POLICY & PROCEDURE	COMP # 1
NIVANO PHYSICIANS, INC. (NIVANO)	Original Effective Date: 01/01/2018 Revised Date: 12/13/2018 Review Date:
DEPARTMENT	COMPLIANCE
SUBJECT	HIPAA - PHI

INTRODUCTION

Nivano Physicians, Inc. (Nivano) has adopted and maintains policies and procedures required by the Health Insurance Portability and Accountability Act (HIPAA) and the American Recovery and Reinvestment Act (ARRA) to:

A. Ensure that Member's health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care;

B. Comply with the requirements of ARRA including, but not limited to, Member requests for restrictions and accounting of disclosures;

C. Protect the public's health and well- being;

D. Adhere to the HIPAA General Administrative Requirements as published in the final rule on December 28, 2000 and amended on May 31, 2002 and August 14, 2002. These requirements are found in Title 45 of the Code of Federal Regulations (C.F.R.) Part 160, Part 162, and Part 164. Comply with the administrative, physical and technical safeguards of the HIPAA Security Rule, as required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and any and all Federal regulations and interpretive guidelines promulgated thereafter;

E. Comply with the California Department of Health Care Services (DHCS); Center for Medicare and Medicaid Services (CMS); and, the HITECH Act breach reporting requirements.

Provide HIPAA training to Nivano Team Members, Governing Board Members and Management; business associates, first tier and downstream entities and vendors with access to Member PHI.

HIPAA PROGRAM

A. Purpose

1. To accept and comply with a common set of general provisions and definitions related to HIPAA and ARRA guidelines.
2. To identify and apply: (a) any HIPAA pre-emption requirements to State law; and (b) any State law that is more stringent than the requirements of HIPAA.
3. To establish Nivano Compliance and Enforcement procedures, based upon HIPAA and ARRA Standards and Implementation Specifications.

B. Scope

1. The HIPAA Program, which falls under the auspices of Compliance, applies to:

a. All Nivano Team Members, Governing Board Members, Management, Contracted Entities/BA

b. Every health care provider, regardless of size, who holds or transmits Member protected health information (PHI) in any form of media, whether electronic, paper or oral (covered entities); and,

c. Nivano business associates, first tier and downstream entities and vendors that perform certain functions or activities on behalf of Nivano that involve the use or disclosure of Member identifiable health information.

C. Organizational Structure and Resources

1. The day-to-day oversight of the HIPAA Program is the direct responsibility of the **Compliance Officer**, who reports compliance issues and activities to Senior Management and the Chief Executive Officer.

2. The **Compliance Officer** oversees all aspects of the Program including but not limited to:
   a. Uses and disclosures of Protected Health Information (PHI): **Definition:** All individually identifiable health information,(including genetic information) whether oral or recorded in any form, that relates to the past, present, or future physical or mental health or condition of a Member; the provision of health care to a Member; or the past, present, or future payment for the provision of health care to a Member (45 C.F.R. § 160.103).PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); in employment records held by a Covered Entity in its role as employer; and regarding a person who has been deceased for more than fifty (50) years. PHI also generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a healthcare professional to identify an individual and to determine appropriate care

   b. Privacy policies and procedures, including but not limited to complaint procedures and compliance with state and federal reporting requirements;

   c. Team Member, Business Associate, First tier and downstream entity, Training program;

   d. Mitigation of any harmful effects caused by use or disclosure of PHI by Nivano Team Members or external associates in violation of Nivano privacy policies and procedures; and,

   e. Maintenance of reasonable and appropriate administrative, technical and physical safeguards to prevent intentional or unintentional use or disclosure of PHI.

2. The Compliance Officer has ultimate responsibility for the HIPAA Program.

3. The Nivano Governing Board will provide oversight of the HIPAA Program.

D. DEFINITIONS

1. **Access and Uses**: For internal uses, Nivano allows Team Member access to PHI subject to qualifying job requirements. Each Team Member is provided appropriate levels of security to perform their job duties.
2. **Authorization:** Nivano must obtain the Member's written authorization for any use or disclosure of PHI that is not for treatment, payment, health care operations or otherwise permitted or required by regulations and/or statutes. Authorizations must be written in specific terms; must be in plain language; and must contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data in accordance with the requirements of HIPAA (45 C.F.R. § 164.508) and California Confidentiality of Medical Information Act (Civil Code § 56.11).

   In most cases, parents can exercise individual rights, such as access to the medical record on behalf of their minor children. However, there are circumstances under which the parent is not considered the personal representative. In these situations, Nivano will defer to California State law to determine the rights of parents to access and control the PHI of their minor children.
3. **Breach:** The term "breach" has the meaning given such term in 45 C.F.R. § 164.402.
   a. Definition: "Breach" means the acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted under 45 C.F.R. Part 164, Subpart E ("Privacy Rule") which compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity can demonstrate that there is low probability that the PHI has been compromised. For purpose of this definition, compromises the security or privacy of the PHI means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at 45 C.F.R. § 164.514(e) (2), date of birth, and zip code does not compromise the security or privacy of the PHI.

      1) The nature and extent of PHI involved (including the types of identifiers and the likelihood of re-identification).

      2) The unauthorized person who used the PHI or to whom the disclosure was made.

      3) Whether the PHI was actually acquired or viewed and;

      4) The extent to which the risk to the PHI has been mitigated

   b. **Exceptions: Breach Excludes:**

      1) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

2) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used, or disclosed in a manner not permitted under the Privacy Rule.

` 3) A disclosure of protected health information where the covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (A covered entity may be a business associate of another covered entity).

4) If the acquisition, access, use or disclosure of protected health information is excluded from the definition of "breach" under paragraph 3.b. above, the reporting requirements of DHCS, and / or CMS do not apply.

4. **Business Associate**: The term "business associate" has the meaning given such term in Title 45, C.F.R. § 160.103.

   a. Except as provided in paragraph 4(b) of this definition, business associate means, with respect to a covered entity, a person who:

      1) On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

         a. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or

         b. Any other function or activity regulated by this subchapter; or

      2) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the services involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person

   b. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph 4(a)(1)of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph 4(2) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities

participating in such organized health care arrangement.

c. A covered entity may be a business associate of another covered entity.

5. **Confidentiality:** Relates to the obligation of the holder of personal information to protect an individual's privacy. This obligation is determined by common practice, and federal and state laws and regulations

6. **Covered Entity:** The term "covered entity" has the meaning given such term in 45 C.F.R. § 160.103.

   a. A health plan.

   b. A health care clearinghouse.

   c. A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter, e.g., HIPAA Administrative Data Standards and Related Requirements.

7. **Disclosure:** The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information (45 C.F.R. § 160.103).

8. **Downstream Entity:** is any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the MA benefit or Part D benefit, below the level of the arrangement between an MAO or applicant or a Part D plan sponsor or applicant and a first tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services. (See, 42 C.F.R. §, 423.501).

9. **Electronic Health Record (EHR):** An electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff (42 U.S.C. § 17921(5)).

10. **First Tier Entity:** is any party that enters into a written arrangement, acceptable to CMS, with an MAO or Part D Plan sponsor or applicant to provide administrative services or health care services to a Medicare eligible individual under the MA program or Part D program. (See, 42 C.F.R. §,423.501).

11. **Vendors / Contractors**: Includes all contracted Providers and suppliers, first tier entities, downstream entities and any other entities involved in the delivery of payment for or monitoring of benefits.

12. **Healthcare Individuals:** An individual physician or other health care professional, a hospital, a provider-sponsored organization, a health maintenance organization, a health insurance plan, or any other kind of health care facility, organization, or plan.

13. **Healthcare Operations:** Includes activities of the covered entity to the extent that the activities are related to covered functions:

    a. Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health

care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner/provider performance, health plan performance, conducting training programs under supervision to practice or improve health care provider skills, training of non-health care professionals, accreditation, certification, licensing or credentialing activities.

c. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs.

d. Business planning and development including formulary development and administration, development or improvement of methods of payment or coverage policies.

e. Business management and general administrative activities of the entity as outlined in 45 C.F.R. §164.501.

12. **Health Care Provider**: A provider of medical or health services; pursuant to Title 42 United States Code (U.S.C.) Section 1395x subsections (s) and (u); and, any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. (45 C.F.R. §160.103.

13. **Health Plan**: An individual or group plan that provides, or pays the cost of, medical care as defined in Title 42 U.S.C. §300gg-91(a)(2) (45 C.F.R. §160.103

14. **Individual**: The person who is the subject of the protected health information (45 C.F.R. § 160.103).

15. **Individually Identifiable Information**: Is Information that is a subset of health information, including demographic information collected from an individual, and:

    a. Is created or received by a health care provider, health plan, employer or health care clearinghouse; and

    b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

        1) That identifies the individual; or,

        2) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

16. **Payment:** Has the meaning given such term in 45 C.F.R. §164.501

17. **Personal Health Record (PHR):** An electronic record of PHR identifiable health information (as defined in section 42 U.S.C. § 17921(11) on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.

18. **Personal Representative**: A person legally authorized to make health care decisions on a Member's behalf or to act for a deceased Member or the estate. The Privacy Rule permits an exception should Nivano have a reasonable belief that the personal

representative may be abusing or neglecting the Member, or that treating the person as the personal representative could otherwise endanger the Member.

19. **PHI: Identifiable Health Information:** Individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information that is provided by or on behalf of the individual; and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
20. **Privacy:** Relates to an individual's desire to control access to their personal information.
21. **Protected Health Information (PHI):** All individually identifiable health information, whether oral or recorded in any form, that relates to the physical or mental health of a Member, the provision of health care to that Member, or the payment for the provision of health care services to an individual (45 C.F.R. § 160.103).
    a. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and, employment records held by a Covered Entity in its role as employer.
22. **Security:** Security, or security measures, encompasses all of the administrative, physical and technical safeguards in an information system (45 C.F.R. § 164.304). It relates to the extent to which information can be stored and provided with access limited to those who are authorized and have a legitimate need to use/disclose such information.

E. PROCEDURE

1. Nivano will use HIPAA definitions, as found in 45 C.F.R. §160.103, 164.402 and 164.501.
    a. Any modifications from the Department of Health and Human Services (DHHS) to the existing definitions will be incorporated into new Nivano policy creation; any applicable existing Nivano policy will be edited/ revised accordingly.
2. Nivano will use the definitions in 45 C.F.R.§1640.202 in general use and in specific reference to determining if HIPAA preempts State Law.

F. USES AND DISCLOSURES

1. **Basic Principle for Use and Disclosure**: Nivano may not use or disclose PHI, except either: (1) as the Privacy Rule permits or requires; or (2) as the Member who is the subject of the information (or the Member's personal representative) authorizes in writing.
2. **Required Disclosures**: Nivano must disclose PHI in only two (2) situations: (a) to Members (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and, (b) to a contracted government agency when it is undertaking a healthcare compliance investigation or review or enforcement action.
3. **Permitted Uses and Disclosures:** Nivano is permitted, but not required, to use and disclose PHI, without a Member's authorization, for the following purposes or situations: (1) To the Member, with limited exceptions; (2) Treatment, Payment and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Limited Data Set for the purposes of research, public health or health care operations. Nivano may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

4. **Marketing:** With the exception of designated marketing activities that may be conducted without Member authorization according to 45 C.F.R.§164.508 (a) (3). it is the policy of Nivano to obtain the Member's authorization prior to using or disclosing PHI for marketing purposes, in compliance with HIPAA regulations, specifically 45 CFR §164.508 (a);
5. **Minimum Necessary:** Nivano will make all reasonable efforts to use, disclose and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure or request. The minimum necessary requirement does not apply in any of the following circumstances:
    a. Disclosure to or a request by a health care provider for treatment;
    b. Disclosure to a Member who is the subject of the information, or the Member's personal representative;
    c. Use or disclosure made pursuant to an authorization;
    d. Disclosure to a contracted government agency for healthcare related complaint investigation, compliance review or enforcement;
    e. Use or disclosure that is required by law; or,
    f. Use or disclosure required for compliance with the applicable requirements of HIPAA Administrative. Data Standards and Related Requirements (45 C.F.R. Subtitle A, Subchapter C).
6. **Accounting of Disclosures of PHI:** Upon Member request, it is the policy of Nivano to provide Members with an accounting of PHI disclosures made by Nivano within the last six (6) years (or shorter period of time if a shorter period is requested) prior to the date on which the accounting is requested.

G. PRIVACY PRACTICES NOTICES

In accordance with HIPAA 45 CFR §164.520, Nivano provides the "Notice of Privacy Practice" to each new Member as follows:

1. At enrollment and annually thereafter;
2. Within 60 days of a material change to the uses or disclosures, the Member's rights, Nivano's legal duties, or other material privacy practices stated in the Notice; and,
3. Upon request by any person including Nivano Members.
4. The Nivano Member Handbook details the plan's security and privacy practices and refers Members to Member Services and/or the Nivano Internet website for further information.

H. ACCESS

It is the policy of Nivano to allow Members or their legal representative to inspect and receive a copy of their PHI within the Nivano *designated record set* upon request, with some exceptions. Members, or their legal representatives, will be requested to submit their request in writing and to submit proof of identity for the release. The "designated record set" is a group of records maintained by Nivano that are used to make decisions about Member

enrollment; provider payments; claims adjudication; and, case or medical management systems.

1. The Privacy Rule except from the right of access the following PHI (45 C.F.R. §164.524):
    a. Psychotherapy notes maintained separate from other mental health records;
    b. Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative actions or proceedings;
    c. Laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access; or,
    d. Information held by certain research laboratories.
2. Nivano may deny access to a Member or their representative in certain specified situations, such as when a health care professional believes that access could cause harm to the Member or another. In such cases, the Member or their authorized representative are given the right to have such denials reviewed by a licensed health care professional. Nivano will provide or deny access in accordance with the reviewing official's determination.

I. AMENDMENT:

Nivano Members have a right to amend their PHI in a designated record set when that information is inaccurate or incomplete (45 C.F.R., § 164.526). To amend their PHI, the member can mail in a written request to Nivano Physicians at PO Box 255568, Sacramento, CA 95865 with proper documentation included the reason to support the requested amendment. Nivano will act on the individual's request for amendment within 60 days upon receipt of request. If an amendment is granted in whole or in part, Nivano must:

1. Amend the information or the record that is the subject of the request;
2. Notify the Member that the amendment has been accepted; and,
3. Notify relevant persons, providers, business associates or organizations identified by either the Member or Nivano, of the amendment.

Nivano may deny an amendment based on the following instances:

1. Information requested to be amended was not created by the provider
2. Information requested to be amended is not part of the designated record set;
3. Information requested to be amended is not information that the Member has a right to access; or,
4. Information requested to be amended is accurate and complete.

If the request is denied, Nivano will provide the Member with the written basis for the denial and inform the Member of their right to submit a statement of disagreement which shall be filed, and subsequently released with, the record; and, a description of how the Member can commence a complaint to Nivano or to the Secretary of DHHS.

Nivano will amend PHI in its designated record set upon receipt of notice to amend from another covered entity.

J. RESTRICTION REQUESTS

In the case that a Member requests under 45 C.F.R. § 164.522 (a)(1)(i)(A), that Nivano restrict the disclosure of his/her PHI, notwithstanding paragraph (a)(1)(ii) of such section, Nivano must comply with the requested restriction if:

1. Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and,
2. The PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

   Members have the right to request that Nivano restrict use or disclosure of PHI to notify family members or others about the Member's general condition, location or death.

   Nivano will not agree to the restriction or denial of PHI as requested by the Member if Nivano determines that the information being restricted would impede treatment for the Member being served

K. CONFIDENTIAL COMMUNICATIONS

Nivano permits Members to request an alternative means or location for receiving communications of PHI by means other than those that Nivano typically employs.

Nivano will accommodate reasonable requests if the Member indicates that the disclosure of all or part of the PHI could endanger the Member. Nivano will not question the Member's statement of endangerment

L. ADMINISTRATIVE REQUIREMENTS

1. **Privacy Policies and Procedures**: Nivano has developed and implemented policies and procedures that are consistent with The Privacy Rule.
2. **Privacy Personnel**: Nivano has designated the **Compliance Officer** as their privacy official responsible for developing and implementing its privacy policies and procedures to ensure confidentiality.
3. Privacy policies and procedures are reviewed annually and revised as changes in laws, regulations, and/or the delegate's policies are published.
4. **Compliance Department:** Nivano has designated its Compliance Department as the office responsible for receiving HIPAA related complaints and providing Members and other individuals with information on Nivano HIPAA practices.
5. **Team Member Training**: Training requires that all Nivano Team Members, including management, Providers and Directors demonstrate awareness and understanding of HIPAA Privacy and Security standards, as well as Privacy requirements under the HITECH Act and ARRA. Additionally, business associates, first tier and downstream entities and vendors who have access to Member PHI must document that their workforce members have been trained on these standards.
   a. Nivano provides training for all Team Members on its privacy and security policies and procedures, as necessary and appropriate for them to carry out their functions and report their privacy concerns.

b. The Nivano "New Hire Orientation" manual is provided to every newly hired Team Member.

c. Newly hired Nivano Team Members are required to sign a, "Protected Health Information (PHI) Confidentiality Statement" at the time of their Nivano orientation process.

d. Within 90 days of hire, or prior to exposure of PHI, whichever is sooner, Nivano Team Members are required to attend compliance training and to pass a post training test by a score of not less than **85%**. On an annual basis after hire, each Team Member is required to attend compliance training and to pass a post training test by a score of not less than **85%**.

e. Training for Nivano Team Members is provided when material changes have been made to the privacy and security procedures. The training is provided on the changes within a reasonable period of time following approval by the Compliance Officer and the Compliance Committee.

f. The availability of a **Compliance Hotline** to accept anonymous privacy and/or security complaints/concerns regarding HIPAA non-compliance is included in all training sessions as well as appearing on the internal website. Nivano has a zero tolerance policy for retaliatory action against Team Members who report HIPAA concerns.

g. Other training materials for Team Members include, but are not limited to, periodic security updates and privacy and security reminders.

6. Business Associate, First Tier and Downstream Entities and Vendor Training: Nivano provides HIPAA learning experiences including, but not limited to:

    a. Nivano University, which provides a formal training program that includes HIPAA content.

    b. Mailings and publications containing confidentiality reminders.

7. **Provider Training**: Providers are notified of on-site training opportunities available to them by request. Additionally, reported breaches of information by a provider result in letter to the provider offering on-site training for them and/ or their staff members.

8. **Mitigation:** Nivano shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of PHI by its Team Members or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

9. **Data Safeguards:** Nivano maintains administrative, technical and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit incidental use and disclosure. Policies and Procedures have been developed and implemented. However, due to the rise in unauthorized disclosures of protected patient medical records, confidentiality requirements were enhanced by state laws Assembly Bill 211 and Senate Bill 541, effective 1/1/09, with certain provisions amended by Assembly Bill 1755, effective 1/1/15. The bills make Providers accountable for unauthorized access to medical information, not just for unlawful use or disclosure. Every healthcare entity must implement appropriate administrative, technical, and physical safeguards to protect the privacy

of a patient's medical record information and safeguard it from unauthorized access or unlawful access, use, or disclosure. Administrative fines for violations range from $25,000 to $250,000.

a. Nivano utilizes a document cross shredding service and there are securely locked shredder bins in each business area to hold confidential documents prior to shredding.

b. Hard copy documents containing PHI are secured under lock and key during non-business hours; and all Team Members have been provided with "PHI Protectors" to be placed over any and all confidential documents that are in process at their desks.

c. Procedures are in place to ensure faxes containing PHI are not left unattended and fax machines are in secure areas.

d. Procedures are in place for mailing PHI only by secure methods. Disks and transportable media sent through the mail are encrypted.

e. Nivano has a mechanism in place to encrypt and decrypt ePHI.

f. The Nivano Information Technology Department has termination procedures in place for terminating access to PHI/ePHI when the employment of a workforce member or contractor ends or access to ePHI is inappropriate.

g. The Nivano Information Technology Department has policies and procedures in place for electronic security from unauthorized disclosure, i.e., passwords; screen time-outs; secure E-Mail; etc. Team Member responsibilities for electronic security are included in compliance training for Team Members.

h. The Nivano Information Technology Department has implemented technical safeguards to protect PHI. **They are detailed in IT Policies and Procedures**.

i. Nivano protects the privacy of individual Member PHI by de-identifying PHI when released for purposes other than treatment, payment or healthcare operations; for use without the Member's authorization; and, for purposes other than those legally required under HIPAA to protect public safety.

j. The Nivano Team Member Handbook addresses the policy for verbal PHI, including Team Member discussion outside the Nivano offices.

k. Nivano has implemented a policy that addresses verifying the identity of the individual requesting PHI prior to release of the information. By administering this policy, Team Members put forth their best efforts to send PHI, in any format, to the appropriate requestor.

l. The Facilities Department has implemented physical safeguards for PHI including, but not limited to, controlled secure access to all areas of the buildings as detailed in their Policies and Procedures including secure access to IPA including assigned keyfob entry system for staff and front desk unlock and sign in sheets for approved visitors.

m. Nivano educates its Team Members on the importance of privacy laws and the policy on privacy of medical information.

n. Team Members are made aware that appropriate, documented action will be taken should unauthorized access occur; and, any incident of unauthorized access will be

reported to the Appropriate entity and to the affected patient within fifteen (15) days after detection of the breach

9. **Compliance**

   a. The **Compliance Department** conducts monthly in-house, random departmental HIPAA walk throughs to assess Team Member compliance with the Nivano PHI privacy policy. If the walk throughs warrant further action, the Compliance Department will increase the number of walk throughs until scoring is adequate.

   b. An annual risk analysis is performed in coordination with the Compliance and IT Department. The annual risk analysis results are stored and reviewed annually to ensure improvement and adequacy.

   c. Nivano requires that business associates who may be recipients of PHI must agree, in writing, to certain mandatory contract provisions regarding the use and disclosure of PHI.

   d. Nivano monitors contracted providers and business associates for compliance with HIPAA regulations prior to contracting and annually thereafter.

   e. Measures are taken by the Compliance department upon notification of any HIPAA violations. The remedial actions for any staff, contractors, or others affiliated can include write ups, probation, termination of contract, and more.

10. **Notification of Privacy Breach**: Nivano maintains and implements policies and procedures for providing notification of suspected and/or actual privacy breaches for all lines of business to the appropriate regulatory agencies. The Nivano **Compliance Department** investigates such breaches or unauthorized uses or disclosures of PHI

11. **Complaints/HIPAA Non-Compliance**: Nivano has a policy and procedure in place for Members, Team Members, Business Associates or other individuals to submit complaints and/or incidents of non-compliance with HIPAA requirements to the plan and/or to the Secretary of DHHS.

12. **Retaliation and Waiver:** Nivano does not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by DHHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. Nivano does not require a Member to waive any right under the Privacy Rule as a condition for obtaining treatment, payment and enrollment or benefits eligibility.

13. **Documentation and Record Retention**: Nivano maintains archived manuals containing privacy policies and procedures, privacy practice notices, disposition of complaints and other actions, activities, and designations that the Privacy Rule requires for a period of ten (10) years.

14. **Medical Identity Theft:** Nivano includes an explanation of this fast-growing type of crime in HIPAA Team Member training programs and educates Team Members relative to ways in which to identify the types of medical identity theft and the ways in which they can safeguard confidential information.

M. REPORTING UNAUTHORIZED ACCESS OR DISCLOSURE

Nivano only provide the following required notifications if the breach involved unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

1. **Breaches of Unsecured PHI, Affecting Fewer than five hundred (500) Individuals**
   a. For breaches that affect fewer than five hundred (500) individuals, Nivano must provide the Secretary of the Department of Health and Human Services (DHHS) with notice annually. All notifications of breaches occurring in a calendar year must be submitted within sixty (60) days of the end of the calendar year in which the breaches occurred. This notice must be submitted electronically by following the link below and completing all information required on the breach notification form. A separate form must be completed for every breach that has occurred during the calendar year. Link to Form: http://ocrnotifications.hhs.gov/.

2. **Breaches of Unsecured PHI, Affecting five hundred (500) or More Individuals:**
   a. If a breach affects five hundred (500) or more individuals, Nivano must provide the Secretary of DHHS with notice of the breach without unreasonable delay and in no case later than sixty (60) days from discovery of the breach. This notice must be Submitted electronically by following the link below and completing all link information required on the breach notification form.
   Link to Form: http://ocrnotifications.hhs.gov/

3. All security breaches that require a security breach notification to more than five hundred (500) California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Office of the Attorney General. http://oag.ca.gov/ecrime/databreach/reporting.
   a. In addition to notifying the affected Members, Nivano is required to provide notice to prominent media outlets serving the State or jurisdiction. Nivano will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and must include the same information required for the individual notice.

4. **Submission of Additional Breach Information to DHHS**
   a. If a breach notification form has been submitted to the Secretary and additional information is discovered, Nivano may submit an additional form, checking the appropriate box to signal that it is an updated submission. If, at the time of submission of the form, it is unclear how many individuals are affected by a breach. Nivano provides an estimate of the number of individuals affected. As this information becomes available, an additional breach report may be submitted as an addendum to the initial report.

5. **Reporting breaches to the Department of Health Care Services (DHCS)**

a. Nivano must also notify DHCS when a breach occurs that affects a Medi-Cal Member. Notification is provided to the DHCS Privacy Office, Information Security Office and to the Contract Manager within the following timelines:

1) By telephone, e-mail or fax within twenty-four (24) hours of discovery if PHI was or suspected to have been acquired by an unauthorized person.

2) After sending initial notice, Nivano will have seventy-two (72) hours from the date of discovery to provide DHCS with an initial Privacy Incident Report (PIR). Within ten (10) calendar days of discovery of the breach a final, completed PIR will be submitted to DHCS, unless an exception has been obtained from DHCS for additional time needed to complete investigation.

6. **Member Breach Notifications**

a. The Nivano Member(s) whose PHI has been breached must be notified in writing of the breach in accordance with CMS and DHHS requirements. Nivano is required to also notify the affected Member(s) in written form and must be provided without reasonable delay and in no case later than sixty (60) days following the discovery of a breach. This notification must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected Members should take to protect themselves from potential harm, a brief description of what Nivano is doing to investigate the breach, mitigate the harm and prevent further breaches, as well as Nivano contact information.

7. Nivano Internal Breach Notification

a. The Nivano Compliance Officer must be notified of any and all unauthorized breaches within the regulatory timeline requirements.

8. Reporting Breach to Contracted Health Plans

a. Breach will also be communicated to Nivano contracted Health Plans within a sixty (60) day time frame following the discovery of a breach. This notification must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach and a brief description of what Nivano is doing to investigate the breach, mitigate the harm and prevent further breaches.

By Mail to: Compliance Officer
Nivano Physicians, Inc.
1420 River Park Dr. Suite 200
Sacramento, CA 95815
By E-Mail to: Compliance@nivanophysicians.com

By Compliance Hotline: 916-407-2000 (Ext. 2509)