Policies and Procedures

FIS Policy and Procedure Attestation

Fabian Insurance Services and its affiliated Network Entities (individually and collectively called “FABIAN INSURANCE SERVICES” herein) abide by a system-wide Policy and Procedure. Policy and Procedure is the cornerstone of our corporate culture and a key element of our Compliance Program. The Policy and Procedure thoroughly defines behavior and work procedures expected of our employees, management, vendors, volunteers and others who interact with FABIAN INSURANCE SERVICES. The purpose of the Policy and Procedures is to reinforce FABIAN INSURANCE SERVICES’s institutional values and to serve as a guide for moral, ethical, and legal behavior. Adherence to the Policy and Procedures promotes FABIAN INSURANCE SERVICES’s reputation for integrity and honesty in the community and ensures that FABIAN INSURANCE SERVICES is compliant with applicable laws, rules, and regulations.

Attestation

- I confirm that I have received a copy of CMS distribution requirement of the Code of Conduct/Policy and Procedures in form of email or instructed to refer to Fabianinsurance.com
- I understand that it is my responsibility to read Business Code of Conduct and the Policies & Procedures, and the Compliance Program are distributed to employees within 90 days of hire, when there are updates, and annually thereafter via email or instructed to refer to Fabianinsurance.com
- I also understand that any knowledge provided to me by Fabian Insurance Services from Business Code of Conduct
- Fabian Insurance Services Code of Conduct along with the attestation, Compliance Program Policy and Procedures and can be clarified by my supervisor or Compliance Officer.
- I confirm I will carry out my day-to-day work within the spirit and letter of the Code of Conduct.
- I understand that I have a personal duty to bring all (real or suspected) violations of the Code of Conduct to the attention of my supervisor and/or Compliance Officer. Concerns may also be submitted to the Hotline. (1-863-274-5555 #4) or http://fabianinsurance.com See “For Agents” at bottom of page.
- I understand that it is against FABIAN INSURANCE SERVICES policy to be punished or retaliated against for upholding the Code of Conduct and for obeying the laws and regulations that apply to my job. Retaliation should be reported immediately.
- I agree that I have read, understand and will comply with the terms of this Code of Conduct Attestation and all applicable policies and procedures. I understand that my failure to comply with the Code of Conduct may result in disciplinary action, up to and including termination of employment or student status, or loss of FABIAN INSURANCE SERVICES privileges or contractual or affiliation rights.

Name: _____

Email address: _____

Affiliation: ☐ Employee ☐ Temporary Employee ☐ Contractor ☐ Student ☐ Volunteer ☐ Vendor

Other (specify): _____

Signature: _____ Date: _____

Initial: _____

Policies and Procedures

Table of Contents:

Opening Statement

At Fabian Insurance Services, we are committed to maintaining the highest standards of compliance, professionalism, and ethical conduct in all aspects of our operations. This living Policy and Procedures Document serves as a comprehensive guide to ensure that our practices align with all applicable federal and state laws, regulations, and industry guidelines governing health insurance products.

We recognize the dynamic nature of the health insurance landscape and the importance of adapting to legislative and regulatory changes to better serve our clients. To uphold this commitment, the Executive Board will convene quarterly meetings to review, discuss, and update this document as necessary. These scheduled meetings will ensure that our policies and procedures remain current, compliant, and reflective of best practices.

Our dedication to compliance and ethical service is integral to our mission of providing high-quality insurance solutions while fostering trust and accountability with our clients, partners, and regulators. The policies and procedures outlined herein are designed to guide our employees and affiliates in delivering consistent and compliant services.

Quarterly Executive Board Meeting Schedule:

Q1: First Week of January
Q2: First Week of April
Q3: First Week of July
Q4: First Week of October

All updates and revisions to this document resulting from these meetings will be communicated promptly to ensure continued alignment with governing laws and principles.

Fabian Insurance Services is dedicated to excellence and compliance, and this document reflects our ongoing efforts to uphold these values in every aspect of our operations.

Initial: _____

Section 1

HIPAA Privacy Rule Compliance

Policy Title: Handling Member Requests for Protected Health Information (PHI)

Purpose

To provide a clear process for delegate/vendor employees to handle member requests related to Protected Health Information (PHI), ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other applicable privacy regulations.

Scope

This policy applies to all delegate/vendor employees who handle PHI on behalf of Fabian Insurance Services. It covers requests from members to view the Notice of Privacy Practices (NPP), inspect or obtain a copy of their PHI, amend their PHI, restrict the use or disclosure of PHI, and authorize disclosures of PHI outside of Treatment, Payment, and Health Care Operations (TPO).

Policy and Procedure

Requests to View Notice of Privacy Practices (NPP)

Policy: Members have the right to request and view a copy of Fabian Insurance Services' NPP at any time.

Procedure: Delegate/vendor employees must provide a copy of the NPP to the member upon request, either electronically or in paper form.

If the request is made in person, provide a printed copy of the NPP.

If the request is made via phone or email, direct the member to the online NPP available on the company's website or send an electronic copy.

Document the request and the provision of the NPP in the member's record.

Requests to Inspect and Obtain a Copy of PHI

Policy: Members have the right to inspect and obtain a copy of their PHI contained in designated record sets, subject to certain limitations.

Procedure: Verify the identity of the member before providing access to the PHI.

Forward the request to the Privacy Officer or designated team for processing.

Respond to the member's request within 30 days of receiving it. An additional 30-day extension may be applied, if necessary, with written notice to the member(s).

If the request is approved, provide the PHI in the format requested (e.g., electronic or paper). If the requested format is not available, provide the information in an alternative format agreed upon by the member.

If the request is denied (e.g., if the PHI contains information that may endanger another person), provide a written denial explaining the reason and the member's right to appeal.

Requests to Amend PHI

Policy: Members have the right to request an amendment to their PHI if they believe it is inaccurate or incomplete.

Procedure: Verify the identity of the member requesting the amendment.

Forward the request to the Privacy Officer or designated team for review.

Respond to the request within 60 days. If an extension is required, provide a written explanation to the member(s) and extend the response time by no more than 30 days.

If the amendment is accepted, update the PHI accordingly and inform the member(s) of the changes.

Initial: _____

If the request is denied, provide a written explanation to the member, including the reason for the denial and information on how to file a disagreement statement.

Requests to Restrict Usage and Disclosures of PHI

Policy: Members have the right to request restrictions on the use or disclosure of their PHI for treatment, payment, or healthcare operations (TPO).

Procedure

Verify the identity of the member before processing the restriction request.

Forward the request to the Privacy Officer or designated team for evaluation.

Evaluate the feasibility of the requested restriction. Fabian Insurance Services is not required to agree to the requested restrictions but must consider each request.

If the restriction is agreed upon, document the restriction and ensure that it is communicated to relevant departments and Business Associates.

If the request is denied, inform the member in writing, including the reasons for the denial.

Authorizations for Disclosures Outside of TPO

Policy: Members have the right to authorize or deny disclosures of their PHI outside of TPO activities, such as disclosures for marketing purposes or to third parties not involved in their care.

Procedure

Verify the identity of the member before processing an authorization request.

Provide the member with an authorization form that specifies the information to be disclosed, the purpose of the disclosure, and the entities to whom the information will be disclosed.

Ensure that the authorization form is signed and dated by the member.

Maintain a copy of the signed authorization form in the member's record.

Disclose the PHI as authorized by the member, only for the purposes and to the entities specified.

Inform the members that they have the right to revoke the authorization in writing at any time, except to the extent that the action has already been taken based on the original authorization.

Documentation and Record-Keeping

All member requests and the actions taken in response to those requests must be documented and maintained for a minimum of six years, in compliance with HIPAA record-keeping requirements.

Records of member requests must include the request date, the nature of the request, and a summary of the response provided.

Training

All delegate/vendor employees who handle PHI must receive training on this policy and related procedures during onboarding and annually thereafter. Self-study training is provided during onboarding and annually by accessing https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

Employees are responsible for understanding and complying with this policy to ensure the protection of members' privacy rights.

Employees are responsible for reviewing cybersecurity section of the Privacy and Security Guide and using the Security Risk Assessment Tool provided by HealthIT.gov to secure personal devices used in the field. Guidance is available by contacting complianceofficer@fabianinsurance.com

Violations

Any violations of this policy may result in disciplinary action, up to and including termination of the vendor agreement.

Contact Information

For questions or more information regarding this policy, contact the Privacy Officer at:

Initial: _____

Privacy Officers, Luis Hernandez and/or Jeannie Pond
Fabian Insurance Services
863-274-5555
complianceofficer@fabianinsurance.com

Policy Fabian Insurance Services and its business associates may not use or disclose PHI potentially related to reproductive health care without obtaining a valid attestation from the person requesting the use or disclosure. Each request for use or disclosure requires a separate, newly signed attestation.

Components of a Valid Attestation

Procedure A valid attestation must include the following components:

Description of the Information Requested

A specific description of the PHI requested, including either:

The name of any individual whose PHI is sought, or A description of the class of individuals whose PHI is sought (e.g., patients receiving reproductive health services).

Identification of the Recipient of the Information:

The name or specific identification of the person or class of persons to whom Fabian Insurance Services is to make the requested use or disclosure.

Prohibited Purpose Statement:

A clear statement that the use or disclosure of the PHI is not for a purpose prohibited under 45 CFR 164.502(a)(5)(iii). This ensures that the request is not for purposes such as discriminatory activities or other illegal uses.

Statement of Legal Penalties:

A statement indicating that a person may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if they knowingly and in violation of HIPAA obtain individually identifiable health information relating to an individual or disclose such information to another person.

Signature and Date: The signature of the person requesting the PHI, which may be an electronic signature.

The date of the signature

If the attestation is signed by a representative of the person requesting the information, a description of the representative's authority to act on behalf of the requesting individual must be included.

Attestation Review and Approval Process

Procedure

Verification of Attestation

Upon receipt of a request for use or disclosure of PHI related to reproductive health care, the Privacy Officer or designated team member must review the attestation for completeness and validity.

Confirm that the attestation contains all required elements and is written in plain language to ensure it can be understood by all parties involved.

Approval or Denial of Request:

If the attestation is valid and complete, the Privacy Officer may approve the request and proceed with the use or disclosure of the PHI.

If the attestation is incomplete or does not meet the requirements, the request must be denied, and the requester must be informed in writing of the deficiencies.

Documentation of the request and attestation review process must be retained for a minimum of six years.

Documenting the Disclosure:

If the request is approved, document the disclosure, including the date, the specific PHI disclosed, the identity of the recipient, and a copy of the attestation.

Ensure that the PHI is disclosed only to the individual or entity specified in the attestation.

Training and Awareness

Policy: All employees, delegates, and business associates involved in the handling of PHI must

Initial: _____

receive training on this policy and procedure during onboarding and annually thereafter.

Procedure:

The training must include:

The importance of obtaining a valid attestation before using or disclosing PHI related to reproductive health care.

How to review an attestation for completeness.

The potential penalties for unauthorized disclosure of PHI under HIPAA.

The Privacy Officer is responsible for ensuring that training materials are updated to reflect any changes in regulations or company policies.

5. Violations and Enforcement

Policy: Any failure to comply with this policy may result in disciplinary action, up to and including termination of employment or the vendor agreement, as well as potential civil and criminal penalties under HIPAA.

Procedure:

Report any suspected or confirmed violations of this policy immediately to the Privacy Officer.

The Privacy Officer will investigate the incident and take appropriate corrective actions, including re-training, policy updates, or disciplinary measures as necessary.

For questions or more information regarding this policy, contact the Privacy Officer at:
Privacy Officers, Luis Hernandez and/or Jeannie Pond
Fabian Insurance Services
863-274-5555
complianceofficer@fabianinsurance.com

Initial: _____

Section 2

HIPAA Security Rule Compliance

Purpose:

Ensures the confidentiality, integrity, and availability of ePHI by establishing security standards.

Scope

Applies to all information systems that create, receive, maintain, or transmit ePHI.

Procedures

Fabian Insurance Services Administers the Following Safeguards:

Perform and document a regular Security Risk Assessment (SRA) to identify and mitigate vulnerabilities.

Development of a security management process that includes risk analysis, risk management, and sanction policies for violations.

Implements a workforce security policy to ensure that access to ePHI is restricted to authorized users only.

Established security incident procedures for responding to and documenting breaches and security events.

Assigned a HIPAA Security Officer responsible for overseeing security measures and ensuring compliance.

Control access to physical locations where ePHI is stored, such as server rooms or file storage areas.

Implemented policies for the secure disposal of hardware, electronic media, and paper records containing PHI.

Maintain a facility access control plan, including monitoring access to workstations and other equipment that handle ePHI.

Use encryption technologies to protect ePHI at rest and during transmission (e.g., Secure Socket Layer (SSL) encryption for web access).

Implement access controls such as unique user IDs, strong passwords, and automatic logoff for systems containing ePHI.

Use audit controls to track and record access to ePHI and regularly review logs for suspicious activity.

Use secure communication channels, such as encrypted email or secure file transfer protocols, for transmitting ePHI.

Administrative Safeguards for PHI

Policy: All delegate/vendor employees must apply administrative safeguards to ensure the secure handling of PHI throughout its lifecycle.

Procedure:

Access Control: Only authorized personnel shall have access to PHI. Access should be granted based on the minimum necessary principle, limiting access to those who need the information for job-related duties.

Training: All delegate/vendor employees who handle PHI must receive HIPAA training upon hire and annually thereafter. Training should include the proper handling and disposal of PHI.

Incident Reporting: Any suspected or confirmed breach of PHI must be reported immediately to Fabian Insurance Services' Privacy Officer for investigation and appropriate action.

Technical Safeguards for PHI

Policy: Delegate/vendor employees must implement technical safeguards to ensure the security of electronic PHI (ePHI).

Procedure: Encryption: All electronic communications containing PHI must be encrypted using industry-standard encryption methods.

Secure Storage: ePHI must be stored on secure, access-controlled systems with up-to-date antivirus software and firewalls.

Data Transmission: When transmitting ePHI, use secure communication methods such as secure email or encrypted file transfer protocols (FTP).

Initial: _____

Physical Safeguards for PHI

Policy: Delegate/vendor employees must apply physical safeguards to protect paper-based and electronic PHI from unauthorized access, use, or disclosure.

Procedure:

Secure Storage: Paper records containing PHI must be stored in locked cabinets or rooms when not in use. Access should be limited to authorized personnel only.

Workstation Security: Workstations used to access ePHI must be secured when unattended, with screen-lock functionality enabled after a period of inactivity.

Disposal of PHI: Physical records containing PHI must be disposed of using secure methods such as shredding, burning, pulping, or pulverizing. Electronic records must be securely deleted from storage devices in a manner that prevents recovery.

Policy: PHI must be disposed of in a manner that prevents unauthorized access and ensures that the information cannot be reconstructed.

Procedure:

Shredding: Paper documents containing PHI must be shredded using a cross-cut shredder.

Burning, Pulping, or Pulverizing: If shredding is not feasible, documents may be burned, pulped, or pulverized to ensure that they cannot be reconstructed.

Electronic Disposal: ePHI must be permanently deleted using secure data-wiping software or by physically destroying the storage media (e.g., hard drives).

Third-Party Disposal: If using a third-party vendor for disposal, ensure that the vendor is contractually obligated to follow secure disposal procedures and that a Business Associate Agreement (BAA) is in place.

Handling Returned (Undeliverable) Mail, Notices, and Communications Containing PHI

Policy: Returned or undeliverable mail, notices, and other communications containing PHI must be handled and disposed of securely to prevent unauthorized access.

Procedure:

Secure Handling of Returned Mail:

Upon receipt of undeliverable or returned mail containing PHI, delegate/vendor employees must log the receipt of the returned communication and immediately notify the Privacy Officer.

Store the returned mail in a secure, locked location while awaiting further instructions from the Privacy Officer.

Verification and Correction of Address:

Attempt to verify the accuracy of the member's address using available records and correct the address if possible.

If the address cannot be verified or corrected, do not re-send the PHI until further direction is received from the Privacy Officer.

Disposition of Returned Mail:

If the returned mail cannot be delivered after verification attempts, dispose of the mail containing PHI using a secure disposal method, such as shredding.

Document the disposal of the returned mail, including the date, method of disposal, and the individual responsible for the disposal.

Maintain a record of the returned mail and the disposal documentation for a minimum of six years in compliance with HIPAA requirements.

Documentation and Record-Keeping

All disposal activities, including the disposal of PHI and handling of returned mail, must be documented and retained for a minimum of six years.

Initial: _____

Records should include the date of disposal, the method used, and the names of the personnel involved.

Training

All delegate/vendor employees handling PHI must receive training on this policy and procedure during onboarding and annually thereafter.
https://www.cms.gov/marketplace/technical-assistance-resources/assister-programs/best-practices-for-handling-pii-fast-facts.pdf

Training should cover proper handling, disposal of PHI, and the process for handling returned mail and other communications.
https://www.cms.gov/marketplace/technical-assistance-resources/assister-programs/best-practices-for-handling-pii-fast-facts.pdf

Violations

Any violations of this policy may result in disciplinary action, up to and including termination of the vendor agreement.

Report any suspected violations to the Privacy Officer immediately.

Contact Information

For questions or more information regarding this policy, contact the Privacy Officer at:

For questions or more information regarding this policy, contact the Privacy Officer at:

Privacy Officers, Luis Hernandez and/or Jeannie Pond
Fabian Insurance Services
863-274-5555
complianceofficer@fabianinsurance.com

Initial: _____

Section 3

Fraud, Waste, & Abuse Policies & Training Documents

Policy

Fabian Insurance Services follows the Centers for Medicare & Medicaid Services (CMS) mandates that require health insurance agencies establish a comprehensive Fraud, Waste, and Abuse (FWA) policy and procedure to ensure the integrity of the ACA, Medicare and Medicaid programs. The following detailed description outlines the essential components of an FWA policy, including prevention, detection, reporting, and training procedures.

Procedure

It is every Associate's responsibility to prevent, detect, and correct fraud, waste, and abuse and report instances of noncompliance to the organization's compliance officer, State Medicaid Agency, CMS, CMS' designee and /or law enforcement.

The organization's compliance officer is responsible for all aspects of the organization's compliance program.

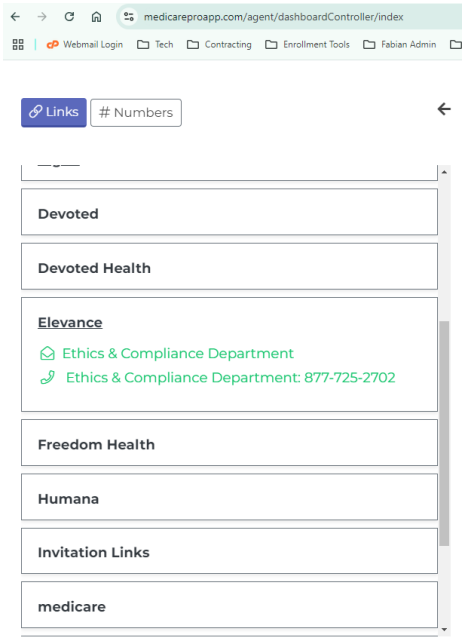
The compliance officer is the organization's link to important compliance information and education. All employees are encouraged to seek guidance concerning any obligations and report any instances of noncompliance.

The following reporting mechanism are available 24/7 to employees (full-time/part-time, temporary employees, interns, volunteers, consultants), Board members, and Downstream Entities (subcontractors/subdelegates) And are ready for intake, assessment, research, tracking, and reporting issues of non-compliance or FWA. All employees (full-time/part-time, temporary employees, interns, volunteers, consultants), Board members, and Downstream Entities (subcontractors/subdelegates) who may report suspected or actual non-compliance or FWA may do so without fear of retaliation from Fabian Insurance Services.

The organization provides multiple resources for assistance and reporting. Reporting may be conducted anonymously, 24/7:

- https://fabianinsurance.com/learning-management/ - See
- Florida State Attorney General: 1-866-966-7226
- Agency for Health Care Administration
- Medicaid Program Integrity: 1-888-419-3456
- Department of Financial Services
- Division of insurance Fraud: 1-800-378-0445
- Department of Health & Human Services
- Office of Inspector General: 1-800-447-8477

Compliance Reporting numbers and emails for all Carriers are available 24/7 located in the MedicarePro CRM Carrier Directory. See example below



Once a violation report is received by the Compliance Officer, Fabian Insurance Services Executive Board Members will conduct a confidential, objective and thorough investigation that includes:

- Collecting evidence such as emails, paperwork, receipts, or computer data.
- Conduct Interviews if necessary
- Documentation and reporting of findings

Initial: _____

- Escalation to appropriate Carrier and/or Authority including but not limited to:
    - Florida State Attorney General, Agency for Health Care Administration, Medicaid Program Integrity, Department of Financial Services, Division of insurance Fraud, Department of Health & Human Services, Office of Inspector General
    - Elevance Health, Aetna, Cigna, United Healthcare, Devoted, Humana, Molina, Freedom, Optimum, Wellcare, Florida Blue, Oscar, Ambetter,AvMed, CareSource
- Fabian Insurance Services will continue to coordinate and assist investigative authorities when required until a resolution is reached.

FWA Training and Education

Training Requirements:

All Agents contracted with Fabian Insurance Services are required to annually recertify with AHIP that includes FWA training modules. Training can be acquired at https://www.ahipmedicaretraining.com/page/login

Documentation:

All agents contracted with Fabian Insurance Services are required to email AHIP Certificates to ComplianceOfficer@FabianInsurance.com for audit purposes.

Initial: _____

Section 4 - Cultural Competency Policies and Training Method

Purpose: To promote understanding and respect for cultural diversity.

Scope: Applies to all staff interactions with clients, and colleagues.

Policy: Fabian Insurance Services supports a culture of diversity and inclusion. We treat everyone with respect. Discrimination or harassment of any kind based on race, color, national origin, religion, sex, gender identity, age, sexual orientation, disability, marital status, genetic information, military or veteran status, or any other characteristic protected by law will not be tolerated. We do not tolerate conduct that is disrespectful, hostile, intimidating, or harassing.

Procedures:

- Annual training on cultural awareness and communication skills.
- Tailoring services to meet the cultural and linguistic needs of clients.
- Evaluation of effectiveness of training.

Initial: _____

Section 5

Non-Discrimination

Policy Statement:
Fabian Insurance Services is committed to providing an environment where all individuals are treated with respect and dignity. We believe in fostering a culture of inclusivity, equity, and fairness. Discrimination or harassment of any kind based on race, color, national origin, religion, sex, gender identity, age, sexual orientation, disability, marital status, genetic information, military or veteran status, or any other characteristic protected by law will not be tolerated.

Purpose:
The purpose of this policy is to ensure that all employees, clients, vendors, and business partners are aware of our commitment to maintaining a discrimination-free workplace. It sets out the principles and guidelines to prevent discrimination and provides procedures for addressing and resolving concerns or complaints of discrimination.

Scope:
This policy applies to all aspects of employment and business operations, including but not limited to recruitment, hiring, training, promotion, compensation, benefits, terminations, and interactions with clients and partners. It applies to all employees, contractors, vendors, and agents of Fabian Insurance Services, as well as to our interactions with clients and third parties.

Prohibited Conduct

Discrimination: Fabian Insurance Services prohibits discrimination in any form against any employee, client, or business partner based on race, color, national origin, religion, sex, gender identity, age, sexual orientation, disability, marital status, genetic information, military or veteran status, or any other characteristic protected by applicable federal, state, or local laws.

Harassment:
Harassment is a form of discrimination that includes unwelcome verbal, written, or physical conduct that demeans or shows hostility toward an individual based on protected characteristics. This includes, but is not limited to, offensive jokes, slurs, epithets, name-calling, physical assaults, threats, intimidation, ridicule, insults, and offensive objects or pictures.

Retaliation:
Fabian Insurance Services strictly prohibits retaliation against individuals who report discrimination or harassment, participate in an investigation of such reports, or oppose discriminatory practices. Retaliation includes any adverse action that might dissuade a reasonable person from making or supporting a complaint.

Delegate/Vendor, will not differentiate, or discriminate against any Member as a result of his/her enrollment in a Health Benefit Plan

Delegate/Vendor, as well as its agents and employees, shall not, in accordance with the Affordable Care Act Section 1557 (42 U.S.C. § 18116), cause an individual to be excluded on the grounds prohibited under Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d et seq.), Title IX of the Education Amendments of 1972 (20 U.S.C. § 1681 et seq.), the Age Discrimination Act of 1975 (42 U.S.C. § 6101 et seq.), or Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. § 794), or subject to any other applicable State and Federal laws, from participation in, be denied the benefits of, or be subjected to discrimination under, any health program or activity offered through the Exchange. (Applicable only to Commercial Exchange line of business)

Responsibilities

Fabian Insurance Services is committed to creating a diverse and inclusive workplace that upholds the principles of equality and respect for all individuals. In alignment with our core values and mission, we affirm our commitment to comply with all applicable federal, state, and local laws regarding equal employment opportunity and non-discrimination. These laws include, but are not limited to:

- Title VI of the Civil Rights Act of 1964: Prohibiting discrimination on the basis of

Initial: _____

race, color, or national origin in any program or activity receiving federal financial assistance.

- Equal Employment Opportunity Act (Executive Orders 11246 and 11375): Ensuring that all employees and applicants for employment have the right to be free from discrimination based on race, color, religion, sex, national origin, disability, and veteran status.
- Americans with Disabilities Act of 1990 (Public Law 101-336): Prohibiting discrimination against individuals with disabilities and requiring reasonable accommodations in the workplace.
- Age Discrimination Act of 1975 (45 CFR part 91): Prohibiting discrimination based on age in programs or activities receiving federal assistance.

Delegate/Vendor, as well as its agents and employees, shall comply with the provisions of the Fair Employment and Housing Act (Government Code, Section 12900, et seq.) and the applicable regulations promulgated thereunder (2 CCR 7285.0, et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code, Section 12990, set forth in CCR Chapter 5 of Division 4 of Title 2, including, 2, CCR Section 8103, et seq., are incorporated into this Agreement by reference and made a part hereof as if set forth in full.

Delegate/Vendor, shall give written notice of its obligations under this clause to labor organizations with which it has a collective bargaining or other agreement.

Policy Guidelines:

Non-Discrimination: We prohibit discrimination, harassment, or retaliation against any employee, applicant, or participant based on the categories outlined above. This policy applies to all employment practices, including hiring, training, promotion, compensation, benefits, and termination.

Equal Opportunity: We provide equal employment opportunities to all qualified individuals. We strive to attract, hire, retain, and promote individuals without regard to race, color, religion, sex, national origin, disability, age, or any other characteristic protected by law.

Reasonable Accommodations: Fabian Insurance Services will provide reasonable accommodation to qualified individuals with disabilities, unless such accommodation imposes an undue hardship on the organization.

Training and Awareness: The organization will conduct regular training programs to ensure all employees are aware of their rights and responsibilities under these laws, as well as the procedures for reporting and addressing any violations.

Reporting Violations: Employees are encouraged to report any incidences of discrimination, harassment, or retaliation to: ComplianceOfficer@FabianInsurance.com. All reports will be handled promptly and with confidentiality to the extent possible.

Commitment to Continuous Improvement: We are committed to reviewing and improving our policies and practices to promote diversity, equity, and inclusion within our workforce.

Subcontracts (Title 42 CFR 438.3(k)):

All subcontracts must meet the provisions of Title 42 CFR 438.3(k). This includes ensuring that subcontractors adhere to the same performance standards and regulations applicable to our organization.

Contracts must specify the obligations and responsibilities of the subcontractor, including adherence to applicable laws and regulations.

Record Keeping Requirements (Title 42 CFR 438.3(u) and Title 42 CFR 422.504(d)):

All records related to contracts, including CA PMG contract documents and Business Associate Agreements (BAA), must be maintained in compliance with Title 42 CFR 438.3(u) and Title 42 CFR 422.504(d).

Records must be accurate, complete, and readily accessible for review and audit purposes.

Initial: _____

Specific retention periods for records must align with federal regulations as well as additional state-specific requirements.

State-Specific Requirements:

Compliance with individual state requirements is mandatory. Each state may have its own citations and stipulations regarding subcontracting and record-keeping. Staff must verify these requirements through the respective state's official website.

Delegate Contract Review:

Prior to finalizing any delegate contracts, a thorough review must be conducted to ensure alignment with record retention requirements. Delegates must comply with all applicable record-keeping obligations outlined in their contracts.

Responsibilities:

Compliance Officer: Ensure all contracts meet regulatory requirements and maintain up-to-date records of state citations.

Agency Managers: Monitor downline compliance with record-keeping protocols and perform necessary reviews of delegation contracts.

Staff: Adhere to policies and procedures regarding subcontracting and record maintenance

Review and Enforcement: This policy will be reviewed annually to ensure ongoing compliance with federal and state regulations. Non-compliance may result in corrective action as outlined in the organization's disciplinary procedures.

Reporting and Complaint Procedure

Filing a Complaint:

Employees who believe they have experienced or witnessed discrimination, or harassment should promptly report the incident to their immediate supervisor, Human Resources, or the designated Compliance Officer. Clients and vendors may report concerns to their primary point of contact at Fabian Insurance Services or directly to the Compliance Officer.

Reports can be made verbally or in writing. Written complaints should include the date, time, location, nature of the incident, and names of any individuals involved or witnesses.

Confidentiality:

Fabian Insurance Services will make every effort to maintain the confidentiality of individuals involved in a discrimination or harassment complaint. Information will be shared only as necessary to conduct a fair and thorough investigation.

Investigation Process:

Upon receiving a complaint, the Compliance Officer or HR representative will conduct a thorough and impartial investigation, which may include interviews with the complainant, the accused, and any witnesses.

The investigation will be completed promptly, and both the complainant and the accused will be informed of the outcome.

Resolution and Corrective Action:

If a violation of this policy is found, appropriate corrective action will be taken, which may include disciplinary action, up to and including termination of employment or contract. The specific action will depend on the severity of the conduct and the surrounding circumstances.

Fabian Insurance Services is committed to taking steps to prevent further occurrences of discrimination or harassment.

Training and Awareness

Employee Training:

All employees are required to attend regular training sessions on non-discrimination, cultural competency, and harassment prevention.

Training will cover applicable federal, state, and local laws, the importance of diversity and inclusion, and

Initial: _____

the procedures for reporting and addressing complaints.

Client and Vendor Communication:

Clients and vendors will be informed of our commitment to non-discrimination and the procedures they can follow if they believe they have experienced or witnessed discrimination or harassment by representatives of Fabian Insurance Services.

Monitoring and Policy Review

Continuous Monitoring:

Fabian Insurance Services will regularly review its practices and procedures to ensure that they are following this policy and relevant laws.

Regular surveys may be conducted to gather feedback from employees regarding the work environment and any potential areas for improvement.

Policy Review:

This policy will be reviewed annually or as needed to ensure it remains effective and up to date with current laws and best practices.

Employees will be notified of any changes to this policy and will receive updated training as necessary.

Non-Compliance and Disciplinary Action

Disciplinary Actions for Violations:

Any employee found to have engaged in conduct in violation of this policy will be subject to disciplinary action, up to and including termination.

Managers and supervisors who fail to act upon reports of discrimination or harassment may also be subject to disciplinary action.

Reporting to External Agencies:

If an individual believes that their complaint has not been handled appropriately by Fabian Insurance Services, they have the right to file a complaint with external agencies such as the Equal Employment Opportunity Commission (EEOC) or other applicable state and federal agencies.

Conclusion

Fabian Insurance Services is dedicated to maintaining a respectful, inclusive, and non-discriminatory environment for all employees, clients, and partners. This policy reinforces our commitment to equality and fairness, ensuring that everyone has the opportunity to work and interact in a safe and welcoming environment. We encourage open communication and will continue to foster a culture where diversity is celebrated, and every individual is valued.

For questions or additional information about this policy, please contact the Human Resources department or the Compliance Officer.

Jeannie Pond –
ComplianceOfficer@fabianinsurance.com.

Initial: _____

Section 6

Employee/Personnel Vaccination Policy

Policy Statement:
Fabian Insurance Services is committed to maintaining a safe and healthy work environment for all employees, clients, and visitors. As part of our commitment to public health and safety, this policy outlines the expectations and procedures regarding vaccinations for employees. Our goal is to protect the health and well-being of our workforce while ensuring compliance with applicable federal, state, and local regulations.

Purpose:
The purpose of this policy is to ensure that all employees are aware of the vaccination requirements, guidelines, and procedures that are in place to minimize the spread of vaccine-preventable diseases within our workplace. This policy aims to protect employees, clients, and the broader community by promoting vaccination as a key strategy in maintaining a healthy work environment.

Scope:
This policy applies to all full-time, part-time, temporary, and contract employees of Fabian Insurance Services, regardless of their role or location. It also applies to employees who may work remotely but have occasional in-person interactions with colleagues or clients.

Vaccination Requirements

Recommended Vaccinations: Fabian Insurance Services encourages all employees to stay up to date with the following vaccinations as recommended by the Centers for Disease Control and Prevention (CDC):

- Influenza (Flu)
- COVID-19
- Measles, Mumps, and Rubella (MMR)
- Tetanus, Diphtheria, and Pertussis (Tdap)
- Hepatitis B (for employees with potential exposure to blood or bodily fluids)
- Varicella (Chickenpox) if not immune

Any other vaccines as advised by the CDC or local health departments during outbreaks or public health emergencies.

Seasonal Vaccinations:

Employees are strongly encouraged to receive the annual influenza vaccine, particularly during the flu season (October through March).

Employees are also encouraged to stay updated with any new COVID-19 boosters as recommended by the CDC.

Job-Specific Vaccination Requirements:

Certain roles or positions that involve interaction with clients in healthcare settings, frequent travel, or other high-risk environments may require specific vaccinations. These requirements will be outlined in job descriptions and discussed during onboarding.

Vaccination Documentation

Proof of Vaccination:

Employees who receive vaccinations relevant to this policy are encouraged to provide documentation of vaccination to the Administrative Office for record-keeping purposes.

Documentation may include a vaccination card, immunization record, or a written statement from a healthcare provider.

Proof of vaccination will be maintained confidentially in the employee's health record and will not be disclosed except as required by law or for safety purposes.

Non-Disclosure Option:

If an employee chooses not to disclose their vaccination status, they must follow alternative safety measures as outlined in the Confidentiality and Privacy Section, such as masking or maintaining physical distance during in-person interactions.

Accommodation and Exemption Requests

Initial: _____

Medical Exemptions:

Employees with medical conditions that prevent them from receiving a recommended vaccine may request a medical exemption. This request must be supported by a written statement from a licensed healthcare provider indicating the medical reason for the exemption.

The request will be reviewed by the HR department, and accommodation will be considered on a case-by-case basis.

Religious Exemptions:

Employees may request an exemption from vaccination based on sincerely held religious beliefs. The request should be submitted in writing to the HR department and will be reviewed individually.

The company will work to provide reasonable accommodation unless doing so would result in undue hardship or pose a direct threat to the health and safety of others.

Alternative Measures:

Employees who are exempt from vaccinations or choose not to disclose their vaccination status may be required to follow additional safety measures, such as wearing masks, maintaining social distance, and participating in regular COVID-19 testing as required by local regulations or company policy.

Compliance and Monitoring

Policy Compliance:

All employees are expected to comply with this policy and any related safety protocols. Non-compliance may result in disciplinary action, including warnings or, in severe cases, suspension or termination.

Regular Review:
Fabian Insurance Services will regularly review this policy to ensure it is in line with current public health guidelines and legal requirements. Updates will be communicated to all employees.

Changes to Local and Federal Requirements:

Should federal, state, or local laws require specific vaccinations for certain employees or during health emergencies, Fabian Insurance Services will adjust this policy accordingly and notify employees of any changes or new requirements.

Confidentiality and Privacy

Confidential Handling of Medical Information:

Information regarding an employee's vaccination status and exemption requests will be treated as confidential medical information. Records will be maintained securely by the HR department and accessed only by authorized personnel.

Fabian Insurance Services will comply with all relevant privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), to protect employees' health information.

Initial: _____

Section 7

Record Retention and Access

Policy: Compliance with Federal and State Record Keeping Requirements for Delegate/Vendor Records Access

Purpose

To establish standards that ensure delegates/vendors provide records access in compliance with federal, state, and health plan policies for record retention and audit access, including federal requirements under Title 42 CFR 438.3(k) and (u) for Medicaid and Title 42 CFR 422.504(d) for Medicare Advantage plans.

Scope

This policy applies to all delegates, vendors, and designees who manage or store records associated with member medical and billing information on behalf of the health plan. It ensures compliance with requirements set forth by federal law, state-specific mandates, and individual contract terms with the health plan.

Policy Statement

Delegates and vendors must comply with all applicable federal and state record-keeping and retention laws, including Title 42 CFR 438.3(k) (regarding subcontract requirements) and 438.3(u) (for Medicaid managed care record-keeping requirements), as well as Title 42 CFR 422.504(d) for Medicare Advantage programs. Delegates/vendors shall provide the health plan or its designees with on-site access, upon request, for the purpose of audit and review. This policy also includes compliance with California's requirements for Provider Medical Group (PMG) agreements, business associate agreements (BAAs), and record retention specifications.

Record Access and Audit Rights

On-Site Access: In accordance with federal law and individual contract provisions, delegates/vendors must permit on-site access for the health plan or its designees to all records pertinent to member medical and billing information, without charge.

Audit Rights: The health plan or its designees retain the right to audit, examine, copy, and transcribe relevant books, documents, and records related to the provision of member services. Compliance with 42 CFR 438.3(u) and 422.504(d) means that these rights are available at any time deemed necessary to ensure quality care, adherence to standards, and regulatory compliance.

Appropriate Working Space: The delegate/vendor shall provide adequate working space to health plan personnel or designees for audit activities, which should occur during regular business hours.

Record Retention Compliance

Retention Period: All records must be maintained for the period specified by federal regulations (e.g., Medicare Advantage retention under 42 CFR 422.504(d)), applicable state laws, and any terms detailed in the delegate/vendor's contract with the health plan. Documentation to support employee screenings against the OIG listing and GSA listing prior to hire (contracting) and monthly thereafter will be maintained for a minimum of 10 years.

State-Specific Requirements: Each state may have its own unique retention requirements that must be observed. The health plan will review individual state requirements through official state websites, and delegates/vendors are expected to comply with any additional retention policies required by state law.

Destruction of Records: Records may only be destroyed in line with federal, state, and contractual guidelines once the required retention period has lapsed.

Compliance with HIPAA and State Privacy Laws

HIPAA Compliance: All records containing member medical information must be maintained in accordance with HIPAA requirements, protecting the confidentiality, integrity, and availability of Protected Health Information (PHI).

State Privacy Laws: Delegates/vendors must also comply with any state-specific privacy regulations and policies that pertain to member data during audits. This includes protecting PHI throughout the audit

Initial: _____

process and ensuring access is limited to authorized personnel.

Procedure for Record Requests

Request Submission: The health plan or its designees will submit a formal written request for access, specifying the scope of the audit and the specific records required.

Response to Request: Delegates/vendors must acknowledge receipt of the request within five business days and coordinate an access date within 15 business days or as agreed upon with the health plan.

Record Preparation: Delegates/vendors are responsible for ensuring that all requested documents are available and properly organized. If any records are unavailable, they must provide a written explanation and estimated timeline for availability.

Documentation and Follow-Up: All findings will be documented, and any deficiencies identified during the audit will require the delegate/vendor to implement corrective actions within the specified time frame.

Enforcement and Non-Compliance

Contractual and Regulatory Enforcement: Non-compliance with these requirements may result in penalties, including termination of the vendor contract and potential reporting to federal or state regulatory authorities if deemed necessary by the health plan.

Review and Update of Policy

Annual Review: This policy shall be reviewed annually or upon any changes in federal or state regulations, such as those under 42 CFR 438.3 and 42 CFR 422.504, to ensure ongoing compliance. Any updates will be communicated to all delegates/vendors promptly.

Training Requirements

Education on Compliance: All delegates/vendors are required to ensure their personnel are trained on record-keeping, HIPAA compliance, and audit requirements to adhere to these federal and health plan guidelines.

Citations:

Title 42 CFR 438.3(k) & (u) – Outlines requirements for Medicaid managed care subcontractor agreements and the record-keeping responsibilities of Medicaid managed care organizations.

Title 42 CFR 422.504(d) – Specifies the record retention requirements for Medicare Advantage plans, mandating the maintenance of records for a minimum of ten years, or as required by law.

Initial: _____

Section 8

Background Check and Exclusion Screening and Downstream Entity Oversite

Policy Statement

Fabian Insurance Services is committed to ensuring compliance with all federal and state regulations regarding background checks, abuse prevention, and notifications to the OIG. All personnel will be screened and monitored according to these regulations to prevent abuse, neglect, and exploitation.

Procedures

Criminal Background Checks (42 CFR § 455.434)

Pre-employment Screening:

All prospective employees, contractors, and agents must undergo a criminal background check before hiring.

Background checks will include fingerprinting and verification against national databases, including the FBI criminal database.

Annual Re-screening:

Current employees will undergo annual re-screening to ensure ongoing compliance.

Employees with new criminal charges must report them within 24 hours.

Freedom from Abuse, Neglect, and Exploitation (42 CFR § 483.12)

Zero Tolerance Policy:

FIS strictly prohibits abuse, neglect, exploitation, or mistreatment of any individual.

All employees are required to report any suspected incidents immediately to the Compliance Officer.

Training:

Mandatory annual training on identifying, reporting, and preventing abuse is required for all employees.

Training records will be maintained for inspection by regulatory authorities.

Investigation of Allegations:

The Compliance Department will investigate all reports of abuse or neglect within 24 hours.

If allegations are substantiated, disciplinary action, up to and including termination, will be taken.

Notification to the Inspector General (42 CFR § 455.106(b))

OIG Reporting:

FIS will notify the OIG if any individual or entity affiliated with the organization is found on the OIG's List of Excluded Individuals/Entities.

Notifications will be made within 30 days of discovery.

Federal Database Checks (42 CFR § 455.436)

Monthly Exclusion Screening:

All employees, contractors, and vendors will be screened monthly against the OIG exclusion list and the System for Award Management (SAM) database.

The Compliance Department will maintain records of all exclusion checks.

Contractor Compliance:

All contractors are required to certify that they conduct monthly checks of their own employees and subcontractors against the OIG and SAM databases.

Social Security Act Compliance (§ 1862(e)(1)(B))

Medicare/Medicaid Screening:

FIS will verify that all healthcare professionals providing services under Medicare/Medicaid programs are not excluded by the OIG.

Verification will be performed before hiring and annually thereafter.

Compliance Monitoring and Auditing

The Compliance Officer will conduct quarterly audits to ensure adherence to this policy.

Initial: _____

Findings and corrective actions will be reported to the Executive Leadership Team.

Recordkeeping

Background check records, training certifications, and audit reports will be maintained for a minimum of seven years.

All records will be stored securely and accessed only by authorized personnel.

Responsibilities

Compliance Department: Responsible for conducting background checks and maintaining records.

Responsible for exclusion checks, abuse prevention training, and reporting to the OIG.

All Employees: Required to comply with all aspects of this policy and report any concerns immediately.

Violations

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

Initial: _____

Section 9

Foreign Corrupt Practices Act (FCPA)

Policy Statement:
Fabian Insurance Services is committed to conducting business with integrity, fairness, and in compliance with all applicable laws and regulations, including the Foreign Corrupt Practices Act (FCPA). The FCPA prohibits bribery of foreign officials and requires companies to maintain accurate books and records as well as internal controls. This policy outlines the responsibilities and procedures to ensure compliance with the FCPA and to prevent bribery and corruption in all business activities conducted by Fabian Insurance Services.

Purpose:
The purpose of this policy is to ensure that all employees, officers, directors, agents, and business partners of Fabian Insurance Services understand their obligations under the FCPA, to prevent corrupt practices, and to establish procedures for reporting and investigating potential violations. It aims to protect the company's reputation and ensure compliance with U.S. anti-bribery laws.

Scope:
This policy applies to all employees, officers, directors, agents, contractors, and business partners of Fabian Insurance Services, including those operating in the United States and in any foreign country where the company conducts business. It covers all interactions with foreign officials, business transactions, and record-keeping practices.

Overview of the Foreign Corrupt Practices Act (FCPA)

Prohibition of Bribery:
The FCPA prohibits offering, promising, or giving anything of value—directly or indirectly—to a foreign official with the intent to influence the official's actions or decisions to obtain or retain business or secure an improper advantage.

Books and Records Requirements:
The FCPA requires that Fabian Insurance Services maintain accurate books, records, and accounts that fairly reflect all transactions, including payments to foreign officials or other third parties. It also requires the implementation of effective internal controls to ensure transparency and prevent improper payments.

Definition of Foreign Officials:
A foreign official is any officer or employee of a foreign government, a public international organization, or any department or agency thereof. This includes employees of state-owned enterprises and candidates for political office.

Anything of Value:
Under the FCPA, "anything of value" is broadly defined and may include cash, gifts, entertainment, travel expenses, charitable donations, job offers, or any other item that could benefit the recipient.

Prohibited Conduct

Bribery of Foreign Officials:
Fabian Insurance Services strictly prohibits offering, giving, promising, or authorizing the payment of money or anything of value to any foreign official for the purpose of:

Influencing any act or decision of that official in their official capacity.

Inducing the official to act in violation of their lawful duties.

Securing any improper advantage.

Assisting in obtaining or retaining business.

Facilitating Payments:
The use of "facilitating payments" to expedite routine government actions (such as processing permits or providing police protection) is strictly prohibited, even if allowed under local law. All payments to foreign officials must be lawful under both U.S. and local law.

Third-Party Payments:
The company prohibits making or authorizing payments through intermediaries, such as agents, consultants, or business partners, if there is reason to believe that such payments could be used for improper purposes. Fabian Insurance Services must conduct due diligence on all third parties to ensure compliance with the FCPA.

Initial: _____

Gifts, Entertainment, and Hospitality

Guidelines for Gifts and Hospitality:

Gifts, entertainment, or hospitality provided to foreign officials must be of nominal value, infrequent, and consistent with local laws and customs.

Any gifts or hospitality must be properly documented, reported to the Compliance Officer, and approved in advance if exceeding a set threshold (e.g., $100).

Cash gifts or cash equivalents, such as gift cards, are strictly prohibited.

Pre-Approval Requirements:

Employees must seek pre-approval from the Compliance Officer before providing any gifts or hospitality to foreign officials, regardless of the value.

Detailed records of the nature, value, recipient, and purpose of the gift or hospitality must be maintained and submitted for review.

Record-Keeping and Internal Controls

Accurate Books and Records:
Fabian Insurance Services must maintain detailed and accurate records of all transactions, expenses, and payments, including those related to foreign officials. All records must be kept in accordance with the company's record retention policy.

Internal Controls:

The company will implement and maintain internal controls to ensure that all payments are properly authorized, documented, and recorded.

Regular audits will be conducted to ensure compliance with the FCPA and this policy.

The Compliance Officer will review and update the company's internal controls and procedures as necessary to address changes in regulations or business practices.

Reporting Violations and Whistleblower Protection

Reporting Procedure:

Employees who become aware of or suspect any conduct that may violate the FCPA or this policy are required to report it immediately to their supervisor, the Compliance Officer, or through the company's anonymous reporting hotline.

Reports may be made anonymously, and all reports will be treated confidentially to the extent possible.

Non-Retaliation:

Fabian Insurance Services strictly prohibits retaliation against any employee who, in good faith, reports a potential violation of this policy or participates in an investigation. Retaliation may result in disciplinary action, up to and including termination.

Investigation Process:

The Compliance Officer will promptly investigate any reported violations and take appropriate action, which may include corrective measures, reporting to relevant authorities, or disciplinary actions against those involved.

Training and Awareness

Mandatory Training:

All employees, officers, and directors of Fabian Insurance Services are required to complete FCPA training upon hire and annually thereafter. Training will cover the key provisions of the FCPA, the company's anti-bribery policy, and procedures for reporting potential violations.

Additional Training for High-Risk Employees:

Employees in roles that involve interactions with foreign officials, international business operations, or third-party management will receive additional, role-specific training on FCPA compliance.

Initial: _____

Disciplinary Actions for Non-Compliance

Consequences for Violations:

Any employee, officer, or director found to have violated this policy or the FCPA will be subject to disciplinary action, up to and including termination of employment.

Contractors, agents, and business partners who violate the FCPA or this policy may have their contracts terminated and may be reported to law enforcement authorities.

Cooperation with Authorities:

Fabian Insurance Services is committed to cooperating fully with regulatory authorities and law enforcement in the investigation and enforcement of the FCPA. Employees are required to cooperate with internal investigations related to FCPA compliance.

Initial: _____

Section 10
Compliance Risk Assessment

Policy Statement:
Fabian Insurance Services is dedicated to maintaining compliance with all relevant regulations, including those established by the Centers for Medicare & Medicaid Services (CMS). This Compliance Risk Assessment aims to identify, evaluate, and mitigate risks that could impact our ability to comply with CMS regulations. The goal is to ensure that our operations, practices, and interactions with clients meet the highest standards of integrity, accuracy, and transparency.

Purpose:
The purpose of this Compliance Risk Assessment is to systematically identify potential areas of non-compliance within Fabian Insurance Services, evaluate their likelihood and impact, and establish control measures to mitigate these risks. This process helps ensure that the company operates in compliance with all applicable laws and regulations, thereby minimizing the risk of regulatory sanctions, fines, and reputational damage.

Scope:
This assessment covers all operational, financial, and administrative activities of Fabian Insurance Services that are subject to CMS regulations, including but not limited to claims processing, marketing practices, data privacy, and fraud, waste, and abuse (FWA) prevention. It applies to all employees, officers, directors, agents, and third-party partners.

Risk Assessment Process

Step 1: Risk Identification
Using The CIS Critical Security Controls (CIS Controls), identify areas where the company's operations may be at risk of non-compliance with CMS regulations to safeguard PII. This involves reviewing internal processes, policies, and procedures, as well as analyzing past compliance issues, audit findings, and changes in CMS rules.

Step 2: Risk Evaluation
Assess each identified risk by evaluating:

Likelihood: The probability that a compliance issue could occur.

Impact: The potential severity of consequences, including financial penalties, legal implications, or harm to the company's reputation.

Step 3: Risk Prioritization
Rank the risks based on their likelihood and impact to determine which risks require the most immediate attention.

Step 4: Mitigation Strategies
Develop action plans to address each identified risk, including the implementation of controls, training, and monitoring processes to reduce the likelihood of non-compliance.

Step 5: Monitoring and Review
Regularly monitor compliance efforts and review the effectiveness of mitigation strategies. Update the risk assessment annually or as needed based on changes in CMS regulations or the company's business operations.

Key Risk Areas and Mitigation Strategies

Data Privacy and Security (HIPAA Compliance)

Risk: Non-compliance with HIPAA regulations, resulting in breaches of protected health information (PHI) and potential fines.

Likelihood: Moderate

Impact: High

Mitigation Strategies:

Implemented robust encryption and data access controls.

Conduct regular HIPAA training for all employees – Training is available

Perform periodic security audits and vulnerability assessments.

Develop an incident response plan for data breaches.

Initial: _____

Establish policies for secure data storage, transfer, and destruction.

Marketing and Communications (CMS Marketing Guidelines)

Risk: Misleading or non-compliant marketing materials that fail to adhere to CMS guidelines, resulting in penalties.

Likelihood: Moderate

Impact: Medium

Mitigation Strategies:

Develop a review and approval process for all marketing materials.

Train marketing staff on CMS regulations and guidelines for promoting Medicare products.

Conduct regular audits of outbound communications and marketing campaigns.

Establish a process for promptly addressing and correcting identified non-compliance in marketing practices.

Compliance with CMS Reporting Requirements

Risk: Failure to meet CMS reporting deadlines or inaccurate reporting, resulting in penalties or loss of contract.

Likelihood: Low

Impact: Medium

Mitigation Strategies:

Create a compliance calendar to track reporting deadlines and requirements.

Quarterly Compliance Review Meetings – Final Week and Day of the Last Month of Each Quarter

Assign responsibility for each reporting requirement to designated staff members.

Implement a quality control process to ensure the accuracy of reports before submission.

Conduct periodic internal audits of reports to ensure adherence to CMS guidelines.

Third-Party Vendor Compliance

Risk: Non-compliance by third-party vendors or downstream entities could result in regulatory penalties for Fabian Insurance Services.

Likelihood: Moderate

Impact: Medium

Mitigation Strategies:

Perform due diligence before engaging with new vendors, including compliance history checks.

Include compliance clauses in all contracts with third-party vendors.

Regularly monitor and audit vendors to ensure adherence to CMS requirements.

Provide training and guidance to third-party vendors on the company's compliance expectations.

Record Retention and Access

Risk: Failure to maintain required documentation or provide timely access to records during audits.

Likelihood: Low

Impact: Medium

Mitigation Strategies:

Develop a comprehensive record retention policy aligned with CMS requirements.

Implement electronic record-keeping systems with controlled access.

Train employees in proper documentation practices and the importance of accurate record-keeping.

Conduct annual reviews of record retention practices to ensure compliance.

Ongoing Monitoring and Reporting

Compliance Officer Responsibilities:

The Compliance Officer is responsible for overseeing the implementation of the compliance risk

assessment, monitoring progress on mitigation efforts, and reporting results to senior management.

The Compliance Officer will also conduct periodic reviews of the risk assessment and recommend updates as needed.

Annual Risk Assessment Review:

The Compliance Risk Assessment will be reviewed and updated annually or whenever there are significant changes in CMS regulations or the company's operations.

Updates will include reassessment of risks, evaluation of the effectiveness of mitigation measures, and identification of new potential risks.

Internal Audits and Reporting:

Internal audits of high-risk areas will be conducted quarterly to assess compliance with CMS regulations and internal policies.

Audit findings, including any identified areas of non-compliance, will be reported to the Compliance Committee, along with recommended corrective actions.

Initial: _____

Section 11 - Code of Conduct Document/Manual

- COC will be reviewed and updated annually in the first quarter of each year by the Executive Board
- Agents are to be trained on and, attest the code of conduct within 90 days of hire and once annually thereafter.
- See Code of Conduct Document available 24/7 at www.fabianinsurance.com

Initial: _____

Section 12
Communication/TCPA Policies

Purpose:
The purpose of this policy is to ensure compliance with the Telephone Consumer Protection Act (TCPA) and related regulations, which govern the use of automatic dialing systems, prerecorded voice messages, text messages, and calls to residential and mobile phones. This policy is designed to protect consumers' rights to privacy and prevent unsolicited communications from the health insurance agency while ensuring that all marketing and customer outreach activities are conducted lawfully.

Scope:
This policy applies to all employees, contractors, vendors, and agents of the health insurance agency who are involved in making outbound calls or sending text messages to prospective or existing customers. It encompasses all types of communication, including marketing, sales, surveys, customer service, and informational messages.

Overview of TCPA Requirements

The TCPA is a federal law that regulates telemarketing calls, auto-dialed calls, prerecorded voice messages, text messages, and faxes. The law is enforced by the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC). Key provisions of the TCPA relevant to the health insurance agency include:

Prohibition of Auto-Dialed Calls to Cell Phones: Prohibits using an automatic telephone dialing system (ATDS) or prerecorded voice messages to call or text a cell phone without prior express consent from the recipient.

No Prerecorded Voice Messages Without Consent: Requires prior express written consent before sending prerecorded voice messages for telemarketing purposes.

Do Not Call (DNC) Registry: Prohibits calls to numbers on the National DNC Registry, unless there is an established business relationship or explicit consent.

Calling Hours Restrictions: Prohibits calls before 8 a.m. or after 9 p.m. in the recipient's time zone.

Identification of Caller: Requires that the caller identifies themselves, provide the name of the company, and offer a contact phone number.

Obtaining and Documenting Consent

Prior Express Written Consent:

Obtain prior express written consent before making auto-dialed calls or sending text messages for telemarketing purposes to cell phones.

Consent must include a clear and conspicuous disclosure that the recipient agrees to receive such calls or messages. It must specify that these communications may be made using an automatic dialing system or prerecorded voice.

Consent must be documented and retained for at least five years, and it should include the date, time, and method by which consent was obtained.

Implied Consent for Non-Marketing Calls:

Consent may be implied for informational calls or messages (e.g., appointment reminders, policy updates) if the customer has provided their phone number during the course of an inquiry or transaction.

Even in these cases, maintain records of the customer’s consent and their phone number.

Do Not Call (DNC) Procedures

Internal DNC List:

Maintain an internal DNC list of consumers who have requested not to receive future calls or texts from the agency.

Update the internal DNC list regularly and ensure compliance with consumers’ requests within 30 days.

Employees must check this list before making any outbound calls or sending text messages to ensure compliance.

Initial: _____

National DNC Registry:

Subscribe to the National DNC Registry and scrub all outbound calling lists against this database every 31 days to ensure that no calls are made to numbers on the registry.

Calls to numbers on the National DNC Registry are allowed only if there is a current established business relationship or express written consent from the recipient.

Established Business Relationship (EBR):

An EBR allows calls to a consumer for up to 18 months after the last purchase or transaction or three months after an inquiry, even if their number is on the National DNC Registry.

Document the date and nature of any business transactions or inquiries to ensure compliance with EBR timeframes.

Call Restrictions and Identification

Calling Time Restrictions:

All telemarketing calls must be made between 8 a.m. and 9 p.m. local time of the recipient.

For non-marketing calls (e.g., customer service, appointment reminders), calls may be made outside of these hours only with the explicit consent of the recipient.

Caller Identification Requirements:

The caller must provide their name, the name of the health insurance agency, and a contact phone number during the call.

Ensure that the caller ID displayed to the recipient is accurate and identifies the health insurance agency.

Use of Automatic Dialers and Prerecorded Messages

Automated Telephone Dialing System (ATDS) Use:

Use of ATDS or automated dialing software must be restricted to phone numbers for which prior express written consent has been obtained.

Disable automated dialing capabilities for numbers that have been identified as non-consenting or on any DNC lists.

Prerecorded Voice Messages:

Prerecorded messages may only be used for non-telemarketing purposes (e.g., important policy information, claims status updates) unless prior express written consent has been obtained for telemarketing messages.

Provide a clear opt-out mechanism during the prerecorded message, allowing the recipient to request not to receive future messages.

Text Messaging Compliance

Text Message Consent:

Obtain prior express written consent before sending text messages for marketing purposes.

For non-marketing texts (e.g., appointment reminders, policy updates), document any implied consent provided by the customer when they share their mobile number.

Opt-Out Mechanisms:

Include a simple opt-out mechanism in each text message, such as "Reply STOP to unsubscribe."

Process opt-out requests immediately and ensure that recipients who have opted out are added to the internal DNC list.

Training and Awareness

Employee Training:

Provide training to all employees involved in outbound calling or messaging, including sales, marketing, and customer service teams.

Training should cover the requirements of the TCPA, proper use of auto-dialers, consent documentation, and DNC compliance.

Initial: _____

Ongoing Refresher Courses:

Conduct regular refresher training sessions to keep employees updated on any changes to the TCPA or company policies.

Document attendance and completion of training sessions.

Monitoring and Quality Assurance

Call Monitoring:

Monitor a sample of outbound calls regularly to ensure adherence to TCPA rules and the agency's internal policies.

Address any violations or issues identified during monitoring through retraining or disciplinary action.

Quality Assurance Reviews:

Conduct periodic audits of consent records, call logs, and DNC compliance procedures to identify areas for improvement.

Engage external compliance consultants if necessary to review and assess TCPA compliance practices.

Penalties for Non-Compliance

Federal Penalties:

Violations of the TCPA can result in significant fines, including up to $500 per violation, and up to $1,500 per violation for willful or knowing violations.

Individuals may also file lawsuits against companies for violations, potentially leading to substantial settlements.

Internal Disciplinary Actions:

Employees or contractors who violate this policy may face disciplinary action, up to and including termination of employment or contract.

Policy Review and Updates

Annual Review:

Review this TCPA policy annually or whenever significant changes occur in the regulations.

Update the policy to reflect any changes in federal, state, or local regulations or agency practices.

Policy Availability:

This policy is available 24/7 to all employees and clients on the Fabian Insurance Services Website.

Employees will be notified of any changes to the policy through internal communications or during training sessions.

Conclusion:

This TCPA policy ensures that all outbound communication activities are compliant with federal regulations while respecting the rights and privacy of consumers. By adhering to these procedures, the health insurance agency aims to maintain trust and integrity in its interactions with clients and prospects.

Initial: _____

Section 13
Computer System Backup Policies

Policy Statement:
Fabian Insurance Services is committed to maintaining the integrity, confidentiality, and availability of its electronic information systems and data, as required by the Centers for Medicare & Medicaid Services (CMS) regulations and other applicable laws. This Computer System Backup Policy establishes the procedures for regular backups of electronic data to protect against data loss, unauthorized access, and ensure business continuity.

Purpose:
The purpose of this policy is to outline the requirements for data backup, storage, and recovery procedures to ensure that critical data is safeguarded and can be restored in the event of a system failure, data corruption, or disaster.

Scope:
This policy applies to all employees, contractors, and third-party vendors of Fabian Insurance Services who have access to the company's computer systems, data, and applications, including electronic health records (EHR), billing systems, and customer databases.

Data and Documents E-Stored and Backed-Up

1. Client Health Information (PHI)

- Includes all HIPAA-protected health information such as medical history, and prescription drugs.
- Examples: NEADS Analysis Data, Explanation of Benefits (EOBs), and prior authorizations.

2. Personally Identifiable Information (PII)

- Includes client demographic and contact information that could identify an individual.
- Examples: Names, addresses, Social Security numbers, Medicare and Medicaid identification numbers, phone numbers, and email addresses.

3. Policy and Enrollment Records

- Documents related to client insurance policies and enrollment details.
- Examples: Signed insurance applications, plan selections, coverage details, and proof of eligibility.

4. Payment and Billing Records

- Financial documents related to premium payments and agency accounts.
- Examples: Receipts, invoices, payment schedules, and electronic payment transaction logs.

5. Agent and Staff Records

- Internal documents concerning employees and agents.
- Examples: Licensing documentation, training certifications, contracts, and non-disclosure agreements (NDAs).

6. Compliance and Regulatory Documents

- Documents required for audits or compliance with legal and regulatory requirements.
- Examples: HIPAA compliance checklists, CMS guidelines, state insurance approvals, and audit logs.

7. Contracts and Agreements

- Legal agreements with clients, providers, or vendors.
- Examples: Client-agent contracts, service agreements, and business associate agreements (BAAs).

8. Correspondence Records

- Communications related to client service, claims, and policy inquiries.
- Examples: Email correspondence, chat logs, and customer service notes.

Initial: _____

9. Marketing and Outreach Materials

- Records of marketing campaigns and client communications.
- Examples: Direct mail templates, campaign response logs, and permission/opt-in records for communications.

10. Operational and Procedural Documentation

- Internal documentation for business continuity and daily operations.
- Examples: Policy and procedure manuals, disaster recovery plans, and IT security protocols.

Backup Frequency and Schedule

Daily Backups:
All critical data, including patient records, financial information, and operational data, must be backed up daily. Incremental backups should be performed throughout the day to capture changes made to data.

Weekly Full Backups:
A full backup of all systems, applications, and databases will be conducted weekly to ensure comprehensive data recovery capabilities.

Monthly Archive Backups:
Monthly archive backups will be maintained to preserve historical data for compliance and audit purposes.

Backup Methods

Automated Backup Solutions:
Automated backup systems will be used to minimize human error and ensure consistent backup execution. Backup solutions must include encryption to protect sensitive data both at rest and in transit.

Offsite Backups:
Backups will be stored securely offsite, ensuring that copies of critical data are available in the event of a disaster affecting onsite systems. Offsite storage facilities must meet security standards and comply with CMS regulations.

Cloud Backup Services:
Cloud-based backup solutions may be utilized, provided that they comply with applicable security and privacy standards, including HIPAA. All cloud providers must sign a Business Associate Agreement (BAA) with Fabian Insurance Services.

Backup Storage and Security

Access Controls:
Access to backup data must be restricted to authorized personnel only. Access logs must be maintained to monitor who accesses backup systems and data.

Data Encryption:
All backups containing sensitive information must be encrypted using industry-standard encryption protocols to protect data confidentiality.

Physical Security:
Physical security measures must be in place for all backup media stored offsite, including secure facilities with controlled access.

Data Recovery Procedures

Regular Testing:
Backup systems must be tested at least quarterly to ensure that data can be successfully restored. Tests will simulate different disaster scenarios to evaluate recovery time and effectiveness.

Recovery Time Objective (RTO):
Establish and document an RTO for critical systems to minimize downtime in the event of a data loss incident. RTO will be assessed annually and adjusted as necessary based on business needs.

Recovery Point Objective (RPO):
Define the maximum acceptable amount of data loss measured in time, which determines the frequency of backups. This will guide backup scheduling and procedures.

Documentation and Record Keeping

Backup Logs:
Backup operations must be logged, including details such as the date, time, type of backup (full,

Initial: _____

incremental, archive), and personnel involved. Logs will be reviewed regularly to identify any issues.

Policy Documentation:
This policy and any associated procedures must be documented, maintained, and accessible to all employees responsible for data backup and recovery operations.

Retention of Backup Data:
Backup data must be retained according to regulatory requirements and company policy. Typically, full backups will be retained for a minimum of seven years, unless otherwise specified by applicable laws or regulations.

Employee Training and Awareness

Training Programs:
All employees with access to sensitive data must receive training on this policy, data backup procedures, and the importance of data security. Training will be conducted upon hire and at least annually thereafter.

Awareness Campaigns:
Regular awareness campaigns will be conducted to reinforce the importance of data backups, security measures, and employee responsibilities in protecting sensitive information.

Compliance and Enforcement

Monitoring Compliance:
The Compliance Officer will monitor adherence to this policy and conduct periodic audits to ensure compliance with backup procedures and security measures.

Non-Compliance Consequences:
Failure to comply with this policy may result in disciplinary action, up to and including termination, as well as potential legal ramifications.

Policy Review and Revision

Annual Review:
This Computer System Backup Policy will be reviewed annually and updated as necessary to reflect changes in CMS regulations, technology, or business operations.

Policy Updates:
Employees will be notified of any significant changes to this policy, and updated copies will be made available through the company intranet or other communication channels.

Initial: _____

Section 14 - Offsite Storage Policies

Policy Statement:
Fabian Insurance Services is committed to ensuring the confidentiality, integrity, and availability of sensitive data, including protected health information (PHI) and other critical business records. This Offsite Storage Policy establishes guidelines for the secure storage of electronic and physical records offsite, ensuring compliance with Centers for Medicare & Medicaid Services (CMS) regulations, HIPAA standards, and other applicable laws.

Purpose

The purpose of this policy is to outline the procedures and requirements for the offsite storage of sensitive information and records, ensuring that all data is adequately protected against unauthorized access, loss, or damage.

Scope

This policy applies to all employees, contractors, and third-party vendors of Fabian Insurance Services who manage, access, or store sensitive data offsite. This includes physical records, electronic data, and any associated materials that contain PHI or other sensitive information.

Definitions

Offsite Storage: The secure storage of physical documents and electronic data at a location away from the primary business premises of Fabian Insurance Services.

Protected Health Information (PHI): Any information about health status, provision of healthcare, or payment for healthcare that can be linked to an individual.

Business Associate: A person or entity that performs services on behalf of, or provides certain functions or activities for, a covered entity that involves the use or disclosure of PHI.

Offsite Storage Procedures

Selection of Offsite Storage Providers

Due Diligence:

Only use reputable offsite storage providers that have been thoroughly vetted. Ensure they have appropriate security measures in place to protect sensitive data.

Verify that offsite providers comply with HIPAA and CMS regulations and are willing to enter into a Business Associate Agreement (BAA) if they will have access to PHI.

Security Measures:

Ensure that the storage facility has adequate security measures in place, including access controls, surveillance systems, and environmental controls to protect against fire, water damage, and unauthorized access.

Physical Records Storage

Documentation:

Maintain a detailed inventory of all physical records sent offsite, including the contents, date of transfer, and storage location.

Implement a check-in/check-out system to track the retrieval and return of physical records stored offsite.

Access Controls:

Restrict access to physical records stored offsite to authorized personnel only. Access logs should be maintained to document who accessed the records and when.

Secure Transport:

When transferring physical records to an offsite location, use secure transport methods. Ensure that records are transported in locked containers and are monitored during transit.

Electronic Data Storage

Data Encryption:

All electronic data stored offsite must be encrypted both in transit and at rest to prevent unauthorized access.

Initial: _____

Access Controls:

Implement strong access controls for electronic records stored offsite, including user authentication, role-based access, and periodic access reviews.

Backup Procedures:

Ensure that electronic data stored offsite is regularly backed up according to the company's data backup policy. This includes maintaining backup copies in a separate location to ensure data redundancy.

Record Retention and Disposal

Retention Schedule:

Adhere to the record retention schedule defined by CMS and other regulatory requirements. Maintain records for the required duration and ensure compliance with all relevant laws.

Disposal Procedures:

When records are no longer needed, dispose of them securely to prevent unauthorized access. For physical records, use shredding services that comply with HIPAA regulations. For electronic data, ensure complete data deletion in accordance with industry best practices.

Employee Training and Awareness

Training Programs:

All employees who manage, access, or store sensitive data offsite must receive training on this policy and the importance of protecting PHI and other sensitive information.

Conduct regular refresher training and awareness campaigns to reinforce security practices related to offsite storage.

Compliance and Monitoring

Compliance Audits:

Conduct regular audits of offsite storage practices to ensure compliance with this policy, HIPAA regulations, and CMS guidelines.

Review the offsite storage providers' security measures and practices annually to ensure they continue to meet compliance requirements.

Incident Reporting:

Any security incidents, including breaches or unauthorized access to offsite records, must be reported immediately to the Compliance Officer. An incident response plan should be followed to investigate and mitigate any identified risks.

Policy Review and Updates

Annual Review:

This Offsite Storage Policy will be reviewed annually and updated as necessary to reflect changes in regulations, best practices, or company operations.

Communication of Changes:

Employees will be notified of any significant changes to this policy, and updated copies will be made available through the company intranet or other communication channels.

Initial: _____

Section 15

Disaster Recovery Plan

Policy Statement:
Fabian Insurance Services is dedicated to ensuring the continuous operation of its business and the protection of sensitive data, including protected health information (PHI). This Disaster Recovery Plan outlines the procedures and protocols to be followed in the event of a disaster, ensuring compliance with Centers for Medicare & Medicaid Services (CMS) guidelines, HIPAA regulations, and best practices for data protection and business continuity.

Purpose

The purpose of this Disaster Recovery Plan is to establish a comprehensive framework for responding to disasters, restoring operations, and protecting sensitive data to minimize the impact on clients and business operations.

Scope

This plan applies to all employees, contractors, and third-party vendors of Fabian Insurance Services involved in disaster recovery efforts. It encompasses all aspects of disaster recovery, including IT systems, facilities, and critical business functions.

Risk Assessment

Identify Potential Risks:
Conduct a thorough assessment to identify potential disasters that could impact operations, including:

Natural disasters (hurricanes, tornadoes, floods, fires)

Cybersecurity incidents (data breaches, ransomware attacks)

Technical failures (hardware malfunctions, software outages) Assessed by CIS Con

Human factors (employee error, sabotage)

Impact Analysis:
Evaluate the potential impact of identified risks on business operations, clients, and sensitive data. Prioritize risks based on their likelihood and potential severity.

Disaster Recovery Team

Team Structure:
Roles and Responsibilities:
See also FIS Emergency Action Plan

Team Leader: Luis Hernandez
Operations & Communications Coordinator: Jeannie Pond
Facilities Coordinator: Rossy Adams
Employee Liaison: Alianah Hernandez

Overseeing the effort: Managing the entire disaster recovery effort, including ensuring effective communication and coordination

Making decisions: Making critical decisions as needed

Reporting on progress: Reporting on the progress of the recovery

All disaster recovery team members should have significant leadership experience and a deep understanding of business operations.

Other responsibilities of a disaster recovery team include:

- Overseeing data recovery management
- Conducting risk assessments and mitigation procedures
- Training employees and spreading awareness after disasters
- Evaluating historical disasters to identify areas for improvement
- Managing service provider contracts and DR service vendors
- Setting alerts to notify employees when a disaster occurs
- Establishing roles and duties for each team member
- Securing physical locations
- Coordinates all recovery efforts and communication referencing emergency phone/text and email tree
- Technology: Manages data recovery and restoration of IT systems.
- Operations Oversight: Oversees the continuity of business operations.

Initial: _____

Disaster Recovery Procedures

Refer to the disaster recovery template available 24/7 on the Cloud Server>Shared Admin>Business Continuity Team

Communication Plan

Internal Communication:
Develop a communication plan to keep employees informed during a disaster. This may include:

Regular updates via email or company intranet.

Use of emergency notification systems to reach all employees.

External Communication:
Establish a protocol for communicating with clients, vendors, carriers and the media as soon as it is safe to do so. Appoint a designated spokesperson to provide consistent and accurate information.

Training and Testing

Employee Training:
Conduct regular training sessions for all employees on disaster recovery procedures, emergency protocols, and their specific roles in the recovery process.

Disaster Recovery Drills:
Schedule and conduct disaster recovery drills at least annually to test the effectiveness of the plan. Evaluate the results and update the plan as needed.

Compliance and Monitoring

Monitoring Compliance:
The Compliance Officer will monitor adherence to this Disaster Recovery Plan and conduct periodic audits to ensure compliance with CMS guidelines and HIPAA regulations.

Review and Update:
This plan will be reviewed and updated annually or as necessary to reflect changes in operations, technology, and regulations.

Documentation and Record Keeping

Record Retention:
Maintain detailed records of disaster recovery activities, training sessions, drills, and any incidents that occur. These records will be kept for a minimum of seven years or as required by applicable regulations.

Policy Documentation:
Ensure that all policies, procedures, and contact information related to the disaster recovery plan are documented and easily accessible to authorized personnel.

Policy Review and Updates

Annual Review:
This Disaster Recovery Plan will be reviewed at least once a year by the Executive Board Members, and updates will be made as needed based on lessons learned, regulatory changes, or operational shifts.

Communication of Changes:
Employees will be notified of any significant changes to this plan, and updated copies will be made available through the company intranet or other communication channels.

Initial: _____

Section 16
Business Continuity Plan

Disaster Recovery Policy: Backup, Storage, and Recovery of Electronic Protected Health Information (ePHI)

Purpose

This policy ensures that Fabian Insurance Services maintains secure, retrievable, and compliant backups of electronic protected health information (ePHI) to safeguard against data loss and ensure continuity in case of system failures or disasters. It complies with federal regulations under Title 45 CFR §164.308(7)(i)-(ii) and §164.312(a)(2)(ii), and other contractual requirements, such as those from AHCA, FHK, ODMR, and Carriers including but not limited to Elevance Health.

Scope

This policy applies to all Fabian Insurance Services systems containing ePHI, including cloud-hosted data environments, backup facilities, and disaster recovery sites. It covers secure storage, retrieval, and handling of backup data to comply with federal and state requirements.

Policy Statement

Fabian Insurance Services commits to backing up ePHI daily, securing it in offsite U.S.-based locations, and implementing a disaster recovery plan to ensure that backups are retrievable, and systems are resilient in case of failure. Offsite backups are stored both electronically and physically, as required by VA CCC and other contractual obligations.

Data Backup and Disaster Recovery

Data Backup

Daily Backups: Fabian Insurance Services will perform daily backups of all systems containing ePHI, as required by Title 45 CFR §164.308(7)(ii)(A) and the VA CCC requirements. Backup activities will ensure that exact copies of ePHI are created and retained.

Backup Retention and Verification: Backups will be stored per the retention requirements defined in the AHCA and carrier contracts. Systems must be verified regularly to confirm the integrity and accessibility of backups.

Compliance Evidence: Backup logs and records of backup verifications will be maintained and made available as evidence of compliance with data backup requirements.

Disaster Recovery Plan

Disaster Recovery Procedures: Fabian Insurance Services has a comprehensive disaster recovery plan (DRP) that aligns with Title 45 CFR §164.308(7)(ii)(B), including procedures to restore access to ePHI following an emergency or failure. This DRP will be reviewed annually or as needed to incorporate updates from contract amendments (e.g., Indiana HCC 51705, amendment #4).

Geographically Diverse Facilities: In accordance with Elevance Health MSA 4.9.9, the DRP includes the use of two geographically diverse facilities. If the primary site is unavailable, services will be restored at a secondary site with staffing and resources to ensure continuity without additional charges.

Secondary Site Location(s):
CoHatch Lakeland:
211 E Main St, Lakeland, FL 33801

Evidence of Compliance: Disaster recovery exercises and logs of recovery drills will be documented as evidence of compliance.

Emergency Access to Systems

Emergency Access Procedure: To comply with Title 45 CFR §164.312(a)(2)(ii), emergency access procedures are in place to ensure immediate access to ePHI during an emergency. Access to systems during an emergency will follow strict protocols to ensure the security and privacy of ePHI.

Compliance Evidence: Logs of emergency access events and records of authorization will be maintained to show adherence to this standard.

Secure Storage of Backups

Offsite Backup Storage

Initial: _____

U.S.-Based Storage Requirement: In compliance with Title 45 CFR §164.310(d)(2)(iv) and VA CCC requirements, all backups of ePHI must be stored in secure, U.S.-based offsite facilities. Data storage is restricted to U.S. locations, with no offshore storage permitted, although data processing may occur in other locations if data resides on U.S.-based servers.

Physical Security of Storage Sites: All physical backup media, if applicable, will be stored in a secure facility that meets physical safeguards as per Title 45 CFR §164.310. Facilities are monitored and access-controlled to prevent unauthorized access to physical backup copies.

Evidence of Compliance: Physical and electronic security reports, as well as records of offsite storage facility inspections, will be documented to demonstrate compliance with offsite storage requirements.

4.2 Cloud Backup and Data Location Requirements

U.S.-Based Cloud Hosting: For cloud-hosted ePHI, data must remain on servers physically located within the United States, per the Indiana HCC contract and AHCA data location requirements.

Contractual Adherence: All data hosting in cloud environments must follow requirements outlined in contract agreements such as the CA MSA and BAA attachment, which prohibit offshore storage of Health Plan confidential information.

Compliance Evidence: Documentation from cloud service providers and configuration audits verifying the U.S.-based location of data storage will be retained.

s1.3 Geographic Diversity for Disaster Recovery Sites

Backup and Alternate Sites: Per Elevance Health MSA 4.9.9, Fabian Insurance Services will maintain at least two geographically diverse sites for disaster recovery purposes. This ensures that, should one location become unavailable, a backup site is immediately ready for service restoration, including necessary staffing and resources.

Compliance Evidence: Site configuration records and evidence of geographic diversity, including recovery site activation records, will be documented to verify compliance.

s1.4 Evidence of Compliance and Review

Evidence Documentation: Backup logs, access logs, disaster recovery test results, facility inspection reports, and geographic redundancy documentation will all serve as evidence of compliance.

Annual Review and Updates: This policy will be reviewed annually to incorporate updates from federal, state, and contract requirements. Any changes or amendments will be communicated to relevant personnel to ensure ongoing compliance.

Citations

Title 45 CFR §164.308(7)(i)-(ii) - Federal requirements for contingency plans, including data backup and disaster recovery standards.

Title 45 CFR §164.312(a)(2)(ii) - Emergency access standards for systems containing ePHI.

Title 45 CFR §164.310(d)(2)(iv) - Physical safeguards for secure offsite backup storage.

VA CCC Requirement - Mandates daily backups and offsite storage of ePHI within the United States.

Contractual References:

AHCA Contract No. FP 103 and FP068, FHK Contract No. 2020-03, ODMR 2021-0024, Elevance Health MSA 4.9, CA MSA, and related BAAs.

This policy ensures Fabian Insurance Services adheres to all applicable federal, state, and contract requirements for data backup, storage, and disaster recovery, maintaining the security and integrity of member ePHI.

Initial: _____

Section 17
Emergency Management Plan

See Also FIS Emergency Action Plan

Policy Statement:
Fabian Insurance Services is committed to ensuring the safety and well-being of its employees, clients, and assets in the event of emergencies, including fires, tornadoes, and hurricanes. This Emergency Management Plan provides guidelines for preparedness, response, recovery, and mitigation in such situations, specifically tailored to the unique risks associated with Mulberry, Florida.

Purpose:
To establish a framework for effective emergency management in the face of natural disasters, ensuring the safety of personnel and minimizing disruption to business operations.

Objectives:

Ensure the safety of employees and clients during emergencies.

Minimize property damage and protect company assets.

Maintain essential business functions during and after emergencies.

Communicate effectively with employees, clients, and emergency services.

Risk Assessment

Fire Risks: – Roles/Responsibilities/Timeframe

Causes: Electrical faults, equipment malfunctions, arson, cooking accidents.

Preventative Measures: Regular maintenance of equipment, fire extinguishers, and smoke detectors; employee fire safety training.

Tornado Risks: – Roles/Responsibilities/Timeframe

Seasonal Occurrence: Typically, from late spring to early summer in Florida.

Preventative Measures: Employee training on tornado safety, regular tornado drills, and clear identification of safe areas.

Hurricane Risks:

Seasonal Occurrence: June 1 to November 30.

Preventative Measures: Early warning systems, evacuation plans, and securing property and equipment.

Preparedness – Roles/Responsibilities/Timeframe

Training and Drills

Conduct regular emergency preparedness training sessions for all employees, focusing on fire safety, tornado safety, and hurricane preparedness.

Schedule drills for fire evacuations and tornado sheltering at least twice a year.

Emergency Supplies

Maintain an emergency supply kit that includes:

First aid supplies

Flashlights and batteries

Non-perishable food and water (enough for at least 72 hours)

Portable phone chargers

Emergency contact list

Communication Plan

Establish a communication protocol for notifying employees and clients in case of emergencies:

Use multiple communication channels (text messages, emails, company intranet) for alerts.

Maintain an updated contact list for all employees and clients.

Assign a spokesperson to communicate with the media if necessary.

Initial: _____

Response Procedures

Fire Emergency

Evacuation Plan: See Diagram Included on FIS Emergency Action Plan

Identify and clearly mark all exits.

Designate safe assembly points outside the building.

Conduct regular fire drills to familiarize employees with evacuation routes.

Fire Extinguishing:

Train employees on the proper use of fire extinguishers.

Designate a Fire Warden to oversee evacuations and ensure everyone is accounted for.

Tornado Emergency

Shelter Procedures:

Identify the safest area in the building (interior rooms, basements, or designated shelters).

Notify employees immediately when a tornado warning is issued.

Communication:

Use a loudspeaker or intercom system to inform staff of the situation.

Have a plan to monitor weather updates via local news and NOAA weather radios.

Hurricane Emergency

Pre-Hurricane Preparedness:

Monitor storm forecasts and issue alerts as needed.

Secure and reinforce windows and doors in anticipation of strong winds.

Create a plan for securing company property and data (backups, securing equipment).

Evacuation Procedures:

Develop an evacuation plan for employees and clients if necessary.

Establish communication with local authorities and follow their guidance regarding evacuations.

Recovery and Mitigation

Post-Emergency Evaluation

Conduct a debriefing after any emergency event to evaluate the response and identify areas for improvement.

Gather feedback from employees on the effectiveness of the emergency response plan.

Business Continuity Planning

Develop a business continuity plan outlining how operations will be restored after an emergency, including:

Prioritizing critical business functions.

Identifying alternate work locations if necessary.

Communicating recovery plans to employees and clients.

Ongoing Training and Review

Regularly review and update the Emergency Management Plan based on lessons learned from drills and actual emergencies.

Provide ongoing training to ensure all employees remain informed about procedures and safety protocols.

Responsibilities –

See Also Section 15 – Disaster Recovery Plan

Emergency Management Team: Rolls. Responsibilities, Actions Timeframe

Luis Hernandez – Leadership

Aliana Hernandez - Committee Coordinator

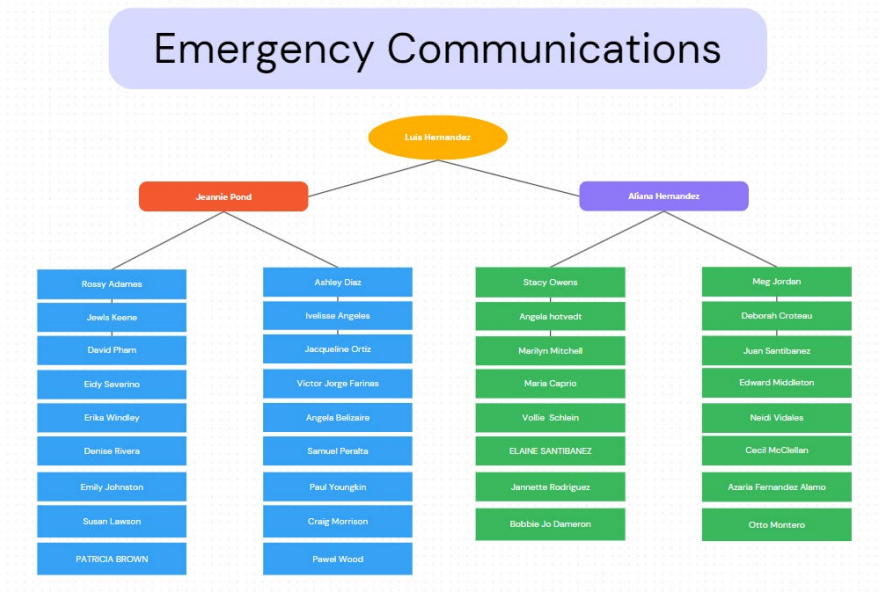
Rossy Adames – Administrative and Facilities

Jeannie Pond – Communications and Operations

Responsible for overseeing the implementation of this plan, including training, drills, and communication.

Initial: _____

Activates phone tree to maintain continuous client coverage – all are to be programmed into committee cell phones.



Ensure that emergency supplies are maintained and accessible.

All Employees:

Responsible for familiarizing themselves with emergency procedures and participating in training and drills.

Report any safety hazards or concerns to the Emergency Management Team.

Policy Review and Updates

This Emergency Management Plan will be reviewed annually and updated as necessary to reflect changes in regulations, best practices, or company operations.

Employees will be notified of any significant updates to the plan.

Initial: _____