Valid Through: January 1, 2024

Live Compliance

# Statement of Satisfactory Assurances of HIPAA Compliance

## EZClaim Software LLC (“EZClaim”) Designated HIPAA Security and Compliance Contacts:

**Mr. James Johnson**
Address: 101 N. Tryon St., Suite 112 Charlotte NC, 28246
Contact Phone: (980) 999-1585
Email Address: admin@livecompliance.com

**Mr. Ed Graf**
Address: 540 Devall Drive, Suite 301 Auburn AL, 36832
Email Address: edward.graf@fullsteam.com

## Satisfactory Assurance from EZClaim Software LLC (“EZClaim”)

45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)
In accordance with the final rule, covered entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, no matter how far down the chain the information flows.

EZClaim, as of the date of this document, has acquired updated business associate agreements from business associates and subcontractors. Additionally, EZClaim has acquired or is currently seeking satisfactory assurances of HIPAA compliance from each of our subcontractors.

## Workforce Training

§164.308(a)(5) Required
All EZClaim workforce members have received HIPAA security and privacy training including the latest Omnibus revisions to the HIPAA final Rule. Live Compliance administers workforce training and exams. All training, exams and certifications are retained for all employees. Furthermore It is the policy and procedure of EZClaim as follows:

Policy - Security awareness and training ensures that all workforce members are aware of our security policies and procedures and have been trained on security and privacy issues. It is the Policy of EZClaim to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, temporary workers, and volunteers.

HIPAA training shall be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with individually identifiable health information. All new hires will be provided HIPAA training via the Live Compliance portal and a posttest on the material covered within the training course to ensure comprehension of relevant and appropriate HIPAA policies and procedures. A minimum passing grade of 80% will be required.

The Security Officer is responsible for carrying out these requirements in a timely manner according to the following procedure.

Procedure - The designated Security Officer will conduct and document security training for new workforce members when they are hired.

Any workforce member who identifies potential security problems within the facility that can be corrected by additional training should immediately notify the Security Officer. HIPAA training, at minimum, shall include the basics of HIPAA itself; the basics of HIPAA's privacy and security requirements and restrictions; and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.

HIPAA training shall also include a review of the Workstation Use and Security Policy; a review of the Sanction Policy; a review of contingency and emergency mode operations plans; a review of HHS HIPAA Investigations Policy; PHI Uses and Disclosures Policy; and a review of relevant and appropriate technical security measures.

All Training Records will be kept for a minimum of 6 years. HIPAA training shall be conducted periodically for all employees, but no less than once per year.

In addition to the initial security and privacy training EZClaim will disseminate periodic security reminders.  Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training.

We will use them in the following:

- Security Reminders are part of our staff meetings
- Security Reminders are posted on the company intranet
- Conduct security training whenever there are changes in the security environment and as needed to keep the staff up-to-date on how confidential information is handled.

Advise all non-workforce members on our security and privacy policies and require a current Business Associate Agreement prior to permitting access of PHI.

## Security Risk Assessment, Risk Analysis and Remediation:

HIPAA itself is a set of guidelines rather than hard-set / well-defined rules.  Some of the areas HIPAA focuses on are not to be tested via automated processes and require manual examination. HIPAA control points are often high level and lack specific values to check for. In cases where controls are examined which contain explicit values, these queries use values taken from other public standards and benchmarks.

EZClaim Technical, Subjective and Objective Security Risk Analysis, Physical Safeguards Risk Assessment and analysis, Organizational Administrative Risk Analysis and HIPAA Management Plan for all EZClaim locations have been accurately, thoroughly performed and reviewed and are monitored regularly.

EZClaim conducts routine comprehensive technical vulnerability scans and audits using an industry-leading objective vulnerability scanner to identify and remediate potential security vulnerabilities in our systems and applications per HIPAA Security Rule requirements. Vulnerability scanning and remediation is performed continuously, with more comprehensive scans conducted on at least a monthly basis.

Administrative safeguards such as risk management, training, and policies and procedures are reviewed and updated annually at a minimum. Additional focused audits on physical safeguards, technical safeguards, and other administrative areas are performed periodically. Audit reports are analyzed to identify deficiencies and implement corrective actions for ongoing improvement.

## HIPAA Security and Privacy Policies and Procedures

Overview of EZClaim's HIPAA Privacy and Security Policies and Procedures

| | |
|---|---|
| **Documentation policy**<br>§164.530(J)(1)(II) §164.312(B)(2)(I)<br>**Termination procedure**<br>§164.308(A)(3)(II)(C)<br>**Sanction policy**<br>§164.308(A)(1)(II)(C)<br>**Workforce clearance procedure**<br>§164.308(A)(3)(II)(B)<br>**Authorization and supervision procedure**<br>§164.308(A)(3)(II)(A)<br>**Employee training**<br>§164.308(A)(5)<br>**Assigned security officer**<br>§164.308(A)(2)<br>**Risk assessment and risk management**<br>§164.308(A)(1)<br>**Information system activity review**<br>§164.308(A)(1)(II)(D)<br>**Security reminders**<br>§164.308(A)(5)(II)(A)<br>**Access authorizations**<br>§164.308(A)(4)(II)(B)<br>**Clearinghouse functions**<br>Addressable<br>**Access establishment and modification**<br>§164.308(A)(4)(II)(C)<br>**Log-in monitoring**<br>§164.308(A)(5)(II)(C)<br>**Password management**<br>§164.308(A)(5)(II)(D)<br>**Protection from malicious software**<br>§164.308(A)(5)(II)(B)<br>**Contingency plan**<br>§164.308(A)(7)<br>**Data backup plan standard; contingency plan**<br>§164.308(A)(7)(II)(A) | **Audit controls**<br>§164.312(B)<br>**Person or entity authentication** §164.312(D)<br>**Person or entity authentication** §164.312(D)<br>**Encryption and decryption**<br>**Encryption**<br>§164.312(E)(2)(II)<br>**Integrity controls**<br>§164.312(E)(2)(I)<br>**Transmission security**<br>§164.312(E)(1)<br>**Mechanism to authenticate ePHI**<br>§164.312(C)(2)<br>**Evaluation of business associates**<br>**Satisfactory assurance from business associates**<br>**Marketing to patients**<br>**Sale of PHI**<br>**Sensitive health information of the deceased**<br>**Fundraising**<br>**Incidental disclosures of PHI**<br>**Written consent to disclose PHI**<br>**Minimum necessary rule**<br>**Restriction of access to PHI**<br>**Notice of privacy practices**<br>**Access to PHI**<br>**Alternative communication of PHI**<br>**Privacy training**<br>**Disaster recovery plan (standard: contingency plan)** §164.308(A)(7)(II)(B) |

EZClaim routinely reviews policy decisions as the technology marketplace and physical attributes of our organization changes.

## Specific Responsibilities of the Security Officer include, but are not limited to:

- Ensuring that Security Risk Assessment is conducted initially and repeated periodically as needed
- Developing and implementing appropriate policies and procedures based on the Risk Assessment
- Completing and maintaining an up-to-date inventory of hardware and software with ePHI and access
- Ensuring that the organization information assets are protected by implementing and enforcing:
    - Our security policies and procedures
    - Directing and carrying out the Security Objectives of the policies and procedures
    - Maintaining and reviewing documentation of levels of access
    - Investigating all security incidents. In the event that unsecured protected information is "breached" and the use of the information poses a significant risk of financial, reputable or other harm, we will notify patients of the situation and the steps needed to protect themselves against harm due to the breach. We will inform HHS and take any other steps required by law.
    - Working to ensure that Business Associate Contracts are up-to-date and are in place for all vendors, associates and other entities that require access to Protected Health Information.
    - Training workforce members on our security policies and procedures and ensuring compliance by enforcing our sanction policies.
    - Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the HIPAA Compliance Officer, administration, and legal counsel as applicable.
    - Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
    - Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
    - Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
    - Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
    - Analyze the security of the facility and implement devices, tools, and techniques to strengthen our facility security to a reasonable level, in order to safeguard the facility and equipment therein from disasters, unauthorized physical access, tampering, and theft.
    - Plan, analyze, test, update, and execute all contingency operations, disaster recovery plans, emergency mode operations plans, and emergency access procedures.

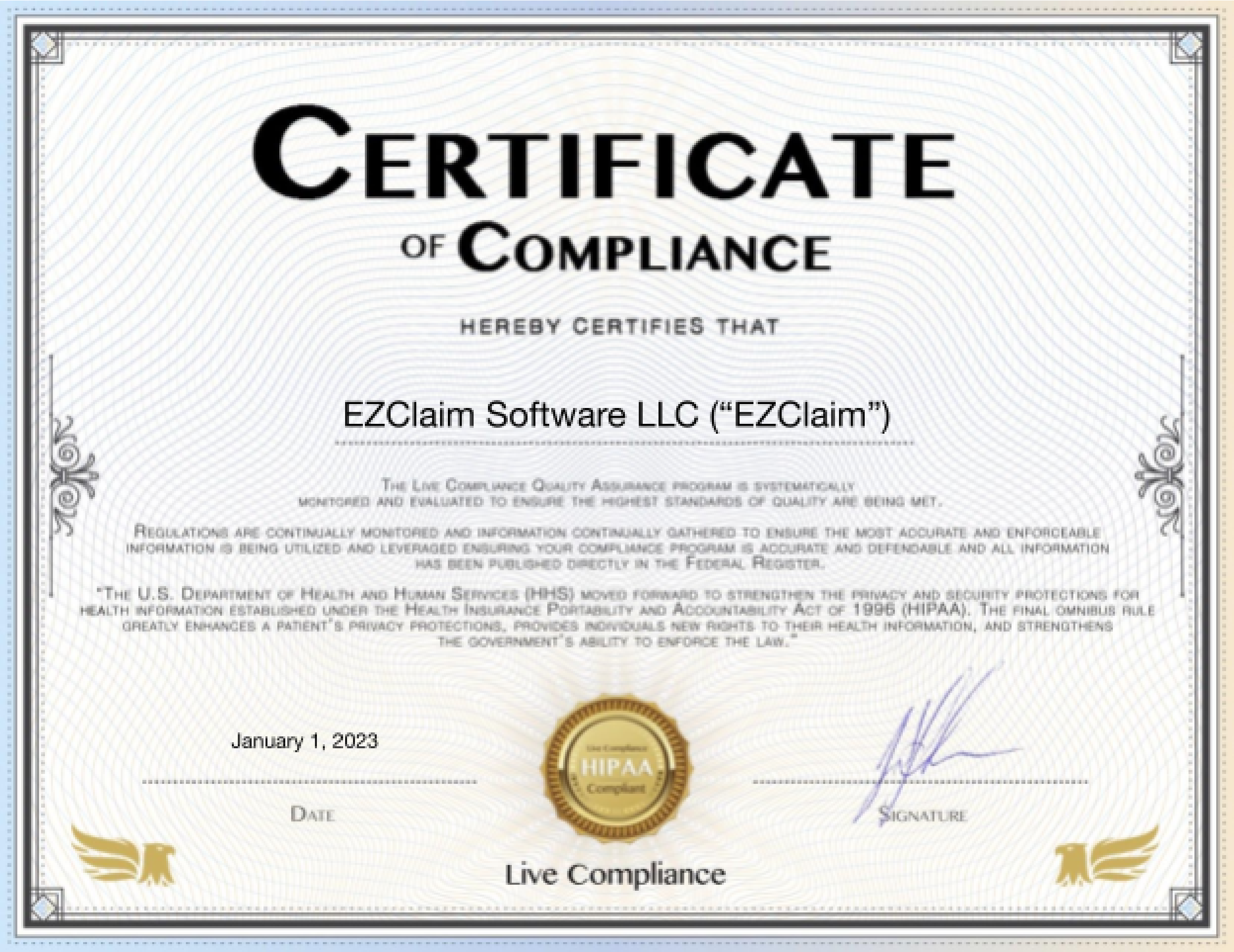
- Review all contracts under which access to confidential data is given to Live Compliance, bring those contracts into compliance with the Privacy and Security Rules, and ensure that confidential data is adequately protected when such access is granted.
- Ensure that all policies, procedures, and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- Ensure that future initiatives are structured in such a way to ensure client privacy and security.
- Conduct periodic privacy audits and take remedial action as necessary.
- Oversee employee training in the area of privacy and security.
- Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
- Remain up-to-date and advise on new technologies to protect data privacy and security.
- Remain up-to-date on laws, rules, and regulations regarding data privacy and security, and update policies and procedures as necessary.
- Anticipate client concerns and questions about our use of their confidential information and develop policies and procedures to respond to those concerns and questions.

Valid Through: January 1, 2024

Live Compliance

**Compliance consultant and compliance maintenance and third party assessor.**

**Live Compliance, LLC**
http://www.LiveCompliance.com
Phone: (980) 999-1585
Email: info@LiveCompliance.com



# CERTIFICATE

## OF COMPLIANCE

HEREBY CERTIFIES THAT

EZClaim Software LLC (“EZClaim”)

THE LIVE COMPLIANCE QUALITY ASSURANCE PROGRAM IS SYSTEMATICALLY MONITORED AND EVALUATED TO ENSURE THE HIGHEST STANDARDS OF QUALITY ARE BEING MET.

REGULATIONS ARE CONTINUALLY MONITORED AND INFORMATION CONTINUALLY GATHERED TO ENSURE THE MOST ACCURATE AND ENFORCEABLE INFORMATION IS BEING UTILIZED AND LEVERAGED ENSURING YOUR COMPLIANCE PROGRAM IS ACCURATE AND DEFENDABLE AND ALL INFORMATION HAS BEEN PUBLISHED DIRECTLY IN THE FEDERAL REGISTER.

“THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) MOVED FORWARD TO STRENGTHEN THE PRIVACY AND SECURITY PROTECTIONS FOR HEALTH INFORMATION ESTABLISHED UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA). THE FINAL OMNIBUS RULE GREATLY ENHANCES A PATIENT'S PRIVACY PROTECTIONS, PROVIDES INDIVIDUALS NEW RIGHTS TO THEIR HEALTH INFORMATION, AND STRENGTHENS THE GOVERNMENT'S ABILITY TO ENFORCE THE LAW.”

January 1, 2023
DATE

Live Compliance
HIPAA
Compliant

SIGNATURE

Live Compliance

*Authenticity Tracking-*
*ba145f622b0b15b5b0b31eb95110b64b*