HIPAA PRIVACY & SECURITY WHITE PAPER

JANUARY 2017

44 Tehama Street
San Francisco CA
94105

+1.415.770.2020

legal@captureproof.com

TABLE OF CONTENTS

OVERVIEW

CAPTURE_PROOF implements a number of measures to ensure the privacy and security of the health information held and transmitted.

In our implementation of privacy and security protocols for health information security, *CAPTURE_PROOF* is **HIPAA, NIST 800-53, FIPS, and US-EU Privacy Shield Compliant**. *CAPTURE_PROOF* reviews our policies and implementation of policies annually with the aim of meeting and exceeding industry standards for health information security.

CAPTURE_PROOF's Governance policies are designed to ensure the appropriate security of all health information across the environment, in compliance with existing laws. Information Security and complying with HIPAA and HITECH are an integral part of our business operations, therefore *CAPTURE_PROOF* has established a program of sufficient rigor to address its own compliance requirements while also meeting the expectations of its customers.

The Federal Information Processing Standard (FIPS) are a set of standards that describe document processing, encryption algorithms and other information technology standards for use by government contractors and vendors who work with the agencies, and need to demonstrate security standards consistent with those used by US government agencies. *CAPTURE_PROOF* meets and exceeds these standards.

The NIST publications are voluntary guidelines and best practices for state, local, and tribal governments and the private sector, which provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in information systems. *CAPTURE_PROOF* uses these guidelines as standards in meeting and exceeding our security obligations under HIPAA.

Finally, *CAPTURE_PROOF* complies with the US-Swiss Safe Harbor Framework and US-EU Privacy Shield Framework as regulated by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. *CAPTURE_PROOF* has certified that it adheres to these frameworks' Safe Harbor Privacy Principles.

This white paper is a high-level overview of the security and privacy protocols in place, and their implementation by *CAPTURE_PROOF* to ensure the integrity of health data transmitted and stored by and within the *CAPTURE_PROOF* platform.

SECURITY FRAMEWORK & STANDARDS

Control frameworks and security standards are often interchangeable terms depending upon the creator. For the purposes of this white paper, control frameworks, controls, and standards are interchangeable, as the "intent" of each of them is to provide some definition to a practice or set of practices that if performed, will protect the organization's information assets. These consist of documented, executed, tested, implemented, and monitored controls which reduce the risk of threats to the *CAPTURE_PROOF* platform.

HIPAA

In the U.S., certain organizations, called covered entities, that create, maintain, transmit, use, and disclose an individual's protected health information (PHI) are required to meet Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements. Individuals or entities, like *CAPTURE_PROOF* who perform certain functions or activities as a service to a covered entity, are termed "Business Associates", and are equally expected to meet the requirements of HIPAA.

Under HIPAA's Privacy Rule, *CAPTURE_PROOF* restricts uses and disclosures of PHI, creates individual rights with respect to their PHI, and implements security- focused administrative requirements. Among other requirements, under the HIPAA Privacy Rule, *CAPTURE_PROOF* also implements reasonable safeguards for PHI to prevent any intentional or unintentional use or disclosure that is in violation of the requirements of HIPAA.

Under HIPAA's Security Rule *CAPTURE_PROOF* operates to ensure the confidentiality, integrity, and availability of its ePHI, to protect against reasonably anticipated threats or hazards to the security or integrity of its ePHI, to protect against reasonably anticipated impermissible uses and disclosure of its ePHI, and to ensure compliance by our employees with these standards. Additionally, the Security Rule requires *CAPTURE_PROOF* to put in place detailed administrative, physical, and technical safeguards to protect ePHI. To do this, covered entities are required to implement access controls and set up backup and audit controls for electronic PHI in a manner commensurate with the associated risk.

CAPTURE_PROOF is fully compliant with HIPAA, and holds Business Associate Agreements with all Covered Entities and other Business Associates we work with to ensure those we partner with, are held to the same security and privacy standards with which hold our user's data.

NIST 800-53

The National Institute of Standards and Technology (NIST) Special Publication 800-53, entitled, "Recommended Security Control for Federal Information Systems", breaks security controls into 17 control "families" and three "classes" (Managerial, Operational, Technical) of controls.

CAPTURE_PROOF uses this control framework to meet security, privacy, and breach notification standards as outlined by HIPAA. *CAPTURE_PROOF* uses these standards as our minimum standards for controls to be implemented to protect the *CAPTURE_PROOF* platform, based on risks assessed.

FIPS

FIPS, or Federal Information Processing Standards, ensures *CAPTURE_PROOF's* compliance with federal security and data privacy requirements. FIPS are developed by the National Institute for Standards and Technology (NIST) to use when no voluntary standards exist to meet federal requirements. They address: the compatibility of different systems, the portability of data and software, cost-effective computer security; and privacy of sensitive information in federal computer systems. The CAPTURE_PROOF platform's infrastructure is FIPS compliant.

US-EU PRIVACY SHIELD COMPLIANT

CAPTURE_PROOF respects and treats personal data on a level equal to or exceeding the principles set forth in the US/EU Privacy Shield and the US/Swiss Safe Harbor. *CAPTURE_PROOF* shall annually self-certify with the US Department of Commerce that it has met these principles and shall provide a link to the Privacy Shield list. *CAPTURE_PROOF* agrees to be subject to the enforcement and investigatory powers of the U.S. Federal Trade Commission for these purposes.

When *CAPTURE_PROOF* collects personal information directly from individuals in the EEA or Switzerland, we commit to protecting the security and integrity of the information. We commit to informing them about the types of data we collect about them, the purposes for which we use the data, the right to access their own personal data, the types of third parties to which we disclose the data, the choices and means, if any, that we offer for limiting their use and disclosure of personal information about them, and how subjects covered by this policy can contact CAPTURE_PROOF with any inquiries or complaints. We commit to responding to complaints from individuals within 45 days, to participation in dispute resolution free of charge to the individual, and, in certain circumstances, to submission to binding arbitration. We may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. CAPTURE_PROOF commits to reporting the approximate number of requests to access personal data by public authorities. We commit to protecting personal data when transferred to third-party agents by contractually requiring those agents to provide the same level of protections.

Notice of these rights and obligations will be provided, in clear and conspicuous language, when individuals are first asked to provide personal information to *CAPTURE_PROOF*, or as soon as practicable thereafter, and in any event before *CAPTURE_PROOF* uses or discloses the information for a purpose other than that for which it was originally collected.

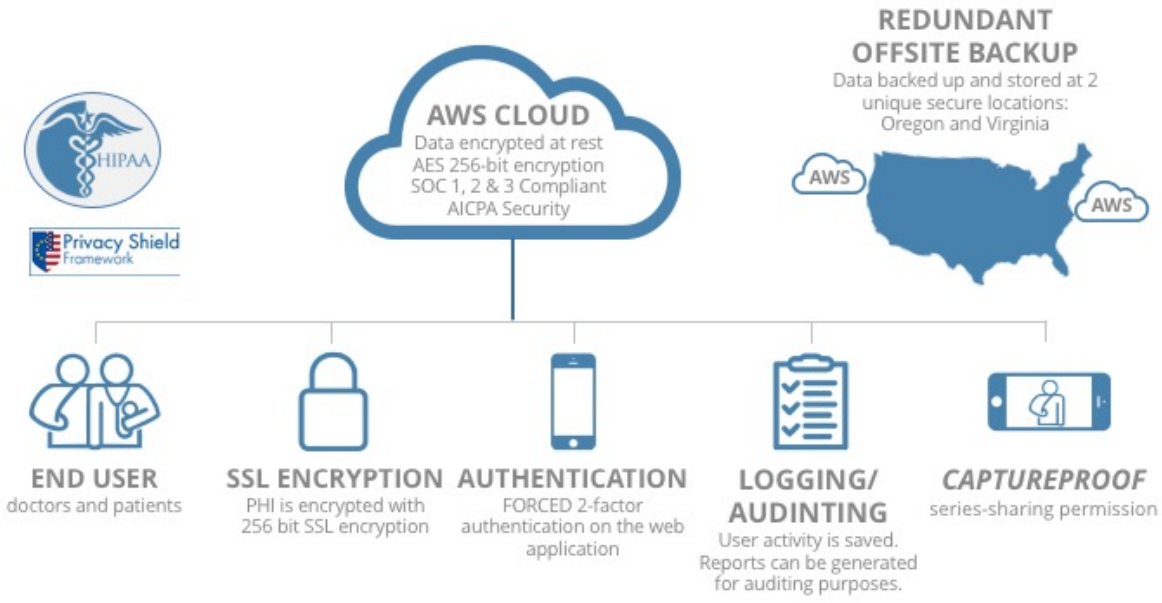
Where *CAPTURE_PROOF* receives personal information from its subsidiaries, affiliates or other entities in the EEA or Switzerland, *CAPTURE_PROOF* uses that information in accordance with the notices those entities provided to the individuals to whom that personal information relates, and the choices made by those individuals.

KEY SECURITY & PRIVACY ELEMENTS

At *CAPTURE_PROOF* we are very confident that we have industry leading security in place. We do not deal with physical PHI, rather all patient data onto our platform exists in electronic form as ePHI.

END-TO-END SECURITY: FOLLOW THE DATA

One of the best ways to understand the multiple levels of security in the *CAPTURE_PROOF* platform, is to review the path of a photo or video from end user (Health Care Provider or Patient) to our cloud storage, noting that any data transmitted or at rest is encrypted. This process and its key security features at each stage are mapped out in Figure A.



USER ACCOUNTS

User accounts are password protected. Upon successful entry of a unique username, password and authentication token granted through mobile SMS, the user then gains access to his or her account.

Except as stated in the next sentence, *CAPTURE_PROOF* employees are prohibited from viewing the content of files you store in a user's *CAPTURE_PROOF* profile, and are only permitted to view file metadata (e.g., file names and locations).

Only a limited set of employees with advanced Security and Privacy Training have access to user data for the reasons specifically stated within *CAPTURE_PROOF* Privacy Policy, namely when *CAPTURE_PROOF* is legally required to do so.

In these limited circumstances, there is strict policy and technical access controls that prohibit employee access except in these rare circumstances.

SECURE TRANSFERS

Your files are sent from *CAPTURE_PROOF's* mobile and web apps to our servers over a secure channel using SSL encryption, the standard for secure Internet network connections.

AUDITING & LOGGING

CAPTURE_PROOF's auditing process tracks all records that are created, deleted and modified. It also tracks activity on the site by users, such as, login, page view, viewing images, adding notes and other activity on the site by Patients and Medical Professionals.

BAA WITH AMAZON WEB SERVICES

CAPTURE_PROOF currently has a signed Business Associate Agreement (BAA) with Amazon Web Services (AWS). Amazon's Security White Paper can be found here. aws.amazon.com/whitepapers

As *CAPTURE_PROOF* has built a system on top of the AWS cloud infrastructure, our compliance responsibilities are shared. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS provides assurance related to the underlying infrastructure and *CAPTURE_PROOF* owns the compliance initiatives related to anything placed on the AWS infrastructure.

SECURE STORAGE & RESERVED INSTANCES

All data stored in our databases is symmetrically encrypted using AES 256 keys. Amazon Web Services stores data over several large-scale data centers. You can find more information about Amazon Web Services' security at the Amazon Web Services' website. Encryption keys are stored using further encryption.

DATA BACKUPS

CAPTURE_PROOF and Amazon Web Services keep redundant backups of all data over multiple locations to prevent the remote possibility of data loss.

HIPAA SECURITY STANDARDS

CAPTURE_PROOF is HIPAA compliant. The following is a shortlist, of the NIST controls used to ensure the privacy and security of PHI transmitted and held by the *CAPTURE_PROOF* platform.

NIST security controls have a well-defined structure, and serve as a standard by which *CAPTURE_PROOF* defines the infrastructure necessary to ensure the privacy and security of our user's

data in addition to complying with health and personal information privacy laws, including, but not limited to HIPAA and the EU/Swiss-US Safe Harbor Principles.

According to the NIST framework, the security controls are organized into classes and families for ease of use in the control selection and specification process. *CAPTURE_PROOF* implements these three general classes of security controls (i.e., technical, administrative and physical).

HIPAA TECHNICAL SAFEGUARDS

This is a snapshot of *CAPTURE_PROOF's* technology, and the policy and procedures for its use that protect PHI and control access and prevent unauthorized access to it. These outline some, but not all, of *CAPTURE_PROOF's* technical safeguards.

This is just a sampling of our technical safeguards in place, for more information please contact: security@captureproof.com

NIST ACCESS CONTROL STANDARDS 164.312(a)

Unique User Identifications:	• users are identified with a randomly generated user authentication number • the number, not visible to users, is used for logging and auditing actions within the platform
Emergency Access Procedure	• emergency access protocol outlining individuals authorized to trigger protocol and implement manual processes • outlined processes support continuity of operations
Encryption, Decryption, and Automatic Logoff	• all ePHI is encrypted at rest using AES SHA256 cipher and hash • ePHI in transit, encrypted (256-bit SSL with TLS 1.2) • 2-factor auth login and automatic log out after 10 min of inactivity on web

NIST ACCESS CONTROL STANDARDS 164.312(c)1

Mechanisms to Authenticate ePHI	• Amazon S3 regularly verifies the integrity of data stored using check sums • Amazon S3 calculates check sums on all network traffic to detect corruption of data packets when storing or retrieving data
Identify Users Authorized to Access ePHI	• all users must authenticate via both password and 2-factor auth, for both front and back end access • media Rx are owned by one patient and one/many clinicians • ePHI can be added to the system but cannot be deleted • all access to front and back end of platform is audited
Assess Data Integ Process	• internal monitoring systems look at real-time access logs to ensure processes are working as required – revisions made accordingly

NIST ACCESS CONTROL STANDARDS 164.312(b)

Identify Activities to be Tracked or Audited	*CAPTURE_PROOF* audits at minimum: • login attempts, failures, and successes • when ePHI is created, updated, or destroyed • when user information changes • when ePHI is accessed
Developed Standard Operating Procedure	*CAPTURE_PROOF* audits: • network vulnerabilities • breaches in confidentiality and security of PHI • performance problems and flaws in applications. • improper alteration or destruction of ePHI (information integrity). • data from logs and audit trail are used to generate exception reports quarterly
Implement the Audit/System Activity Review Process	• *CAPTURE_PROOF* audits access and activity • Logs are generated daily, weekly and monthly

HIPAA ADMINISTRATIVE SAFEGUARDS

Physical measures, policies, and procedures are used to manage the selection, development, implementation, and maintenance of PHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information. This is just a sampling of our technical safeguards in place, for more information please contact: security@captureproof.com

NIST SECURITY MGMT PROCESS 164.308(A)(1)(I)

Risk Assessment and Risk Management Program	• conduct regular vulnerability scans using industry standard vulnerability scanning tools • daily, weekly, monthly, and quarterly scans with an increasing scan depth • active notification system is in place to alert for changes in infrastructure integrity – directed to Security Officer

INFORMATION ACCESS MGMT 164.308(A)(4)(I)

Access Authorization Back-End Access	• identity-based and role-based access controls implemented • clear procedure for documentation, review and modification of user's access rights
Access Authorization Front-End Access	• direct access to ePHI enabled by *CAPTURE_PROOF*, to patient owner of ePHI, and care teams he/she consents to be shared media

NIST DATA BACKUP PLAN 164.308(A)(7)(II)(A)

Data Backup Plan and Disaster Recovery Plan	• *CAPTURE_PROOF* regularly backs up ePHI by encrypting it and storing it in multiple, geographically separate locations via AWS • formal agreements/BAAs are in place with any external organizations • AWS is SAS 70 II certified enabling *CAPTURE_PROOF* to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Zone is designed as an independent failure zone • procedures in place to enable restoration of any data loss • AWS' Business Continuity Plan (BCP) supports ongoing, worldwide business and the ability to scale to the increased scope of catastrophic events • *CAPTURE_PROOF* has contingency procedures and strategies which address allowable outage times

HIPAA PHYSICAL SAFEGUARDS

Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. This is just a sampling of *CAPTURE_PROOF's* physical safeguards in place, for more information please contact: security@captureproof.com

NIST FACILITY ACCESS CONTROLS 164.310(a)(1)

Facility Security Plans	• no PHI stored physically at *CAPTURE_PROOF* facilities • clear policies in place to safeguard company facilities and equipment from unauthorized physical access, and theft • AWS has SAS 70 II certification • at AWS, physical access is controlled using professional security staff utilizing video surveillance, intrusion detection systems, etc.

NIST WORKSTATION USE/SECURITY 164.310(b)-(c)

Workstation Function ID and Safeguard Implementation	• clearly identified workstation protections for those personnel authorized to access ePHI • Key technology safeguards for all *CAPTURE_PROOF* workstations: • full HDD encryption • auto lock workstations after 5 min • auto log out after 10 minutes

CAPTURE_PROOF SECURITY & PRIVACY POLICIES

You can find our Terms and Conditions, Security & Privacy Policy, Acceptable Use Policy, and Safe Harbor Privacy Policy at: captureproof.com/home/terms.html

By using *CAPTURE_PROOF's* Services, our users are agreeing to be bound by the Terms found on this page. *CAPTURE_PROOF* occasionally revises these terms from time to time, and the most current version will always be posted on our website.

CAPTURE_PROOF COMPANY PROFILE

CAPTURE_PROOF is the HIPAA compliant platform for patients and providers to communicate remotely using chat, photos and videos. Patients use CAPTURE_PROOF to show-and-tell symptoms allowing providers the ability to see what the patient is describing. Patients don't have to struggle to explain their symptoms, and providers don't have to guess what the symptoms look like. For more information on how to get CAPTURE_PROOF set up for your institution.

Contact Us: +1.415.770.2020

Email Us: support@captureproof.com

Visit Us Online: captureproof.com

DISCLAIMER

This white paper is not intended to constitute legal advice. You are advised to seek the advice of legal counsel regarding compliance with HIPAA, HITECH, EU PRIVACY SHIELD and other laws that may be applicable to you and your business.