eFMLA, Inc.
7406 Alban Station Court, Suite B-210
Springfield, VA. 22150

Data Privacy and Security Policy

Protecting the privacy and security of our client's confidential data information is a top priority for eFMLA, Inc. This Data Privacy and Security Policy governs data collection, storage and usage and applies to:

- https://www.efmla.com,
- https://ww4.efmla.com
- https://www2.efmla.com and
- eFMLA, Inc.

For the purposes of this Data Privacy and Security Policy, unless otherwise noted, all references to "eFMLA", or "eFMLA, Inc." are interchangeable and include https://www.efmla.com and https://ww4.efmla.com. The eFMLA website is a Software Support Services site, consisting of an interactive user interface for clients' authorized users, including FMLA administrators, employees and selected health care providers. The site is encrypted and secured with SSL. By using the eFMLA website, clients consent to the data practices described in this policy.

1.0 Collection of Personally Identifiable Information

eFMLA, Inc. does not collect any personal information about our clients, their administrators, or their employees unless it is voluntarily provided. In order to provide clients with the services offered, eFMLA may collect Personally Identifiable Information ("PII") as part of processing Family Leave Medical Act (FMLA) related notices, certification and forms, such as the client's employees':

- First and Last Name;
- Mailing Address;
- E-mail Address;
- Telephone Number; and
- Work location.

Clients, FMLA administrators, clients' employee, and health care providers must provide certain PII in order to effectively utilize eFMLA's services. For example, eFMLA will use such information to facilitate and effectuate communications between clients and their employees, between and employee and the employee's health care provider(s) (or an employee's covered family members' health care provider(s)) in relation to services the client and/or its employees have requested from eFMLA.

2.0 Use of Personally Identifiable Information

eFMLA will collect and use PII solely to operate and deliver the services requested by the client, the client's FMLA administrators or its employees.

2.1 Data Storage

Employee data is stored in a secure database that is only accessible by the eFMLA software.

- The primary datacenter utilizes a hardened building within another building.
- Internet access is provided from 5 sources over diverse fiber paths.
- Redundant power is provided by large APC UPS systems plus backup power generators.
- Datacenter is built out of non-combustible materials, and has gas fire suppression.
- Physical access to the datacenter interior is restricted behind locked doors to a limited number of staff, equipment cabinets are all locked when not being worked on, numerous security cameras record access 24/7 inside and outside of the datacenter.
- Data from the server is backed up to multiple locations at the primary datacenter on a daily basis. In addition, data is automatically backed up to a full-disk-encrypted offsite backup file server on a regular basis. The offsite backup server cannot be booted up or its data read without password entry from an attached keyboard. In the event of a full loss of the primary datacenter in a disaster, the remote backup will be used to restore operation of the service.

The data is stored for as long as client desires or until we are asked to delete it by an authorized representative from the client. The entire data set is archived/backed-up locally every hour and offsite daily to a secure commercial storage vault. See Section 4.5 below for the 'Right to Deletion'.

The information in the database is stored in a secure database and the data is passed between encrypted channels through HTTPS.

2.2 Database Overview

The system was designed to require users to provide the minimum amount of PII possible to enable clients to (a) fully utilize the eFMLA software, (b) process requests for FMLA leave from employees, (c) communicate with employees regarding FMLA or other leaves of absence, (d) provide FMLA notices and forms, and related documents to employees, and (e) to enable employees and FMLA administrators to send and receive medical certifications to health care providers.

In addition:

- Only demographic information is contained/required by the system which is available in the public domain. Note: Some records may contain PII if said information was entered by the employee or FMLA administrator directly into the eFMLA database within one of several 'Other or More Information Needed' freeform input fields.
- No Social Security Numbers (SSN) are required by the system.
- There is no payment information, other than date paid, amount paid, check number or CC last 4, stored in the eFMLA databases.

3.0 Nondisclosure of Information with Third Parties

eFMLA will not sell, rent or lease its customer lists to third parties. In addition, neither eFMLA nor its employees, officers or business associates will share any PII with any third party at any time. All such PII will be held strictly confidential. eFMLA may send clients emails to provide customer support. All such third parties with whom eFMLA conducts business are prohibited from using any information in the eFMLA system except to provide those services to eFMLA, and they are required to maintain the confidentiality of any PPI.

4.0 Computer Information

Information about clients' computer hardware and software is not collected by eFMLA.

4.1 Use of Cookies

The eFMLA website may use "cookies" to help clients, FMLA administrators and employees personalize their online experience. A cookie is a text file that is placed on your hard disk by a web page server. Cookies cannot be used to run programs or deliver viruses to clients' computers. Cookies are uniquely assigned to the client, and can only be read by a web server in the domain that issued the cookie.

Individual users have the ability to accept or decline cookies. Most Web browsers automatically accept cookies, but users generally have the option modify their browser settings to decline cookies. If the user chooses to decline cookies, the user may not be able to fully experience the interactive features of the eFMLA services.

4.2 Security of Personally Identifiable Information and HIPAA

eFMLA secures PII from unauthorized access, use, or disclosure. eFMLA uses the SSL Protocol method for this purpose: When personal information is transmitted to our websites, it is protected through the use of encryption, such as the Secure Sockets Layer (SSL) protocol. Secure Sockets Layer (SSL), is cryptographic protocol designed to provide communications security over a computer network. When secured by an SSL connection between a client (e.g., a web browser) and a server

(https://www,efmla.com/), the connection is private (or secure) because a symmetric-key algorithm is used to encrypt the data transmitted. As such, the transmission of information meets the requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 relating to electronic health records. As such, the use of eFMLA also meets the Security and Privacy Rules of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), regarding the security of protected health information (PHI) and electronic PHI (ePHI), including, but not limited to, the electronic storage and transmission of medical records, and procedures in the event of a data breach. All ePHI obtained and stored in the eFMLA software will be held strictly confidential and will not be shared with any third party except as permitted and authorized by law.

However, the eFMLA system may share data with a health care provider designated by a client's employee as authorized to complete a medical certification form. It is the clients' obligation, the obligation of client's employees and the obligation of health care providers, to comply with FMLA regulations and HIPAA as applicable to the FMLA certification process.

4.3 Unauthorized Access

eFMLA strives to take appropriate security measures to protect against unauthorized access to or alteration of PII. However, no data transmission over the Internet or any wireless network can be guaranteed to be absolutely secure from any data breach. As a result:

(a) There are security and privacy limitations inherent to the Internet that are beyond the control of eFMLA; and
(b) The security, integrity, and privacy of any and all information and data transmitted through the eFMLA Site cannot be absolutely guaranteed.

4.4 Data Breach Policy

If a data breach were to occur, eFMLA will promptly (within five (5) business days of becoming aware of the breach) notify its clients so they are aware. eFMLA will reset all user passwords and take other mitigation and damage control measures as required by law. No known data breach has ever occurred during the time eFMLA has been in operation.

4.5 Right to Deletion

Subject to certain exceptions set out below, on receipt of a verifiable request from a client organization, eFMLA will delete all PPI, PHI and ePHI from its records. Please note that eFMLA may not be able to comply with requests to delete such information if it is necessary to:

- Complete the transaction for which the information was collected, provide a service requested by you, or reasonably anticipated within the context of our

ongoing business relationship with the client, or otherwise perform a contractual obligation between the client and eFMLA;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- Comply with the California Electronic Communications Privacy Act or any other State or federal communications or related law;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when our deletion of the information is likely to render impossible or seriously impair the achievement of such research, provided we have obtained the client's informed written consent;
- Enable solely internal uses that are reasonably aligned with client's expectations in assisting with the administration of FMLA and related services as requested;
- Comply with an existing legal obligation; or
- Otherwise use PPI internally in a lawful manner that is consistent with the context in which the client or its FMLA administrators, employees or health care providers provided the information.

5.0 E-mail and Telephonic Communications

eFMLA will only contact clients' employees via email or phone for the purpose of providing announcements, alerts, confirmations, technical support, FMLA administration support, and/or other general communication related to the use of eFMLA system.

6.0 External Data Storage Sites

eFMLA may store clients' data on servers provided by third party hosting vendors with whom it has contracted.

7.0 Changes to this Statement

eFMLA reserves the right to change this Data Privacy and Security Policy from time to time. eFMLA will notify clients regarding any significant changes in the way in which PPI, PHI or ePHI is obtained or stored by sending a notice to the primary email address specified in each client's account, and/or by placing a prominent notice on the 'Main Menu' page of the eFMLA website. A client's continued use of the eFMLA website and/or Services available after such modifications will constitute the client's acknowledgment of the modified Policy agreement to abide and be bound by that Policy.

8.0 Contact Information

eFMLA welcomes clients' questions or comments regarding this Policy. If you have any questions or concerns, or believe that eFMLA has not adhered to this Policy, please contact eFMLA at:

eFMLA, Inc.
7406 Alban Station Court
Suite B-210
Springfield, Virginia 22150

Email Address: support@efmla.com

Telephone number: 855-488-3652

Effective Date: 01/01/2022