Jewish Family Service of San Diego Privacy and Security Policy And Training Certification

Policy:

It is the policy of Jewish Family Service of San Diego (JFS) to maintain the privacy and security of protected information our clients, volunteers and employees entrust to us. Additionally, JFS is aware of and abides by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations, other relevant federal and state law, and the contractual privacy and security requirements to which JFS must comply.

JFS' privacy and security policy is carried out in administrative, technical and physical safeguards intended to ensure the security, integrity, confidentiality, and availability of client health care, case management, and related information. The purpose of these safeguard measures is to protect against reasonably foreseeable threats or hazards to the security of the information, and to protect against unauthorized uses or disclosure of the information.

It is the policy of JFS that all members of the JFS workforce who obtain or have access to protected health information (PHI), personal information (PI) and personally identifiable information (PII) shall adhere to the standards necessary to comply with HIPAA and other privacy laws, including those in JFS' Privacy and Security Plan. Violation of HIPAA requirements and/or the standards in the Plan by members of the workforce will result in disciplinary action up to and including termination of employment or immediate dismissal of unpaid members of the workforce, and civil and/or criminal penalties as provided under HIPAA or other applicable federal and state law.

For ease of reference, the term "protected information," is used to include all three types of information: Protected Health Information, Personal Information and Personally Identifiable Information. Any information that identifies or can be used to identify a JFS client receiving health care, case management, or related services is protected information.

The JFS workforce includes individuals who would be considered part of the workforce under HIPAA, such as employees, volunteers, interns and any other persons whose work performance is under the direct control of JFS, whether or not they are paid by JFS. Other terms such as "personnel" or "staff" may be used to include all of these types of workers.

Acknowledgment and Certification of Training:

I have been provided with the JFS Privacy and Security Policy and access to the Privacy and Security Plan and I have completed training on them. I acknowledge that I have read, understand, and agree to comply with all aspects of the Policy and Plan. I understand that if I fail to comply with any provision of the Policy or of the Plan, I will be subject to disciplinary action, up to and including termination of employment, or immediate dismissal if I am an unpaid member of the workforce, and any applicable civil and criminal penalties as provided by the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state law.

☐ Employee ☐ Intern ☐ Volunteer

_____
Date Completed

Staff Signature Digitally signed by Staff Signature Date: 2020.02.07 08:57:19 -08'00'

_____
Signature

_____
Print Name

Program _____

Documents Included in the Privacy and Security Plan:

The Privacy and Security Plan shall include all privacy and security policies and procedures promulgated by the agency in order to comply with HIPAA and its implementing regulations, other relevant federal and state law, and the contractual privacy and security requirements to which JFS must comply. The Plan includes, but is not limited to, the JFS Privacy and Security Policy and Procedure Manual, Computer User Agreement, and the ETOi User Security and Privacy Agreement. These documents are available on SharePoint on the Project site for "HIPAA Compliance."

No third-party rights (including but not limited to rights of clients, beneficiaries, covered dependents, or business associates) are intended to be created by the Plan. JFS reserves the right to amend or change its Plan at any time (including retroactively) without notice.

Privacy and Security Officers:

The Privacy and Security Officers for JFS are designated by the Chief Executive Officer. The Chief Operating Officer is responsible for the development and adoption of policies and procedures, including those in the Privacy and Security Plan, necessary to protect the privacy and security of Protected Information.

The Chief Operating Officer is designated as JFS' Privacy Officer. The Privacy Officer will also serve as the agency contact person for clients who have questions, concerns or complaints about the privacy of their PI, and for communicating with Business Associates on privacy and security matters. JFS contracts with Evotek, Inc. to provide a Chief Information Security Officer.

Contact information for each Officer is as follows:

Privacy Officer:
Dana Toppel, Chief Operating Officer
Address: Jewish Family Service of San Diego
8804 Balboa Avenue
San Diego, CA 92123
Phone: (858) 637- 3247
Email: danat@jfssd.org

Security Officer:
Matt Stamper, Chief Information Security Officer
Address: Evotek, Inc.
6150 Lusk Blvd., Suite B204
San Diego, CA 92121
Phone: (760) 809-2164
Email: mstamper@evotek.com