medixsafe

SECURITY WHITEPAPER

WWW.MEDIXSAFE.COM ▪ 1-855-633-4972
SECURITY@MEDIXSAFE.COM

MedixSafe has been securing people, places and critical assets since 2009.

We build all of our electronics and our software in-house, with our own team of IT security professionals. We do this because we know our customers trust us with more than just their critical medical supplies: they trust us to connect to their networks, and to protect their data. We take that responsibility seriously – and our commitment to security goes well-beyond the strength of our steel and the rating of our locks.

We are the market-leader in digital security, with the most-secure hardware and software in the industry – and we have the patents to prove it. Our safeguards provide end-to-end security:

- ✓ **Hardware Security:** Our electronics are protected from tampering by secure-boot, code-signing, and active fault monitoring.
- ✓ **Software Security:** Our software is security-hardened, reviewed, and subject to formal change-management.
- ✓ **Data Security:** All data is encrypted, both at rest and in transit. Our patented algorithms minimize PII, and provide the most-advanced protections for biometric data in the industry. Sensitive data is securely erased when it is no longer required.
- ✓ **Network Security:** All communication is fully-encrypted, and exceeds the requirements of NIST, ISO 27400, and HIPAA. We have no hidden passwords, and use advanced techniques to protect against attacks such as spoofing or MITM.
- ✓ **Cryptographic Key Management:** Our cryptographic key management exceeds the standards required for sensitive data protection in the US Federal Government (NIST SP-800-175B).

We have taken a different approach. We build security, data-integrity and privacy into our products from the ground up, as a key part of our commitment to keeping our customers safe.

If you have any questions, please contact us; we would be happy to speak with you, and explain why we believe we have the most-secure products in the market.

Courtney Gibson
Chief Technology Officer
MedixSafe, Inc.

PLATFORM OVERVIEW

This document provides an overview of the security architecture of the MedixSafe platform; this includes our MedixSafe devices and our MedixSafe Cloud platform.

WHAT WE PROVIDE

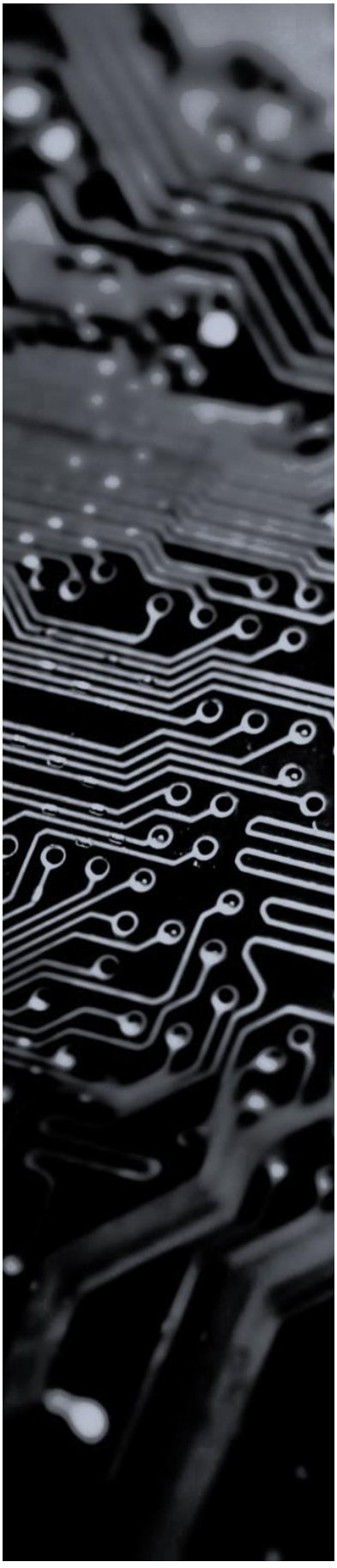
- **MedixSafe Cloud**
  - A cloud-based service, used by our customers to: configure and administer their devices, enroll and manage authorized users, and review logs and alarms.
  - Hosted on AWS, with redundant systems hosted in both the AWS US East and AWS Canada Central zones.
  - Our platform interface is browser-based: there is no client-side software required.
- **MedixSafe Devices**
  - Our IoT-enabled devices provide security for our customers' narcotics and other medical supplies.
  - This includes our SafeLink line of narcotics-control safes, our DoorLink access control solution for pharmacy and supply rooms, and associated hardware.
  - Customers may elect to use a combination of PIN, access cards and/or biometrics to authenticate their users who are allowed to access the safes / rooms.

WHAT WE COLLECT

- **Personal Information:** We collect the name and email address for each user of the product. Additionally, if customers choose to enable these authentication methods, we may also optionally collect PINs, RFID access card data and/or biometric data associated with the users of the product, with opt-out options (see Data Security).
- **Other Data:** (1) The configuration settings for our customers' devices; (2) Logs of how our customers interact with our devices (*e.g.,* accessing a narcotics-control safe; and, (3) Software logs, which contain no PII, no biometric data, and no sensitive information

WHAT YOU PROVIDE

- **Networking:** A basic network connection (Ethernet or Wi-Fi), with access to the public Internet, over a limited number of ports (see Network Security).



medixsafe

HARDWARE SECURITY

The electronics in our safes are tamper-proof and reliable.

Multiple layers of protection ensure that our devices can't be infected with malware, they won't be disabled by ransomware – and they will keep running, even through configuration errors and interrupted firmware upgrades.

These important measures protect our products but, just as importantly, they protect our customers' networks and other devices as well... which is critical at a time when multiple studies have found that **more than 50% of IoT devices have critical vulnerabilities that hackers can exploit right now**[1].

SECURE BOOT

Our devices natively support Secure Boot; a cryptographic signature ensures the software on our devices cannot be tampered with, once it's installed – eliminating the risks of malware and ransomware.

FAULT MONITORING

Three independent hardware watchdogs monitor input voltage and software heartbeats; they will automatically reboot the CPU if an error is detected, ensuring our devices are always ready to work.

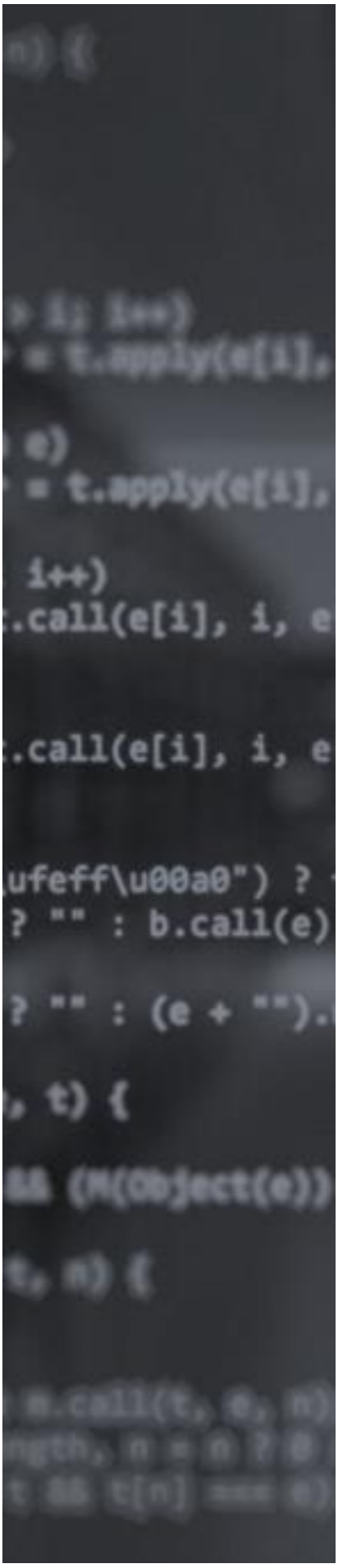
AUTOMATIC ROLLBACK

Configuration changes and firmware upgrades are automatically rolled back by the hardware, in the event of errors or failed updates (ISO 27400:2022).

FBI CERTIFIED

Our biometric hardware is FBI certified (FAP20), and has a False Acceptance Rate (FAR) of better than 1:1,000,000. This is the highest standard of performance and security in the industry.

[1] IBM X-Force Threat Intelligence



medixsafe

SOFTWARE SECURITY

All our software is built in-house, in North America, by our own team of IT security professionals.

We use best practices across our engineering lifecycle, to ensure we are delivering the most secure, reliable software in the industry.

SECURITY HARDENING

Our software has been designed from the ground up to be security hardened. Our devices have no operating system, no extra processes, no open ports, and cannot be logged into – and those security controls cannot be changed.

CODE-SIGNING

We cryptographically-sign our software (ISO 27400:2022). This ensures that only our approved software can be installed, and prevents tampering or the installation of backdoors that could compromise your data or your networks.

CHANGE MANAGEMENT

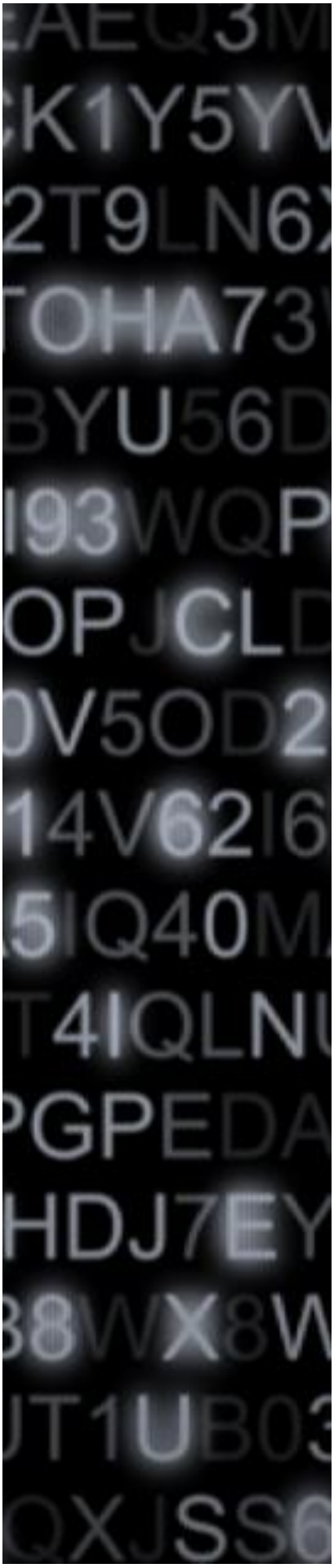
We have a formal change management system for all software and system changes. This includes risk reviews, change tracking, and a formal release process.

CODE REVIEWS

Every code change is peer-reviewed for correctness and security, prior to its acceptance for release.

QUALITY ASSURANCE

Our dedicated Quality Assurance team validates every release against standardized tests that confirm correctness, performance and security, and that no regressions have been introduced.



medixsafe

DATA SECURITY

We are the market leader in digital security, offering the highest level of data production in the industry. Our patented approach ensures our customers' data is protected at all times, and helps address even the most-stringent regulatory requirements.

DATA COLLECTION

Our systems collect the minimum amount of data required to provide our services. This includes: (1) a limited amount of PII (see below); (2) logs of user activity (*e.g.*, safe openings); and, (3) logs of software performance.

DATA IN TRANSIT AND AT REST

Data at rest is encrypted (AES-256), using a randomly-generated key that is unique to each device (ISO 27400). In many jurisdictions this means even the loss of a safe is not a reportable PII breach (HIPAA Security Rule 164.404/406/408/410). Data in transit is encrypted (AES-256), using a randomly-generated key that is unique to each customer (ISO 27400).

PERSONAL INFORMATION

Our systems collect the name, email address and (optionally) a PIN or access-card number for each user. Our patented algorithms protect sensitive data using one-way hashing (SHA-256) to ensure that the data cannot be recovered.

BIOMETRIC DATA (OPTIONAL)

Biometric data collection is optional: customers can elect not to use it, and individual users who do not wish to enroll their biometric data can (optionally) opt out, and use a numeric PIN for authentication. Our system does **not** capture fingerprint images; instead, MedixSafe captures fingerprint templates (ISO 19794-2). This data cannot be used to recover users' fingerprints. As additional safeguards, the templates are strongly encrypted (AES-256) at all times (HIPAA Security Rule 164.312(e)(2)(ii)), and a cryptographic signature (HMAC-SHA-256) ensures templates cannot be tampered with or assigned to a different user (HIPAA Security Rule 164.312(e)(2)(i), 164.312(c)(1)).

DATA RETENTION

Sensitive data on our devices is securely erased when it is no longer required (NIST SP-800-88). Data on our cloud is erased as soon as a customer requests it (*e.g.*, when a user is deleted).

medixsafe

NETWORK SECURITY

Our approach to network security exceeds the requirements of NIST, ISO 27400, and HIPAA.

We have no hidden passwords or pre-shared keys, and we use advanced cryptographic techniques to protect our devices from network attacks such as spoofing or MITM.

TLS

All of our network communications are secured with a minimum of TLS 1.2. This meets the requirements of ISO 27400 and HIPAA 164.312(e)(1), and includes all user data transmission, API calls, commands, configuration, and device logging.

X.509

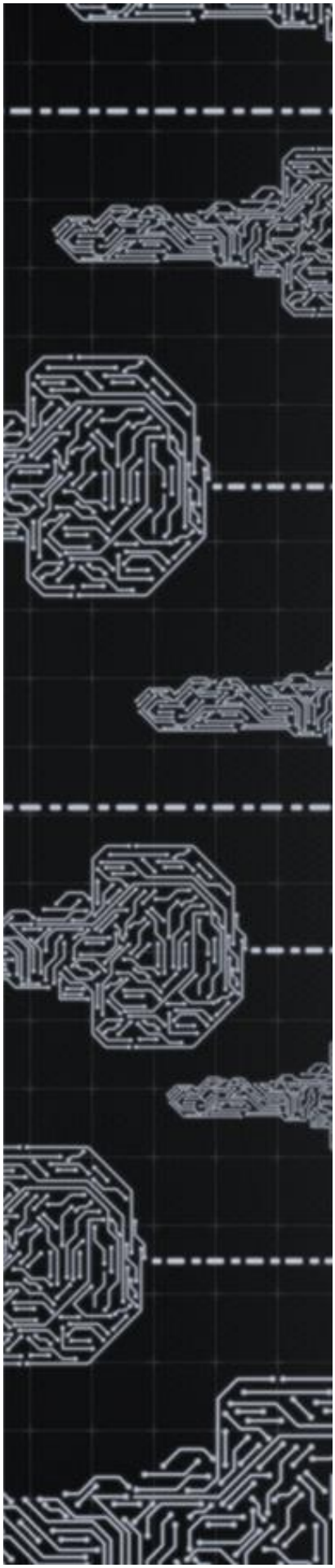
All communications between our devices and our cloud services use X.509 certificate-based logins, with authentication performed in both directions (client-to-server and server-to-client). We have no pre-shared keys or passwords that can be stolen, leaked, or reverse-engineered.

CERTIFICATE VERIFICATION

Both our cloud service and our devices each maintain a trust keystore; this is used to prevent network-based attacks, such as DNS-spoofing, ARP-spoofing, or other on-path (MITM) attacks.

FIREWALLS

Our devices do not accept inbound connections on any port, and outbound connections are restricted: see the *MedixSafe Network Configuration Guide* for full details.



medixsafe

KEY MANAGEMENT

One of the most-overlooked aspects of security – and one of the most-important – is how encryption keys are managed.

Our cryptographic key management exceeds the standards required for sensitive data protection in the U.S. Federal Government (NIST SP-800-175B).

KEY GENERATION

Each MedixSafe device has its own unique encryption keys: this includes both a 256-bit symmetric key that is used to encrypt local data at rest, and a 2048-bit RSA public keypair that is used to secure data in transit. These are generated locally, using a True Random Number Generator, and MedixSafe does not have the ability to access these cryptographic keys.

KEY DISTRIBUTION

Each customer has a unique 256-bit symmetric key, used to provide a second layer of encryption to sensitive user data while it is in transit. These keys are distributed securely to the safes during initial configuration, using the safe's public key.

KEY STORAGE

Cryptographic keys are stored in a dedicated Secure Element, to ensure they cannot be leaked or compromised, even by an attacker with physical access to the device.

LIFECYCLE MANAGEMENT

Device keys, used for encrypting temporary state information (AES-256), are rotated every 30 seconds. Our cloud certificates are rotated every 90 days. Device X.509 certificates are rotated every 365 days. Keys are securely erased when they are retired (NIST SP-800-57, Part 1).

medixsafe

WWW.MEDIXSAFE.COM ▪ 1-855-633-4972 ▪ SECURITY@MEDIXSAFE.COM

REV. 2025-08-25