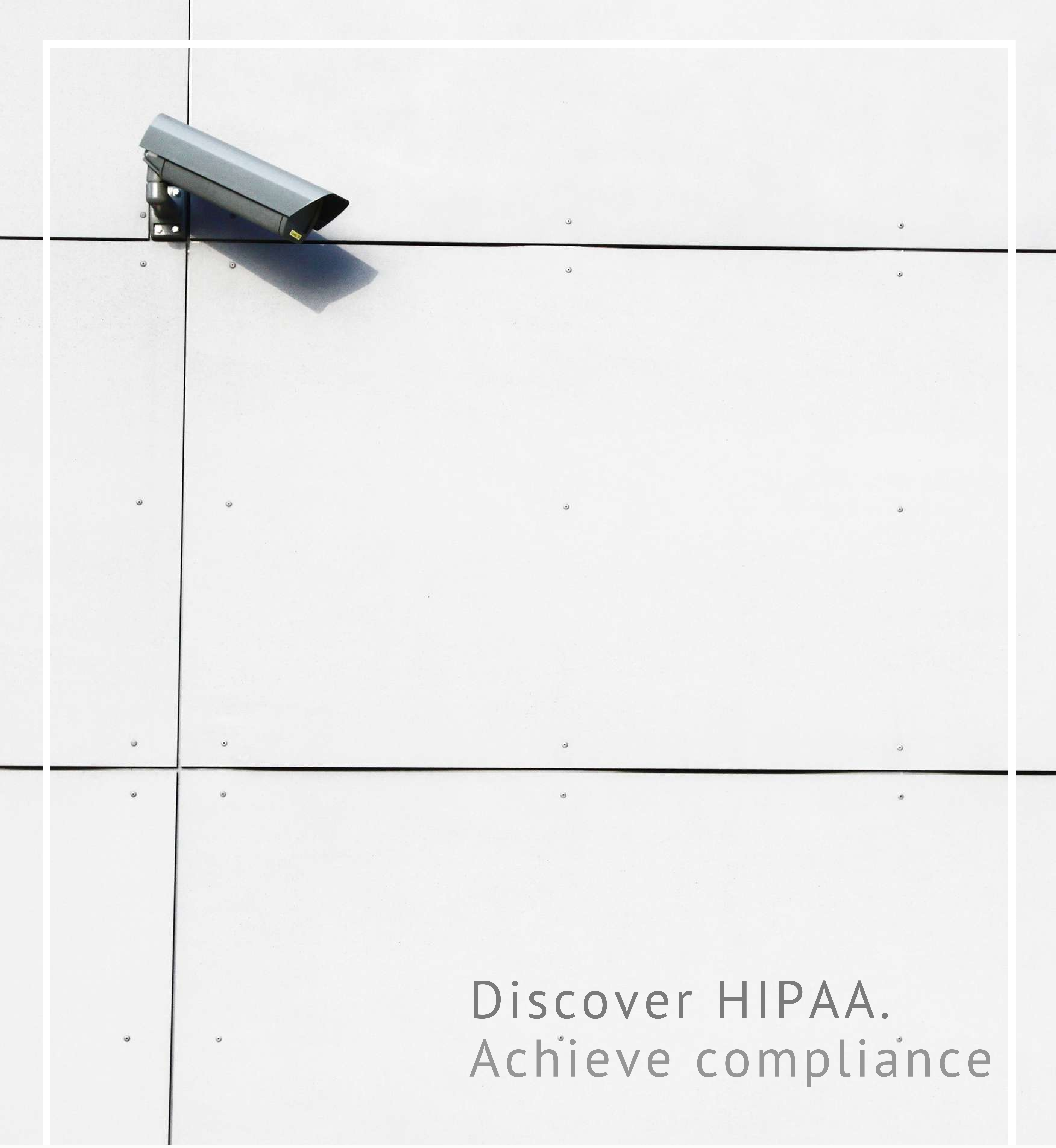


THE ULTIMATE HIPAA IT COMPLIANCE GUIDE

BY LOGSENTINEL

"IT TAKES 20 YEARS TO BUILD A REPUTATION AND FEW MINUTES OF CYBER-INCIDENT TO RUIN IT."
— STEPHANE NAPPO

Technical Requirements

Access control

Implement **technical policies and procedures** for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights

Make sure that you have established certain safeguards ensuring proper access control, such as:

Unmodifiable Audit Logs

Real-time incident reporting

Fraud Detection

Implementation

Prepare an IT plan related to the implementation of the security measures that have not been implemented yet. Conduct an annual internal audit to take proper corrective and preventive measures based on the implementation.

The following four IT aspects should be carefully reviewed and implemented in accordance to the needs of the organisation:

Unique user identification	Emergency access procedure	Automatic logoff	Encryption & decryption
Assign a unique ID (name, number, combination of symbols) to identify and track user identity.	Establish procedures for obtaining necessary electronic protected health information during an emergency.	Make sure you have established procedures to terminate sessions after a predetermined time of device inactivity.	Encrypt and decrypt any protected health information (PHI). Make sure the database you store PHI is also encrypted and the data transfer-secure

Technical Requirements(2)

Audit Control

Implement hardware, software, and procedures that record and examine activity in information systems that contain or use protected health information.

Make sure PHI cannot be accessed by unauthorized parties at any devices - even medical ones. Consider physical assess restriction (locked doors), as well as sofrware / device access restrictions.

Medical Devices

Computers, Printers, Phones

Cloud Storage

Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Technical Requirements(3)

Person or entity authentication

Implement procedures to verify that a person or entity seeking access to electronic protected health information is authorized to receive it.

Make sure all the procedures and processes you implement are in line with your organisation policies. Also make sure that they are being audited on a regular basis

Transmission security

Implement technical security safeguards against unauthorized access to electronic records of PHI that is being transmitted over an electronic communications network

Integrity Controls

Implement security measures to ensure that electronically transmitted PHI is not misused without detection until its disposal.

Make sure you have set up certain event log alerts for tracking misuse.

Encryption

Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

Audit all your records where you store PHI and plan how to minimize it and keep it encrypted.

What We Offer

Protection of PII and health records

We offer a '**Privacy by Design**' secure database. We encrypt every record individually, using a secure key hierarchy making data breach events practically impossible.

Keeping unmodifiable logs of activity

Most of the data breach attempts are initiated by insiders. Very often insiders manage to cover their traces making it impossible to track back who has breached the data. With SentinelTrails, your activity logs will be kept safe on blockchain , so that no one would be able to access your data without any evidence

Fraud and anomaly activity detection

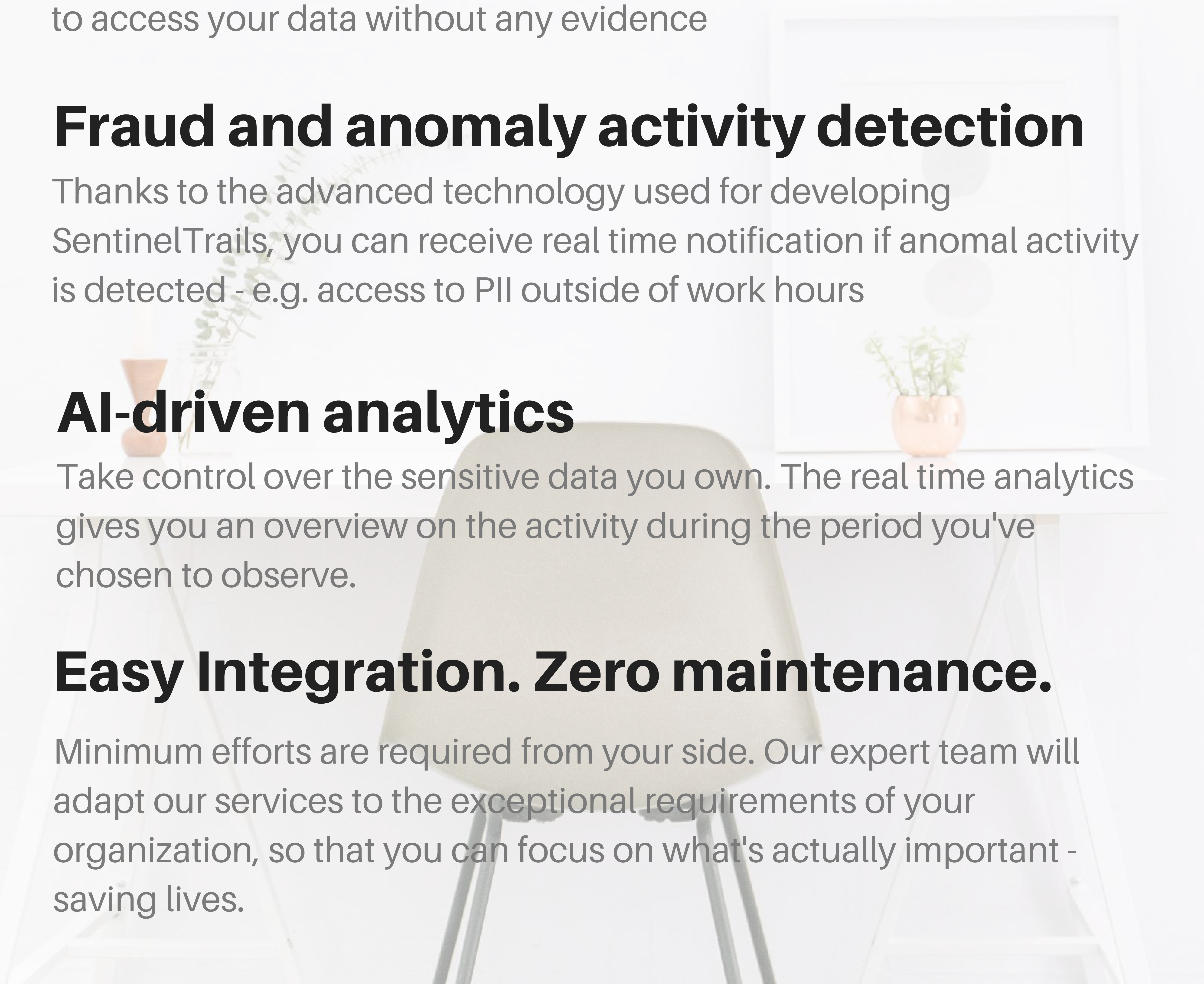
Thanks to the advanced technology used for developing SentinelTrails, you can receive real time notification if anomal activity is detected - e.g. access to PII outside of work hours

AI-driven analytics

Take control over the sensitive data you own. The real time analytics gives you an overview on the activity during the period you've chosen to observe.

Easy Integration. Zero maintenance.

Minimum efforts are required from your side. Our expert team will adapt our services to the exceptional requirements of your organization, so that you can focus on what's actually important - saving lives.



Information Security, Data Protection & Compliance

www.logsentinel.com