



## **PRIVACY AND SECURITY GUIDELINES**

**Concerning Compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") (jointly, "HIPAA"), Applicable Federal and State Laws, Regulations Promulgated Under These Laws (Collectively, "Privacy Laws") and Applicable Contracts (e.g., Business Associate Agreements)**

**River City Medical Group, Inc. dba Vivant Health - 2024**

**PRIVACY AND SECURITY GUIDELINES**

**Table of Contents**

1.	General .....	1
<b>Privacy Officer and Security Officer Responsibilities</b>		
3.	General .....	5
4.	Assessing/Granting Workforce Access to PHI.....	7
5.	Training.....	8
6.	Electronic Monitoring.....	8
7.	Enforcing Vivant Health Policies .....	9
8.	Visitors.....	10
9.	Off-Site Storage of PHI.....	10
10.	Servers.....	10
11.	Malicious Software Protection and Firewalls .....	10
12.	Data Access in Systems.....	11
13.	Remote Access.....	12
14.	Emergency System Access.....	13
<b>Workforce Responsibilities</b>		
15.	General .....	13
16.	Use of Electronic Portable Devices .....	14
17.	Workspace Security .....	16
18.	Transmission of PHI Via Email .....	17
19.	Transmission of PHI Via Facsimile (“Fax”) .....	17
20.	Disclosing PHI Via Telephone .....	18
21.	Copy Machines and Copying Services.....	19

## **PRIVACY AND SECURITY GUIDELINES**

### **Access to and Disclosure of PHI to Persons and Entities Acting on Vivant’s Behalf or Performing Services Under Contract with Vivant**

22.	Providers, Vendors, Business Associates, and Others Not Part of Workforce .....	19
-----	---	----

### **Member Rights and Notice of Privacy Practices**

23.	Member Rights .....	20
24.	Notice of Privacy Practices .....	21
25.	Member Access and Copies.....	21
26.	When Members Request That Their PHI Be Sent to Third Parties .....	25
27.	When No Written Member Authorization is Required Prior to Disclosures to Third Parties .....	26
28.	Special Considerations Regarding Psychotherapy/Mental Health PHI Disclosures to Members .....	27
29.	Special Considerations Regarding Psychotherapy/Mental Health PHI Disclosures to Third Parties .....	28
30.	Special Considerations Regarding Minors’ PHI Disclosures and Document Retention .....	30
31.	Authorization Requirements Prior to Disclosures to Third Parties.....	31

### **Limits on Access, Use and Disclosure of PHI**

32.	Marketing and Fundraising Activities and Other Uses or Disclosures Where Pre-Approval by Privacy Officer is Required .....	33
33.	Minimum Necessary Standard .....	34
34.	Requests for Restrictions on Uses and Disclosures .....	35
35.	Special Restrictions on Certain Types of Health Information: HIV, Substance Abuse, and Genetics .....	35

**PRIVACY AND SECURITY GUIDELINES**

**Documenting Disclosures and Accounting**

36. Documenting Disclosures .....37

**Requests for Modifications and/or Amendments to PHI**

37. Modifications and/or Amendments to Medical and Billing Records.....38

**Disposal of PHI**

38. Data Sanitization and Destruction .....41

**Record Retention**

39. Record Retention.....41

**Reports and Complaints**

40. Reports .....42

41. Complaints.....43

42. No Intimidation or Retaliation.....44

43. Reporting Security Incidents and/or Breaches to Third Parties 44

**Risk Assessment and Risk Logs**

44. Risk Assessment and Risk Logs

**Foreign Corrupt Practices Act (FCPA)**

45. Foreign Corrupt Practices Act

## **PRIVACY AND SECURITY GUIDELINES**

### **PRIVACY AND SECURITY POLICIES**

River City Medical Group, Inc. dba Vivant Health, a California professional corporation (“Vivant”) will protect the privacy and security of identifiable patient health information as required by the Health Insurance Portability and Accountability Act (“HIPAA”) and Subtitle D of the Health Information Technology for Economic and Clinical Health Act (“HITECH”), their implementing regulations and equivalent state privacy laws, and the regulations promulgated under these laws (collectively, “Privacy Laws”) as described in this Privacy and Security Guidelines document (the “Guidelines”) and in Vivant’s other policies and Notice of Privacy Practices (collectively, “Vivant Policies”)

### **PRIVACY AND SECURITY PROCEDURES**

#### **1. General**

1.1 Vivant Policies are, and at all times will be, based upon the risk assessments performed by Vivant, and upon applicable Privacy Laws.

1.2 Vivant will continue to conduct risk assessments and monitor compliance with applicable Privacy Laws as required to protect the confidentiality, integrity, and availability of PHI (as defined below).

1.3 Vivant’s Executive Team - including its Chief Executive Officer, Chief Medical Officer, Chief Operating Officer, Chief Legal Officer/General Counsel, Chief Technology Officer, Privacy Officer, and Security Officer - will timely approve, adopt, and implement Vivant Policies, as well as any modifications as may be necessitated by Privacy Laws.

1.4 Vivant will not use or disclose PHI in a manner inconsistent with Vivant Policies, Vivant’s Notice of Privacy Practices (“NPP”), or applicable Privacy Laws.

#### **2. Definitions**

2.1 Capitalized terms in Vivant Policies, and any subsequent policies adopted by Vivant related to applicable Privacy Laws, have the definitions given them under HIPAA.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

2.2 **Health Information/ Medical Information.** Information that is created or received by Vivant or another health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, whether oral or recorded in any form or medium, and that relates to the past, present or future physical or mental health or condition of an individual, including payment for the provision of health care to an individual.

2.3 **Individually Identifiable Health Information.** Health information that identifies an individual or can be reasonably used in combination with other information to identify an individual.

2.4 **Protected Health Information (“PHI”).** PHI means oral, written, or electronic information that:

- (a) is created or received by a health care provider, health plan, employer, health care clearinghouse, or organizations that contract and provide services to health care providers; 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
  - (i) that identifies the individual; or
  - (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

2.5 **ePHI.** Protected Health Information that is transmitted or maintained in electronic media. Hereafter, the term “PHI” includes ePHI unless otherwise noted.

2.6 **Electronic Health Records (“EHR”).** Electronic versions of a member’s medical records, which may include medical history, notes, and other information about a member’s health including symptoms, diagnoses, medications, lab results, vital signs, immunizations, and reports from diagnostic tests such as x-rays.

2.7 **Business Associate.** A person or entity that creates, receives, maintains, or transmits PHI or performs a PHI-related service or delegated HIPAA obligation, on behalf or as an agent of a Covered Entity or another Business Associate, and that requires access on a routine basis to such PHI or has a persistent opportunity to access PHI without regard to whether it randomly, infrequently, or ever views the PHI.

2.8 **Covered Entity.** A provider of health care services or supplies, as defined in 42 U.S.C. §1395x(s) & (u), an individual or group health insurance plan (including most employer plans) that provides or pays the cost of health care, and a health care clearinghouse.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

2.9 **Business Associate Agreement.** A contract between the Covered Entity and Business Associate to ensure that Business Associate(s) will appropriately safeguard PHI by, among other things, obtaining satisfactory assurances that the Business Associate will use the information only for the purposes for which it was engaged by the Covered Entity, will safeguard the information from misuse, and will help the Covered Entity comply with certain aspects of Privacy Laws.

2.10 **Workforce Members or Workforce.** Vivant's officers, executives, directors, employees, volunteers, trainees, and other personnel, including independent contractors performing work for or on behalf of Vivant that involves PHI and/or whose conduct, in the performance of work for Vivant, is under the direct control of Vivant, whether or not they are paid by Vivant, and regardless of their job classifications defined below or otherwise, and including Privacy Officer and Security Officer.

2.11 **Workspace.** Any physical space where Workforce Members perform their job duties and/or where Vivant's information systems are housed or located.

2.12 **Workstation.** Any station within the Workspace where the Workforce may physically and/or electronically access Vivant and provider systems including, but not limited to, PHI, EHR, and onsite and offsite backup systems.

2.13 **Electronic Portable Device.** Any portable device made available to, or otherwise owned by, Workforce Members, as defined below, that can be used to transmit or store ePHI, including, but not limited to, laptops, devices, compact disks, thumb drives, other hard drives, and PDAs.

2.14 **Vivant-Provided Device.** Any device, including desktop or laptop computers, provided to Workforce Members by Vivant for work-related purposes (e.g., when a Workforce Member is engaging in Vivant business or otherwise performing an activity for the benefit of Vivant and is authorized to perform such task/activity by Vivant as part of their job description), including Electronic Portable Devices.

2.15 **Personal Devices.** Devices owned by or personal to a Workforce Member and not provided by Vivant.

2.16 **Security Incident.** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 CFR 164.304. "Access" as used in defining a Breach does not have the same meaning as "access" as used in defining a Security Incident. In identifying a Security Incident, "access" means "the ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource." 45 CFR 164.304, Subpart C - Security Standards for the Protection of Electronic PHI ("(This definition applies to "access" as used in this subpart [C], not as used in subparts D or E of this part).")

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

2.17 **Unsecure.** In connection with Breach, PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through one or more of the following methods or such other method approved by the Secretary:

- (a) Encryption as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key,” including by processes established by the National Institute of Standards and Technology (NIST), where the confidential process or key that might enable decryption has not been breached;
- (b) Destruction of the media on which the PHI is stored or recorded using a method below, or such other method approved by the Secretary:
  - (i) Shredding or similar method such that the PHI cannot be read or otherwise reconstructed, but not redaction alone;
  - (ii) Electronic clearing, purging, destroying, or deleting consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

2.18 **Compromise.** In connection with unauthorized access to PHI, Vivant is not able to demonstrate that there is a low probability that the privacy of the PHI is threatened by conducting a risk assessment.

2.19 **Breach.** The unauthorized acquisition, access, use, or disclosure of Unsecured, unencrypted PHI that Compromises the security or privacy of such information. The following are excluded from this definition and do not constitute a Breach:

- (a) an unintentional acquisition, access, or use of PHI by a Workforce Member or other authorized person when such acquisition, access or use was made in good faith, within the scope of authority, and does not result in further use or disclosure in a manner not permitted by Privacy Laws;
- (b) an inadvertent disclosure by a person authorized to access PHI if the PHI is not further used or disclosed in a manner not permitted by Privacy Laws;
- (c) a disclosure to an unauthorized person who would not reasonably be able to retain the disclosed information; or
- (d) the unauthorized acquisition, access, use, or disclosure of encrypted PHI or de-identified PHI, as defined under Privacy Laws.



## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

### **Privacy Officer and Security Officer Responsibilities**

#### **3. General**

3.1 Privacy Officer and Security Officer (collectively, “Officers” or “Officer” for either or each of them) will generally have duties as described below, as set forth in Vivant Policies, and as may otherwise be directed by Vivant.

3.2 In general, Vivant’s Privacy Officer will be the primary contact person responsible for overseeing all ongoing activities including monitoring, enforcing, assessing, modifying and/or amending Vivant Policies, including HIPAA policies and procedures, addressing any questions, concerns, and/or complaints from Members (the capitalized term “Member” throughout Vivant Policies will include the patient-member and/or the patient-member’s authorized representative, while “member” refers to only the patient-member) and Workforce regarding Vivant Policies, in accordance with applicable Privacy Laws including, but not limited to, enforcing policies, procedures, and processes as appropriate to prevent and/or mitigate the risk of violation of HIPAA’s “Privacy Rule,” 45 C.F.R. Parts 160 and 164, as well as any other duties as directed by Vivant and outlined below.

3.3 In general, Vivant’s Security Officer will be the primary contact person responsible for monitoring, enforcing, assessing, modifying, and/or amending all information security policies, procedures and technical systems in order to maintain the confidentiality, integrity, and availability or loss of PHI on Vivant’s information technology systems including, but not limited to, developing, implementing, monitoring and enforcing policies and procedures to comply with HIPAA’s “Security Rule,” 45 C.F.R. Parts 160, 162 and 164 and specifically to prevent, detect, contain, mitigate and correct security violations and risks of unauthorized access, uses or disclosures of PHI and/or other violations of Vivant Policies, as well as address any questions, concerns, and/or technological issues relating to PHI regarding Vivant Policies, and perform any further duties as directed by Vivant and outlined below.

3.4 The Privacy Officer will maintain copies of all Vivant Policies and make them available to the Workforce and other appropriate personnel.

3.5 The Privacy Officer will ensure that all Workforce Members acknowledge that they have received and reviewed Vivant Policies and participated in trainings.

3.6 On an ongoing basis, the Privacy Officer will evaluate all Workspace’s physical security, including offsite Workspaces, and implement additional safeguards to ensure the continued confidentiality, integrity, and availability of PHI.

3.7 On an ongoing basis, the Security Officer will evaluate Vivant’s electronic systems and implement additional safeguards to ensure the continued confidentiality, integrity, and availability of PHI.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

3.8 On an ongoing basis, the Security Officer will inventory and document all Vivant hardware and laptops with corresponding asset tag(s), including the original location(s), movement location(s), movement date(s), and person who authorized the movement(s).

3.9 Security Officer, in consultation with Privacy Officer, will approve, in advance, any tangible changes that may impact the physical security of PHI, including changes to walls, doors, locks, or other physical attributes to ensure continued compliance with Vivant Policies and applicable Privacy Laws. The Security Officer will maintain a log of any such changes to the physical structure of the Workspace, including the date(s) of such changes, and who authorized the changes.

3.10 The Security Officer will ensure that proper software programs are installed on all devices used by Workforce Members who can or will access Vivant's email system from their devices.

3.11 Officers may delegate responsibilities under Vivant Policies, as consistent with applicable Privacy Laws, to an individual or individuals, including a Business Associate, to perform the Officer's duties when he/she is or will be absent from the Workspace or otherwise unavailable, when he/she does not have access to all information or systems necessary to perform his/her responsibilities and ensure the privacy and security of all PHI, and reasonably believes the delegated party has enhanced access to information, and/or is otherwise capable of performing the responsibilities required by Vivant Policies.

3.12 If an Officer leaves Vivant's employment, is absent from the Workspace when a need for performance of his/her duties exists, is expected to be absent for an extended period of time, and/or if Vivant determines that an Officer is unable for any reason to perform his/her duties pursuant to Vivant Policies, Vivant will promptly designate a new Officer.

### **4. Assessing/Granting Workforce Access to PHI**

4.1 Officers, in consultation with Human Resources, will ensure that all prospective and current Workforce Members who will or may require access to PHI to legitimately perform their job functions are subject to background checks prior to performing services for Vivant and, in any event, prior to accessing PHI, and will evaluate the results to assure that there is no indication that the prospective or current Workforce Member poses a substantial risk that PHI will be Compromised. Human Resources will maintain documentation related to each Workforce Member's background check.

4.2 All Workforce Members will review, sign, and acknowledge receipt of the Agreement to Maintain Confidential All Protected Health Information and Abide by All Vivant Privacy and Security Policies and Procedures ("Confidentiality Agreement"), and will do so annually. Human Resources will maintain the Confidentiality Agreement for ten (10) years following termination of Workforce Member's employment (or other cessation of Workforce Member's provision of services to or on behalf of Vivant).

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

4.3 Privacy Officer, Security Officer, Human Resources, IT and Department Leadership will work collaboratively to identify and authorize Workforce Members to obtain network and computer access based on their individual job functions and responsibility.

4.4 Privacy Officer and Security Officer will document those Workforce Members who require PHI access to perform their job functions and will ensure they are only accessing the minimum necessary for the Workforce Member to legitimately perform their job function(s). (For example, to comply with the “Minimum Necessary” standard, Vivant may limit the PHI access to a “Limited Data Set,” which includes dates of birth, death, and service, town or city, state, zip code, but does not include name, social security numbers, health plan numbers, etc.). *Social security numbers (SSN) are not displayed in Vivant’s core system (EZ-CAP).*

4.5 Officers will review, monitor and/or audit Workforce Member’s PHI access to ensure access management compliance with Vivant Policies and/or applicable Privacy Laws:

- (a) Security Officer will apply appropriate limitations and user authentication protocols;
- (b) Workforce Members will have access to systems and physical locations containing PHI only to the extent necessary to legitimately perform their individual job functions;
- (c) When a Workforce Member’s job functions change such that, they require either decreased or increased PHI access to legitimately perform their individual job functions, Officers will correspondingly adjust the Workforce Member’s PHI access;
- (d) When it becomes apparent that a Workforce Member will no longer need to access PHI, such as upon resignation or termination, Security Officer will be promptly notified by Human Resources (HR) or other appropriate Workforce Member to ensure that Workforce Member’s PHI access is deactivated upon the cessation of their legitimate business need.
- (e) This is monitored monthly. HR provides the Security Officer with a monthly list of the employees that are currently active. The Security Officer reviews the accounts to monitor with accounts are no longer active.

### 5. **Training**

5.1 Privacy Officer and Human Resources will ensure Workforce is provided training regarding Vivant Policies and applicable Privacy Laws:

- (a) Within three (3) business days of hire, and prior to being granted access to PHI in any event;
- (b) Upon applicable changes to Privacy Laws;
- (c) Upon implementing a material change to Vivant Policies;
- (d) When a Workforce Member’s duties or functions change, or are otherwise affected by changes to Vivant Policies;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (e) As determined appropriate by Officer(s), such as when a Security Incident occurs; and/or
- (f) In no event less than annually.

5.2 The Privacy Officer will maintain copies of all Vivant training materials for at least ten (10) years following each training exercise. Officers will continually evaluate, monitor, and update Vivant's Workforce training program and materials including alerting Workforce to potential and/or actual compromises of PHI, Security Incidents and/or Breaches.

5.3 Officers and Human Resources will ensure that Workforce Members provide written acknowledgment that they have received and reviewed Vivant Policies and participated in all required training. Human Resources will maintain these written acknowledgements for at least ten (10) years.

### **6. Electronic Monitoring**

6.1 At least quarterly, Security Officer will audit or direct an audit of Vivant's electronic systems to ensure compliance with Vivant Policies and applicable Privacy Laws using manual logs, electronic monitoring programs, and/or obtaining reasonable written assurances from vendors including, but not limited to, network-monitoring and vulnerability scanning and, at least annually, network penetration testing (collectively, "Security Audits").

6.2 At least monthly, Security Officer performs vulnerability scans using RapidFire Tools.

### **7. Enforcing Vivant Policies**

7.1 On an ongoing basis as appropriate to comply with Privacy Laws, Management, Human Resources and Officers will assess and monitor any potential and actual risks or vulnerabilities to the confidentiality, integrity, and availability of PHI ("Ongoing Assessments"), including:

- (a) monitoring, auditing, or evaluating Workforce operations, practices, uses, and disclosures of PHI to ensure Workforce's compliance with Vivant Policies;
- (b) ensuring that Vivant Policies are effective and work well with Vivant operations;
- (c) identifying Vivant processes that may result in the unauthorized access, use, or disclosure of PHI, Security Incidents, and/or Breaches;
- (d) identifying practices and processes to mitigate any actual or potential risks of the unauthorized access, use, or disclosure of PHI, or other Security Incidents, and/or Breaches;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (e) promptly responding to reports of actual or potential unauthorized disclosures of PHI, Security Incidents, and/or Breaches and complying with all applicable Privacy Laws; and
- (f) monitoring, auditing, or evaluating Business Associates' or other third-party vendor practices, uses or disclosures of PHI to ensure compliance with Vivant Policies and Privacy Laws.
- (g) conduct annual access management reviews for employees and quarterly reviews for privileged/administrative accounts

7.2 Officers will document all Ongoing Assessments and related activities in accordance with the document retention provisions of Vivant Policies.

7.3 In consultation with the Chief Legal Officer - General Counsel, Officer(s) will make any necessary modifications to Vivant Policies and notify Workforce Members and provide related training as appropriate.

7.4 In the event a Workforce Member violates Vivant Policies and/or applicable Privacy Laws, Officer(s), in consultation with Human Resources, will determine what sanctions should be imposed on the Workforce Member up to and including termination.

7.5 The Privacy Officer will ensure that Human Resources maintains records of any sanctions imposed upon Workforce Member(s) as a result of violations of Vivant Policies and/or applicable Privacy Laws.

### **8. Visitors**

8.1 Officers will implement protocols to ensure that all visitors to Workspace who do not have a legitimate business need to access PHI will not be granted access to PHI.

### **9. Off-Site Storage of PHI**

9.1 Vivant will enter into Business Associate Agreements, as required by applicable Privacy Laws, with respect to any PHI maintained by Business Associates in off-site storage facilities. Vivant will obtain reasonable assurances from Business Associate(s) that PHI will be kept physically secure and separate from any non-Vivant PHI, and that Business Associate(s) will notify Officer(s) prior to making any changes to the physical components of off-site storage facilities that could affect the privacy and security of PHI.

9.2 As with PHI maintained at Workspace, only those Workforce Members authorized by Officer(s) and having a legitimate business need will have access to off-site PHI.

### **10. Servers**

10.1 Security Officer will maintain a plan for the security of Vivant's servers, if any, which will include:

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (a) Ensuring that only authorized Workforce Members and Business Associate(s) are able to physically access the server room. Security Officer will accomplish this by, among other processes, authenticating server room access to only those individuals with a legitimate business need, and creating an electronic logging system that tracks all user access (including user id, day, and time); Security Officer will maintain this log for ten (10) years from date of entry;
- (b) Installing, and configuring the underlying operating system to ensure the confidentiality of PHI;
- (c) Securing, installing, and configuring server software; and
- (d) Maintaining the secure configuration through network penetration tests, applying appropriate patches and upgrades, security testing, log monitoring, and data and operating system file backups.

11. Vivant has a system which creates and logs tickets. Tickets cannot be deleted or modified in the system. The tickets are monitored daily to ensure all tickets are resolved. Malicious Software Protection and Firewalls

11.1 Officers will develop and implement a plan to ensure Vivant's system is protected from malicious software, including:

- (a) Workforce procedures;
- (b) Workforce training;
- (c) Vulnerability detection and mitigation;
- (d) Incident response;
- (e) Administrator privileges;
- (f) Application settings;
- (g) Full Disk Encryption (FDE) Software; and
- (h) Patch management.

11.2 Security Officer will ensure appropriate firewall protections and related safeguards are in place, including anti-virus software solutions with automatic updates scheduled at least daily, and periodically evaluate internal and external network traffic, including ePHI.

- (a) Vivant uses Malwarebytes Anti-Virus on all workstations. Malwarebytes constantly looks for malware and creates a ticket in the Vivant system when a threat is discovered. Malwarebytes also installs a browser extension that monitors web traffic for an extra layer of protection.

11.3 Security Officer will ensure appropriately configured personal firewall protections, Full Disk Encryption (FDE) software and related safeguards are installed on Electronic Portable Devices used for remote access, including anti-virus software solutions with automatic updates scheduled at least daily.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

11.4 The Security Officer will approve any changes to firewall and router settings, per our Security team's recommendation.

11.5 Security Officer uses WPA2 encryption to secure Wi-Fi networks.

11.6 Security Officer will implement continuous security incident monitoring enabled in accordance with security best practices and configured to allow detection and audit of all suspicious or abnormal activity (e.g., Intrusion Detection System/Intrusion Prevention System (IDS/IPS))

11.7 Vivant uses multiple tools like ZIX for email filtering & encryption, email threat protection and secure file transfer; Fortinet Firewall and Firewall Services to manager security services which stops ransomware, breaches, and data theft and finally a secure private VPN tunnel.

11.8 In a ransomware event, the Security Officer will ensure the following appropriate steps are taken:

- (a) Isolate affected systems
- (b) Secure backups
- (c) Disable maintenance tasks
- (d) Identify and investigate the initial device affected
- (e) Report to upper management, then decide whether to pay the ransom

### **12. Data Access in Systems.**

12.1 The Security Officer will approve any changes to Full Disk Encryption (FDE) software (e.g., Microsoft Bitlocker), per our Security team's recommendation.

12.2 The Security Officer will ensure that appropriate controls exist to protect the security of Vivant's internal network and systems.

12.3 Security Officer will ensure that where appropriate a warning banner is displayed stating the computer may only be used by Vivant authorized users who agree to maintain the confidentiality of data accessed, limit use of Vivant systems to authorized business purposes only, and permit Vivant to monitor and log access to systems and data, and that users must log off if they do not agree with these requirements.

12.4 Security Officer will implement a process whereby non-Vivant Workforce Members, such as providers, health plans, clearinghouses and others with legitimate business needs to access PHI on Vivant's web portal, are required to change their password at least every ninety (90) days.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

12.5 In consultation with Human Resources and Privacy Officer as appropriate, Security Officer will promptly deactivate any accounts that no longer have a legitimate business need to access Vivant's information system.

12.6 Workforce Members who can access ePHI will be authenticated using procedures established or approved by the Security Officer, which may include using a unique identifier that is not automatically populated on start-up (e.g., last name, first initial).

### 13. **Remote Access**

13.1 Remote access users will be authenticated using procedures established by the Security Officer and otherwise in compliance with Vivant Policies.

13.2 Workforce Member's access, entry, and modification of ePHI will be tracked using procedures established or approved by the Security Officer. Tracking will identify when ePHI is accessed, entered, modified, and by whom.

13.3 Security Officer will ensure that unique usernames and passwords are used to protect ePHI from unauthorized access and that Workforce may not disable them or attempt to use passwords that meet less stringent requirements than the following:

- (a) Passwords will be a minimum of eight (8) characters, and contain at least one uppercase letter, one lowercase letter, and one number or punctuation character. Passwords will exist for at least one (1) day, and will expire every ninety (90) days;
- (b) Passwords should be a non-dictionary word such as a phrase with no spaces and include a number or symbol, for example: Ucantgu3\$sthis!;
- (c) Passwords may not contain any part of a Workforce Member's name or username;
- (d) Passwords will be unique with each reset and previous passwords cannot be reused;
- (e) After ten (10) failed log-in attempts, the account will lock preventing access.
- (f) Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Vivant information
- (g) Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

13.4 Screen locks will not be disabled or altered.

- (a) Workstation screens will lock after fifteen (15) minutes of inactivity, unless a shorter timeframe is designated by Security Officer.



## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (b) With respect to Electronic Portable Devices with ePHI access, screens will lock after fifteen (15) minutes of inactivity as determined by Security Officer, or as otherwise set forth in this Policy.
- (c) Applications containing PHI will automatically terminate the session after fifteen (15) minutes of inactivity.

### **14. Emergency System Access**

14.1 Officer will ensure that a plan (“Contingency Plan”), is in place and functional at all times to protect the confidentiality, integrity, and availability of data on Vivant’s systems in the event of a disruption or interruption (“Emergency”) of the systems, including:

- (a) Data Backup, at minimum daily;
- (b) Emergency operations, including identification of who is to have emergency access to systems;
- (c) Data Recovery; and
- (d) System Recovery.

14.2 Officers will periodically evaluate the Contingency Plan, assess the critical functions of Vivant’s system in an Emergency, and make any necessary changes to further Vivant Policies and applicable Privacy Laws.

14.3 Officers will develop and/or promote all other safeguards and processes necessary to ensure the confidentiality, integrity and availability of PHI not otherwise addressed in Vivant Policies, and will ensure, to the extent feasible, the operation of mechanisms that corroborate ePHI has not been altered or destroyed in an unauthorized manner, such as error-correcting memory, magnetic disk storage, signal signatures, or check sum technology.

### **Workforce Responsibilities**

### **15. General**

15.1 Workforce Members will comply at all times with Vivant Policies and applicable Privacy Laws and will perform further duties as directed by Vivant and outlined below.

15.2 Workforce Members are encouraged to notify Officer(s) whenever they believe that Vivant Policies should be modified or amended to maintain compliance with applicable Privacy Laws.

15.3 Workforce Members will provide Officers and Human Resources with written acknowledgement of receipt and review of all Vivant Policies, prior to downloading Vivant’s company email software on their electronic mobile devices.

15.4 Workforce Members may not access personal email accounts while logged-on to Vivant’s Workstations.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

15.5 Absent approval from Vivant's Privacy Officer and/or Security Officer, Workforce Members may not access social media accounts (e.g., Facebook, Twitter) while logged-on to Vivant's Workstations.

### **16. Use of Electronic Portable Devices**

16.1 Vivant prohibits the use of Devices (referring to both Vivant-Provided Devices and Personal Devices) without proper authorization from Vivant, as set forth below.

16.2 Workforce Members are not prohibited from using Personal Devices during office hours but are prohibited from using them for work-related purposes and/or to transmit Vivant data absent authorization from Security Officer.

16.3 Workforce Members will obtain prior approval to use a Personal Device for work-related functions to ensure Personal Device(s) are approved to securely connect to Vivant's network and can be supported by Vivant's IT Department.

16.4 Workforce Members are prohibited from using cameras, audio or video-recording devices, video-camera phones, tape recorders or other recording devices, including cameras on mobile phones, on any Device to capture the images of Vivant data (including PHI), unless the activity is approved by the Privacy Officer, work-related and limited to the minimum amount necessary in accordance with Vivant Policies and Privacy Laws.

16.5 Vivant reserves the right to monitor all communications and records of Vivant-Provided Devices and to monitor all communications and records of Vivant's network including Personal Device activity. Workforce Members will have no expectation of privacy regarding such communications or records.

16.6 Security Officer will maintain an inventory of 1) Vivant-Provided Devices, 2) a list of authorized Vivant-Provided Device users, and 3) a list of Workforce Members authorized to use Personal Devices including the type of Personal Device (brand, model) and scope of authorized use ("Device Log").

16.7 Workforce Members will adhere to all federal, state, and local rules and regulations regarding the use of any Device while driving.

16.8 Workforce Members are encouraged to consider their surroundings and provide for or promote their safety and the safety of those around them while using a Device.

16.9 Vivant will provide IT support for Vivant-Provided Devices. Vivant may provide IT support for approved Personal Devices.

16.10 All Vivant-Provided Devices will require a username and password to access.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

16.11 Workforce Members must avoid writing down passwords and change passwords when requested by staff or if passwords are compromised.

16.12 Workforce Members are encouraged to use different passwords for different accounts.

16.13 Workforce Members may change their password when requested or if passwords are compromised. Workforce Members will contact the appropriate staff who oversee the devices.

16.14 The Security Officer will ensure that all Vivant-Provided Devices will lock when they are idle for fifteen (15) minutes. All Vivant-Provided Devices will also lock after ten (10) failed login attempts. All USB and disc drives are disabled. When a Vivant-Provided Device is locked following ten (10) failed login attempts, Workforce Member will notify the IT Department in order to regain access.

16.15 Workforce Members are prohibited from downloading and/or installing any applications or software programs on Vivant-Provided Devices that have not been approved in advance by the IT Department and Security Officer.

16.16 Workforce Members will not leave Devices unattended in unsecure environments and should take steps to avoid theft, such as keeping Devices from view if locked in a car or readily accessible in Vivant's Workspace.

16.17 Lost or stolen Devices that may have been used to transmit or store PHI will be reported to Officers without delay and in no event more than two (2) hours upon discovering a Device is lost or stolen.

16.18 Vivant reserves the right to disconnect or disable Devices used to access Vivant data without notification. Any such Device may be remotely wiped when 1) it is lost or stolen, 2) a Workforce Member is no longer authorized to access Vivant's data (such as upon employment termination), or 3) upon a Security Incident, Breach, or other circumstance that threatens Vivant's data.

16.19 Security Officer will ensure that all Vivant-Provided Devices are returned to Vivant upon Workforce Member no longer requiring access to Vivant data, or prior to appropriately transferring the Vivant-Provided Device to another Workforce Member with authorized PHI access. In the event the Vivant-Provided Device will no longer be used to access Vivant data, Security Officer will promptly disconnect the Vivant-Provided Device from Vivant's network. The Security Officer will ensure the Device Log is updated accordingly.

16.20 Security Officer will remotely or otherwise remove and permanently delete or destroy ("wipe") all Vivant data and any programming, software, or access ports from Personal Devices that have been used for work-related purposes, and thereafter will disconnect the

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

Personal Devices from Vivant's network upon Workforce Member no longer requiring access to Vivant data. The Security Officer will ensure the Device Log is updated accordingly.

16.21 Any circumstances identified by Workforce Members as potentially creating a risk to the security of Vivant's data (such as the abrupt or unplanned resignation of a Workforce Member and/or other termination situation identified as potentially creating a risk to the security of Vivant's data or systems) will be immediately reported to Security Officer and Privacy Officer to allow such Device(s) to be remotely wiped and promptly disconnected from Vivant's network.

### **17. Workspace Security**

To improve the security and confidentiality of company data, Vivant has adopted a Clean Desk Policy for workspaces. This policy reduces the risk of unauthorized access, loss, and damage to information during and outside of normal business hours or when workstations are left unattended.

17.1 Workstations will be kept secure to ensure ongoing compliance with Vivant Policies and Privacy Laws.

17.2 Workforce Members will:

- (a) Ensure that PHI is obstructed from view;
- (b) Utilize dedicated file space and locked cabinets for ongoing, legitimate paper PHI access;
- (c) Utilize secure/locked storage bin(s) to store paper PHI immediately upon the cessation of needing such PHI, continuing until its destruction;
- (d) Lock computer when leaving their workstation;
- (e) Immediately report any suspected or actual Breach or Security Incident to an Officer (as set forth in greater detail in Vivant's Compliance Plan).

17.3 Workforce, in collaboration with Officers, will assess whether PHI in or around Workstations can be visible to individuals who do not have a legitimate business need to access PHI, and will implement and maintain appropriate Physical Safeguards to limit visibility of PHI in Work Stations.

17.4 Vivant supplies dedicated file space and locked cabinets for paper PHI, including secure storage bins where PHI is stored prior to proper destruction. Access is provided only to those Workforce Members who have previously been identified by Privacy Officer, in consultation with Security Officer, as having a legitimate business need, and who have undergone required training with respect to Vivant Policies and applicable Privacy Laws.

17.5 The workplace is equipped with locks on its exterior doors, keypads, an alarm system, a visitor log-in system, locks on appropriate offices, and locks on Workstations and file cabinets containing PHI.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

17.6 When Workforce Members conclude their daily job functions, they will log-off and power down their Workstations and any Electronic Portable Devices that will remain in the Workspace upon conclusion of the workday.

### **18. Transmission of PHI Via Email**

18.1 Workforce Members may transmit PHI within Vivant's information system, which is encrypted and requires password authentication.

18.2 Workforce Members may not transmit PHI via email outside of Vivant's information system unless it is sent via a secure email software program, or sent through a health plan's secure email system, or the PHI is sent in an encrypted attachment and the password to open the attachment is sent by separate email to the intended recipient.

18.3 Workforce Members may not use non-Vivant e-mail accounts to transmit PHI.

18.4 Regarding emails transmitted to Vivant from outside systems, in consultation with the Security Officer, Workforce Members will confirm prior to transmission, to the extent possible, that the method of transmission will be secure. If the transmission has already occurred and a secure method was not used, the Workforce will request that in the future PHI sent via email be encrypted. If the sender refuses or a secure method is not available, Workforce will request that no further transmissions be made until a secure mode of transmission is used. The workforce will promptly report to the Privacy Officer and Security Officer all circumstances in which unsecured PHI is or was transmitted to Vivant.

### **19. Transmission of PHI Via Facsimile ("Fax")**

19.1 Workforce Members may transmit and/or receive PHI by Fax only when:

- (a) No other means exists to provide the requested data in a reasonable manner or time frame;
- (b) The fax machine is in a secure location;
- (c) Reasonable steps have been taken to ensure the fax transmission is sent to the appropriate destination, including prospective confirmation of the recipient's fax number;
- (d) For all transmissions, the following information will be included:
  - (i) the sender's name, address, and telephone number;
  - (ii) the recipient's name and fax number;
  - (iii) the date of the fax;
  - (iv) the number of pages transmitted.
  - (v) a statement similar to the following:
  - (vi) The documents accompanying this fax transmission contain confidential information, some or all of which may be protected

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

health information as defined by the Health Insurance Portability and Accountability Act of 1996. The information is intended only for the use of the individual(s) or entity named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or other action taken regarding the contents of this fax is strictly prohibited. If you have received this fax in error, please immediately notify us by telephone at the number above to arrange for destruction of the document(s). Thank you.

19.2 If a Workforce Member learns that a fax containing PHI has been misrouted, the Workforce Member will promptly contact the unintended recipient, request destruction of the document(s), and written confirmation of destruction. The Workforce Member will also take steps to correct the problem that caused the misdirection and provide written notice to the Privacy Officer that a misrouting has occurred. Each of these steps will be documented by the Workforce Member who sent the fax and provided it to the Privacy Officer, who will maintain the documentation in accordance with Vivant Policies.

19.3 Any PHI received via fax will be properly destroyed once Workforce Member has finished using the PHI for its intended, legitimate purpose.

### **20. Transmission of PHI Via Secure File Transfer Protocol (“SFTP”)**

20.1 Workforce Members that are approved to gain access, may transmit PHI within an Vivant or the Health Plan’s SFTP.

### **21. Disclosing PHI Via Telephone**

21.1 PHI should not be disclosed via text message including, without limitation: patient-member name, initials, street address, city, county, zip code, telephone and fax numbers, email address, social security number (or the last 4 digits), medical record number, health plan beneficiary number, account numbers, license number, dates associated with test measures, such as those derived from a laboratory report, face photographs and other images, and/or any other unique identifying number, characteristic, or code. If texting PHI becomes necessary and there is no reasonable alternative, Workforce Members will notify the Privacy and Security Officers and comply with their instructions in sending text messages.

21.2 PHI may be disclosed over the telephone using the same precautions as if in person. Workforce Members handling a call concerning PHI will make reasonable efforts to confirm the caller’s identity.

21.3 Where feasible, telephones that will be used to discuss PHI should be located in a private area, and conversations conducted in a quiet manner that ensures the confidentiality,

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

integrity, and availability of PHI to the extent possible, giving consideration to whether unauthorized individuals are nearby or the information is of a sensitive nature.

21.4 Before calling a Member, Workforce Members should ascertain which contact number may be used and where messages may be left (e.g., if the Member instructed that messages may be left on the Member's cellular number but not on the home number). When Workforce Members call a member, information about the member's medical condition will not be disclosed unless and until the Member satisfactorily identifies themselves as the Member. Messages left for Members should be limited to:

- (a) the name of the person for whom the message is being left;
- (b) a request that the person return the call;
- (c) the name of the Workforce Member for whom the person may ask when returning the call; and
- (d) the telephone number where the call may be returned.

Example: "Please have Mr. Smith call Vivant at [phone number], and ask for Mary."

### **22. Copy Machines and Copying Services**

22.1 PHI will not be left unattended on Vivant's copy machines.

22.2 PHI WILL NOT BE SENT OUT TO A COPYING SERVICE UNLESS VIVANT'S EXISTING COPYING ABILITIES CANNOT ACCOMMODATE THE JOB, IN WHICH CASE VIVANT WILL HAVE A BUSINESS ASSOCIATE AGREEMENT WITH THE COPYING SERVICE AND WILL ENSURE APPROPRIATE SAFEGUARDS ARE USED DURING THE TRANSPORT AND DELIVERY OF PHI TO AND FROM THE COPY SERVICE.

**Access to and Disclosure of PHI to Persons and Entities  
Acting on Vivant's Behalf or  
Performing Services Under Contract with Vivant**

### **23. Providers, Vendors, Business Associates, and Others Not Part of Workforce**

23.1 Except as provided below, the Workforce will not share PHI with vendors or other third parties who are not Vivant Workforce Members without first requiring the entity or individual to enter into a Business Associate Agreement ("BAA") with Vivant. Once the BAA has been signed, Vivant will retain the original for ten (10) years following termination of the BAA.

23.2 Vivant may allow entities performing services to, for, or on behalf of Vivant to access, use, maintain, transmit, and/or create PHI without Member authorization only if Vivant and such person or entity have entered a written BAA.

23.3 Workforce Members who become aware of persons or entities who propose to perform or are performing services to, for, or on behalf of Vivant who may have access to PHI

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

will determine, through Privacy Officer, whether such persons or entities have BAAs and/or confidentiality agreements with Vivant, and if such information cannot be determined, or if there is any question about the validity of such agreements, will receive the written approval of Privacy Officer before providing access to any PHI.

23.4 Persons and entities with access to Vivant’s Workspace or systems that may result in only incidental exposure to PHI and/or who are not acting on Vivant’s behalf will be asked to execute a confidentiality agreement with Vivant prior to providing services.

23.5 Security Officer and Privacy Officer will create and maintain an inventory of all existing service agreements and outside service providers where no BAA has been entered, and will determine whether a BAA and/or confidentiality agreement is required or prudent under the circumstances, and if so, will enter into a BAA with such persons or entities.

23.6 The Security Officer and Privacy Officer will inventory and maintain a log of all BAAs, Sub-Business Associate Agreements (“Sub-BAAs”), and confidentiality agreements entered into by Vivant.

### **Member Rights and Notice of Privacy Practices**

#### 24. **Member Rights**

24.1 Vivant will not require any member to waive rights to which they are entitled under Privacy Laws as a condition of receiving medical treatment or payment.

24.2 Vivant will not condition medical treatment on whether Member signs an authorization unless, in consultation with Privacy Officer, it is determined that:

- (a) The member is participating in research, the authorization is sought in connection with that research, and the authorization otherwise complies with Privacy Laws and federal laws governing human subject research;
- (b) Member has requested that an Vivant provider perform an examination or provide other treatment, for the express purpose of providing the member’s results to a third party.

#### 25. **Notice of Privacy Practices**

25.1 Vivant’s provision of Notice of Privacy Practices to Members:

- (a) A link to Vivant’s Notice of Privacy Practices (“NPP”) will be provided to Members in their welcome letter at the time of enrollment.
- (b) Vivant will ensure that the most current NPP is available and prominently displayed on its customer service web site, along with a notice that a paper



## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

copy is available and information about how Members may obtain such a copy.

- (c) Vivant will review its NPP at least every three (3) years and ensure not only that the most recent NPP is available through its web site, but also that the notice to Members of how they can obtain a copy is current and prominently displayed.

25.2 Vivant will promptly provide a paper copy of the NPP to any and all Members who request it. Vivant will make a good faith effort to document provisions of the NPP to Members, including the date and manner of transmission.

25.3 Vivant will promptly revise its NPP whenever there is a material change to its uses or disclosures, member's rights, legal duties, or other privacy practices stated in the NPP. Vivant will provide the revised NPP to all new Members at the time of enrollment but may elect not to send the revised NPP to those Members who received a prior version. Vivant will promptly post the revised NPP on its website. Except when required by law, a material change to any term of the NPP may not be implemented prior to the effective date of the NPP in which the material change is reflected.

25.4 Vivant will retain copies of all NPPs issued, documentation regarding provision of the NPP to Members, and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain written acknowledgment. This information will be kept for a minimum of ten (10) years from the date it was last effective.

25.5 Vivant staff reviews the NPP when processing and handling member requests.

### **26. Member Access and Copies**

26.1 Vivant recognizes that every Member has the right to review and/or obtain a copy of his/her PHI. Unless limited by Member, by virtue of the fact that the Member's PHI originated from another provider whose Designated Record Set does not include all of Member's requested records, or by applicable Privacy Laws, all medical records received and/or maintained by Vivant will be provided in response to valid requests, other than designated psychiatric records. (A "Designated Record Set" are those records used to make decisions about individuals, a provider's medical and billing records about individuals, or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. It does not include internal data analyses Vivant conducts related to claims, contracting, referrals, etc.)

26.2 Vivant requires that Member requests for PHI be in writing, which request will include information authenticating the member's identity, such as date of birth, gender, home address, telephone number, email address and, where applicable, power of attorney or other legal documentation.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

26.3 In response to Member requests for PHI, Workforce Members will verify that the information provided matches the identity of the requestor. Once the validity of the PHI request has been verified, Workforce Member will notify Privacy Officer of the request within two (2) business days. The notice will include any relevant information, including:

- (a) the scope of PHI requested;
- (b) by whom;
- (c) when;
- (d) to whom PHI should be sent;
- (e) the requested mode of transmission (e.g., mail, facsimile, ePHI);
- (f) the actual mode of transmission (i.e., if Member requests ePHI, RCMG will provide such ePHI in the requested format, or, if not readily producible as requested, in an alternative electronic format agreed to by Vivant and Member);
- (g) where PHI should be sent; and
- (h) any facts supporting an extension of time to respond, if necessary.

26.4 Only those Workforce Members who have been authorized by Privacy Officer and possess a demonstrated legitimate business need may fulfill Member requests for PHI, including authorizations to disclose PHI to third parties. Only the minimum amount of PHI necessary to meet the request and/or authorization may be used or disclosed.

26.5 An authorized Workforce Member and/or Privacy Officer will determine whether the request will be granted in full, in part, or denied, and/or whether Vivant is required to obtain an authorization from Member, pursuant to Vivant Policies and/or applicable Privacy Laws.

- (a) If an authorization is required, Vivant will provide an authorization form to Member.
  - (i) The completed, original authorization form will be provided to the Privacy Officer for review and a determination of whether to permit the requested use or disclosure. (“Use or disclosure” may only be for purposes related to the specific function being performed (e.g., facilitating payment));
  - (ii) The original authorization form will be maintained by Privacy Officer in a secure, locked file cabinet or a digital copy will be saved in the Compliance H Drive folder in accordance with Vivant Policies.

26.6 The following timeframe will apply to Member access and copies of PHI:

- (a) Vivant will permit the inspection within five (5) business days after receiving the written request;
- (b) Vivant will transmit copies within fifteen (15) business days after receiving the written request;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (c) If the request relates to an appeal regarding eligibility for a public benefit program (e.g., Medi-Cal), Vivant will transmit copies within thirty (30) business days after receiving the written request;
- (d) If Vivant determines that a summary of the member's medical record will be prepared in lieu of providing copies of the record, Vivant will transmit the summary within ten (10) business days after receiving the written request, except that if it is determined that additional time is needed (in the event the record is extraordinarily long or because the member was discharged from a health facility within the last ten (10) days), Vivant will have thirty (30) business days after receiving the written request to provide the summary and will notify the Member of this and the date when the summary will be provided. Vivant will notify Member in writing within thirty (30) days after receiving the written request of the reason for Vivant's delay and/or circumstances not reasonably within Vivant's control that caused the delay or need for an extension of time within which to respond to the request, and the date on which the information will be provided (to comply with federal law).

26.7 Unless Member requests otherwise, Vivant will mail the paper PHI to Member at the postal address on file with Vivant. If Member requests that PHI be transmitted in electronic format and the Member PHI is maintained in electronic format, then Vivant will provide the Member PHI in electronic format.

26.8 If the Privacy Officer determines that applicable Privacy Laws require denying PHI access, Privacy Officer will appoint a licensed health care professional not involved in the original decision to conduct the review.

26.9 Privacy Officer will notify Member in writing within five (5) business days after receiving the written request, including:

- (a) the basis for the denial;
- (b) subject to applicable Privacy Laws, a statement that Member may have the right to have an Vivant-appointed licensed health care professional review the denial;
- (c) the procedure by which Member may file a complaint with Vivant; and
- (d) the procedure by which Member may file a complaint with the Department of Health and Human Services.

26.10 If the requested PHI is not maintained by Vivant, Vivant will direct Member to the Business Associate, individual, or entity that maintains the PHI, if known.

26.11 The Privacy Officer will ensure that all documentation relating to Member PHI requests will be maintained for at least ten (10) years.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

26.12 If a member's request for a copy of PHI is approved or Vivant agrees to a summary or explanation of such information, Vivant may impose a reasonable fee as a condition of receiving PHI, provided that the fee includes only the cost of:

- (a) Copying, including the cost of supplies for, but not the labor associated with, copying the PHI requested, not to exceed \$0.25 cents per page or \$0.50 cents for records that are copied from microfilm or another similar medium;
- (b) Postage when the individual has requested the copy, summary, or explanation be mailed; and
- (c) Preparing an explanation or summary of the protected health information, if agreed to by the individual; unless Patient informs Vivant that they believe they are or may be the victim of medical identity theft or Patient is requesting copies to support an appeal regarding Medi-Cal/Medicaid eligibility, in which event Vivant will provide all relevant records free of charge. The Privacy Officer will determine the relevance of the Patient's records to the identity theft or eligibility appeal upon a reasonable review of the circumstances.

26.13 Vivant may charge reasonable costs for PHI provided to third parties, as set forth above.

26.14 If PHI is returned to Vivant as "undeliverable" by the USPS it will be cross-cut shredded, or otherwise destroyed utilizing a NIST-approved standard.

### **27. When Members Request That Their PHI Be Sent to Third Parties**

27.1 Prior to disclosing PHI, Workforce Member will verify Member's identity and confirm that the requested disclosure is appropriate under Vivant Policies and applicable Privacy Laws. If a Workforce Member has any questions or doubts as to the authenticity of Member and/or whether PHI should be disclosed, Workforce Member will promptly notify Privacy Officer.

27.2 Privacy Officer will review, on a case-by-case basis, all non-routine requests for PHI (that is, those requests not addressed in Vivant Policies), determine whether the requests are valid, and ensure that any related disclosures comply with Vivant Policies and applicable Privacy Laws.

27.3 Vivant will comply, without requiring Member to explain the reason for the request, with Member requests that Vivant communicate or send the PHI to a designated third-party recipient by alternative means or at alternative locations ("alternative communications requests"), but only if such request is reasonable. Reasonable means of communication may include transmissions via telephone (but not text), facsimile, e-mail, courier service, overnight express mail, etc. Reasonable alternative locations may include work addresses (physical or electronic), post office boxes, etc. Alternative communications requests that may interfere with

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

Vivant's ability to obtain payment for services provided to the member are not reasonable and will be denied; unless Member provides sufficient assurances that payment will be made in a manner satisfactory to Vivant. The Privacy Officer is authorized to grant, or deny, proper alternative communications requests.

27.4 All alternative communications requests will be in writing and submitted to the Privacy Officer. The request will include:

- (a) member's name;
- (b) date of request;
- (c) Member's signature;
- (d) designated recipient;
- (e) requested mode of transmission (e.g., facsimile, e-mail, courier, etc.);
- (f) location/address of delivery;
- (g) type of PHI requested (e.g., billing, related to a service date or a specific provider); and
- (h) acknowledgement that Member was informed of his/her responsibility to pay for any charges related to the alternative communication request; and
  - (i) How Member intends to pay for the costs of the alternative communication.

27.5 If a Business Associate's ("BA") activities and/or obligations regarding the disclosure of PHI that is the subject of an alternative communications request will be affected by the request, Vivant will notify the BA of the nature and scope of the request.

27.6 The Privacy Officer will ensure that all alternative communications requests are documented, along with Vivant's response, for at least ten (10) years from the date of the request(s).

### 28. **When No Written Member Authorization is Required Prior to Disclosures to Third Parties**

28.1 Workforce Members may use or disclose PHI to third parties without first obtaining a valid Member authorization and without providing Member an opportunity to agree or object to Vivant uses or disclosures pursuant to applicable Privacy Laws under the following circumstances:

- (a) When the use or disclosure is made to facilitate treatment, payment or health care operations;
- (b) When the use or disclosure is required by law, upon approval from Privacy Officer;
- (c) When the use or disclosure relates to an individual who has been deceased for more than 50 years (but note, the authorization will identify an

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

expiration deadline that could be longer than 50 years under California law);

- (d) When the use or disclosure is to a coroner, medical examiner, and/or law enforcement to identify a deceased person, determine a cause of death, or perform other duties as required by law;
- (e) When the use or disclosure is to a funeral director in accordance with law as necessary to carry out their duties upon a person's death;
- (f) When the information to be used or disclosed is de-identified in accordance with applicable Privacy Laws, as approved by Privacy Officer or Security Officer;
- (g) When the use or disclosure is to a state-recognized or federally recognized disaster relief organization for the purpose of responding to disaster welfare inquiries (basic information including the member's name, city of residence, age, sex, and general condition may be disclosed);
- (h) When the use or disclosure is otherwise determined by Privacy Officer to be appropriate and comply with applicable Privacy Laws.

28.2 Vivant may disclose PHI to a member's family member, other relative, close personal friend or representative, person responsible for member care, or other person involved in the member's care or payment for services if:

- (a) Vivant obtains Member's written consent prior to disclosure;
- (b) Vivant gives Member the opportunity to object to the disclosure, and/or determines from the circumstances that Member does not object to the disclosure;
- (c) Necessary to notify or assist in notifying a family member, personal representative, or other person involved in the member's care or payment for services (e.g., hospitalization or overdue bill)'
- (d) The opportunity to consent or object to the use or disclosure of PHI is not possible due to member incapacity or an emergency situation. In this event, Workforce Member will notify Privacy Officer who will determine whether it is in the member's best interest to make the use or disclosure;
- (e) In all instances, only that PHI relevant to the third person's involvement with the member will be disclosed.

28.3 A member's PHI will be disclosed without Member authorization when required by federal, state, or local law, including disclosures to Department of Health and Human Services for purposes of enforcing Privacy Laws. Upon receiving a request for PHI from a government agency and/or pursuant to any other legal process, Workforce Member will promptly notify Privacy Officer and:

- (a) Verify that any written request made is on official government letterhead or pleading;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (b) Request that the legal authority submit its request in writing, if feasible;
- (c) When a government agency is acting through a third-party proxy, request written verification on official government letterhead, in a contract, memorandum, purchase order, or other document authenticating the requestor's authority;
- (d) Request official credentials such as an identification badge or other proof of government status if the request is made in person. Make a copy of the provided identification, and maintain such records for ten (10) years;
- (e) If required, document all disclosures in a log maintained by the Privacy Officer.

28.4 If Vivant is not required by law to make the disclosure, the Privacy Officer, or Workforce Member designated by Privacy Officer, will deny the PHI request.

### **29. Special Considerations Regarding Psychotherapy/Mental Health PHI Disclosures to Members**

29.1 Members may request their psychotherapy notes (notes recorded by a mental health professional documenting or analyzing the contents of a conversation during a counseling session) or mental health records (records specifically relating to evaluation or treatment of a mental disorder including alcohol and drug abuse records).

29.2 A Member's authorization is required prior to disclosing psychotherapy notes or mental health records. The authorization must be a separate and independent document, and must include:

- (a) A description of the information to be disclosed;
- (b) The identity of the person or class of persons who may disclose the information;
- (c) The identity of the person or class of person to whom the information may be disclosed;
- (d) A description of the purpose of the disclosure;
- (e) An expiration date for the authorization; and
- (f) The signature of the person authorizing the disclosure.

29.3 However, no authorization is required when the disclosure is required by law such as for mandatory reporting of abuse, and mandatory duty to warn situations regarding threats of serious and imminent harm by the member to self or others.

29.4 A Member's request for mental health records may be refused if a health care provider determines that there is a substantial risk of significant adverse or detrimental consequences to the member if such access were permitted, subject to the following conditions:

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (a) The provider must make a written record and include it with the requested mental health records;
- (b) The record must note the date of the request and describe the specific adverse or detrimental consequences to the member that the provider anticipates would occur if inspection or copying were permitted; and
- (c) The provider must inform the Member of the provider's refusal and inform the Member of the right to require the provider to permit inspection by, or provide copies to, another licensed provider designated by written authorization of the Member.

### **30. Special Considerations Regarding Psychotherapy/Mental Health PHI Disclosures to Third Parties**

30.1 Third parties may receive a member's psychotherapy notes or mental health records.

30.2 As with psychotherapy/mental health disclosures to Members, an authorization is required. The authorization must be a separate and independent document, and must include:

- (a) A description of the information to be disclosed;
- (b) The identity of the person or class of persons who may disclose the information;
- (c) The identity of the person or class of person to whom the information may be disclosed;
- (d) A description of the purpose of the disclosure;
- (e) An expiration date for the authorization; and
- (f) The signature of the person authorizing the disclosure.

30.3 However, no authorization is required when the disclosure is required by law such as for:

- (a) mandatory reporting of abuse;
- (b) mandatory duty to warn situations regarding threats of serious and imminent harm by the member to self or others; or
- (c) when a member, in the opinion of his or her psychotherapist, presents a serious danger of violence to reasonably foreseeable victim(s), then the member's mental health records may be released to the potential victim(s) and to law enforcement agencies and county child welfare agencies as the psychotherapist determines is needed for the protection of the potential victim(s).



## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

30.4 A third-party request relating to a member's participation in outpatient treatment with a psychotherapist will not be granted unless the request:

- (a) is from a law enforcement or regulatory agency pursuant to an investigation of unlawful activity or for licensing, certification, or regulatory purposes and is not otherwise prohibited by law; or
- (b) is from law enforcement, or from the target of a threat, directed to a psychotherapist in which additional information is clearly necessary to prevent a serious and imminent threat; or
- (c) is from a law enforcement or regulatory agency directed to a psychotherapist in which such agency is investigating adverse events related to drugs or medical devices; or
- (d) is from a law enforcement or regulatory agency directed to a psychotherapist in which such agency is investigating instances of abuse under the Welfare and Institutions Code; or
- (e) is submitted in writing and includes:
  - (i) Member's signature;
  - (ii) the specific information relating to a member's participation in outpatient treatment with a psychotherapist being requested and its specific intended use or uses;
  - (iii) the length of time during which the information will be kept before being destroyed or disposed. A person or entity may extend that timeframe, provided that the person or entity notifies Vivant, any BAA, and any third-party performing services to Vivant related to the extension. Any extension notification will include the specific reason for the extension, the intended use or use of the information during the extended time, and the expected date of destruction of the information;
  - (iv) a statement that the information will not be used for any purpose other than its intended use; and
  - (v) a statement that the person or entity requesting the information will destroy the information, and all copies in the person's or entity's possession or control, will cause it to be destroyed, or will return the information and all copies before or immediately after the original or extension time has expired.

### 31. **Special Considerations Regarding Minors' PHI Disclosures and Document Retention**

31.1 Vivant will adhere to all applicable Privacy Laws governing the use or disclosure of minors' medical records.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

31.2 Parents or guardians generally may access a minor's medical records when such access is not inconsistent with State or applicable Privacy Laws.

31.3 Minors may receive medical treatment for certain services that do not require parental consent (e.g., services related to sexual assault, family planning, pregnancy, abortion, etc.). Minors may access their medical records relating to these medical services that did not require parental consent.

- (a) Parental or guardian consent is required for children under age 12 seeking medical services for drug and alcohol abuse, and sexually transmitted diseases.

31.4 A minor's request to see their mental health records may be refused if it is determined that access to the records would have a detrimental effect on the physician's professional relationship with the minor or on the minor's physical safety or psychological well-being.

31.5 The Privacy Officer will ensure that records containing minors' PHI will be maintained for one year past age 18 or for ten (10) years, whichever is longer.

### **32. Authorization Requirements Prior to Disclosures to Third Parties**

32.1 When Workforce Member receives a request for PHI from an individual or entity other than Member, or pursuant to any other third-party request not addressed herein, these procedures apply:

- (a) Authorized Workforce Member will provide the requester with Vivant's authorization form, which will:
  - (i) be handwritten by the signatory to the authorization, or in typeface no smaller than 14-point type;
  - (ii) contain authorization language and corresponding signature clearly separate from any other language on the form;
  - (iii) Is signed and dated by the Member, or
    - (1) spouse of the member or person financially responsible for the member seeks records that are the Minimum Necessary for the sole purpose of processing an application for health insurance or enrollment in a nonprofit hospital plan, health care service plan, employee benefit plan and where the member is to be an enrolled spouse or dependent under the policy or plan; or
    - (2) beneficiary or personal representative of a deceased member;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (iv) provide the identities of those authorized to disclose the medical information;
  - (v) identify the scope of information those authorized to disclose may transmit;
  - (vi) provide the identities of those authorized to receive the medical information;
  - (vii) identify the scope of the authorized recipient's uses and disclosures upon receipt;
  - (viii) provide a date after which Vivant, or its authorized third-party vendor (BAA), is no longer authorized to use or disclose the medical information;
  - (ix) provide a date after which the authorized recipient is no longer authorized to use or disclose the medical information;
  - (x) include language from Vivant to the authorized recipient outlining the permissible scope of uses or disclosures as allowed by Member;
  - (xi) advise the signatory of their right to receive a copy of the authorization; and
  - (xii) advise that the Member may revoke the authorization, subject to Privacy Laws (e.g., law enforcement investigations).
- (b) Upon receipt of an authorization form, those Workforce Members authorized by Privacy Officer will obtain reasonable assurances from Member or determine based upon a review of the authorization and the member's medical record, that the authorization is valid, has been signed and dated by Member, and is complete under applicable Privacy Laws.
- (i) Authorized Workforce Members will further ascertain whether the authorization seeks the use or disclosure of more than one type of PHI ("compound authorization form"). If so, authorized Workforce Member will obtain Privacy Officer's approval in determining whether the authorization is valid. (Most authorizations under HIPAA other than those for use or disclosure of psychotherapy notes may be combined, except when a Covered Entity has conditioned the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of one of the authorizations (45 CFR 164.508(b)(3)), and as otherwise disallowed under Privacy Laws and as set forth in this Policy. Combining the authorization with other documents (e.g. waivers, consents to treatment, conditions of admission, etc.) is generally prohibited.)
- (c) Authorized Workforce Members will document all request dates;
- (d) Authorized Workforce Members will calendar the number of days to respond from receipt of the request;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (e) Authorized Workforce Members will work with Privacy Officer to provide timely responses;
- (f) Authorized Workforce Members will promptly determine whether a response can be provided within the required time frame, or if an extension may be necessary;
- (g) Authorized Workforce Members will provide information to Privacy Officer sufficient to justify an extension, if necessary.

32.2 If any Workforce Member, authorized or other, has questions regarding any of the foregoing authorization procedures, they will consult with the Privacy Officer.

32.3 Upon receipt of a written notice from Member revoking an authorization, Vivant will discontinue using or disclosing PHI related to the underlying authorization. Revoking an authorization will have no effect on Vivant's prior uses and disclosures made in reliance thereon. Additionally:

- (a) Authorized Workforce Member will promptly provide notice of the revocation to Privacy Officer;
- (b) Privacy Officer will promptly notify any Business Associates affected by the revocation; and
- (c) The Privacy Officer will attach the revocation to the original authorization and update Vivant's records accordingly.

32.4 If Vivant receives more than one authorization to disclose a member's PHI to the same third party, the most recently dated authorization will be used. Otherwise, if Vivant receives more than one authorization resulting in an inconsistency, authorized Workforce Member will give the competing authorizations to Privacy Officer, who will review and address the inconsistencies.

### **Limits On Access, Use and Disclosure of PHI**

#### **33. Marketing and Fundraising Activities and Other Uses or Disclosures Where Pre-Approval by Privacy Officer is Required**

33.1 Vivant will comply with all applicable Privacy Laws governing marketing and fundraising activities (e.g., marketing and fundraising is prohibited with respect to Medi-Cal patients).

33.2 All uses and disclosures not addressed in Vivant Policies will be approved in advance by the Privacy Officer.

33.3 Workforce Members will submit all requests for uses and disclosures related to PHI marketing and fundraising activities to the Privacy Officer, who will review such requests for conformance with applicable Privacy Laws.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

33.4 In accordance with Privacy Laws, Vivant requires a valid Member authorization before use or disclosure of PHI for marketing purposes, unless: (1) the marketing occurs in a face-to-face communication between Vivant and the member; or (2) the marketing is nothing more than providing a promotional gift of nominal value to the member (e.g., a coaster or refrigerator magnet).

### **34. Minimum Necessary Standard**

34.1 When disclosing PHI, Workforce Members will make reasonable efforts to disclose only the minimum amount of PHI necessary to accomplish the legitimate business purpose, unless the Minimum Necessary standard is inapplicable under Privacy Laws as determined by Privacy Officer. Circumstances in which the Minimum Necessary standard does not apply include:

- (a) Disclosures to, or requests by, a health care provider for a member's treatment;
- (b) Uses by, or disclosures to, Member (subject to certain exceptions identified in this Policy such as with respect to psychotherapy notes or pursuant to law enforcement investigations);
- (c) When Member has signed an authorization permitting the use or disclosure of PHI;
- (d) Disclosures to law enforcement and/or regulatory agencies as required by law; and/or
- (e) When the use or disclosure is otherwise required by applicable Privacy Laws.

34.2 Disclosures of entire medical records will not be made except pursuant to all applicable procedures in Vivant Policies and applicable Privacy Laws. In instances where disclosure of a member's entire medical record is requested and appropriate, Workforce Member should nevertheless document why the entire medical record was disclosed.

34.3 Workforce Members may assume that the individual or entity requesting PHI has requested only the minimum amount necessary if:

- (a) The disclosure is to a public official or other individual/entity identified in 45 CFR §164.512 of Privacy Laws.
- (b) The disclosure is to another Covered Entity, such as a provider, hospital, or health plan.
- (c) The disclosure is to another Workforce Member with authorized PHI access.
- (d) The disclosure is to a Business Associate with authorized PHI access.
- (e) The disclosure is to a researcher who has provided appropriate documentation from an Institutional Review Board or Privacy Board.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

34.4 Workforce Members disclosing PHI should consult with Privacy Officer when there is any question regarding the Minimum Necessary standard, or the procedures described herein.

### **35. Requests for Restrictions on Uses and Disclosures.**

35.1 Vivant will comply with a member's written request(s) to restrict disclosure of their PHI, unless otherwise required by Privacy Laws, if:

- (a) The PHI pertains solely to a health care item or service for which the health care provider involved has been paid by an individual or entity on the member's behalf;
- (b) The disclosure is to a Covered Entity for the purpose of facilitating payment or health care operations;
- (c) The disclosure is to a health care provider to whom certain PHI has previously been restricted ("Restricted Provider"), but the PHI that is the subject of the current disclosure bears no connection to the care or treatment that the Restricted Provider is offering or providing to the member; and/or
- (d) Member requests that their information not be disclosed to a family member or close personal friend.

35.2 When a Workforce Member receives a written request from Member to restrict the use or disclosure of PHI, Workforce Member will deliver the written request to Privacy Officer. The Privacy Officer will review the written request and ensure the Member is informed whether Vivant has agreed to the requested restriction(s). The Privacy Officer will also ensure that all Business Associates are notified of the requested restriction(s).

35.3 The Privacy Officer will take reasonable steps to ensure the request and disclosure is appropriately documented.

### **36. Special Restrictions on Certain Types of Health Information: HIV, Substance Abuse, and Genetics**

36.1 HIV Information. Absent written authorization, Vivant will not disclose any information regarding HIV test results, care, and/or treatment that identifies or tends to identify the individual about whom the HIV-related information relates, subject to the following exceptions:

- (a) The physician who confirms a positive HIV test of a patient under his or her care may disclose the results to a person reasonably believed to be the spouse or sexual partner of the patient, to a person with whom the patient has shared the use of hypodermic needles, or to the local health officer, but may not identify information about the patient, and only after the

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- physician discusses the results with the patient, offers counseling, and attempts to obtain consent to notify others;
- (b) A Person (a member's provider or Vivant if the information is lawfully in Vivant's possession) may disclose identity-specific HIV test results to the Member or any person authorized to consent to the underlying test under Health and Safety Code section 120990 and Family Code section 6926;
  - (c) A Person may disclose identity-specific HIV test results to the patient's health care provider or the provider's agent or employee for the purpose of diagnosis, care, or treatment;
  - (d) A Person may disclose identity-specific HIV test results to a local health officer when necessary to locate a blood donor whose blood tested positive when reasonable efforts by the blood bank or plasma center to locate the donor failed;
  - (e) A Person may disclose identity-specific HIV test results to the designated officer of an emergency responder who could have been exposed to HIV through their employment, though both the officer and responder are subject to confidentiality requirements;
  - (f) A Person may disclose identity-specific HIV test results to comply with a state or federal reporting requirement, including to the Office of AIDS for the California Department of Public Health ("CDPH") and the U.S. Centers for Disease Control and Prevention;
  - (g) A Person may disclose identity-specific HIV test results to a health care provider who receives donated body parts.

36.2 Alcohol or Drug Abuse Information. Records regarding the identity or treatment of any member in connection with alcohol and drug abuse treatment will be kept confidential, which confidentiality will continue indefinitely. Written authorization from the Member is required prior to disclosing such records, which records may be disclosed only to the extent, under the circumstances, and for the purposes set forth in the authorization.

- (a) A member's alcohol or drug abuse records may be disclosed without an authorization under the following circumstances:
  - (i) In communications between qualified professional persons employed by the treatment program;
  - (ii) To qualified medical persons to the extent necessary to address a medical emergency;
  - (iii) To qualified personnel for the purpose of conducting scientific research, management audits, financial and compliance audits, or program evaluation (such personnel may not identify, directly or indirectly, any individual member in any subsequent report);
  - (iv) When authorized by a court of law.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (b) All disclosures outside of Vivant will be approved in advance by the Privacy Officer in consultation with legal counsel.

36.3 Genetic Information. Genetic information may not be used or disclosed for underwriting purposes. Genetic information includes information about an individual's genetic tests, the genetic tests of the individual's family members, the manifestation of a disease or disorder in the individual's family members, or any request for or receipt of genetic services, or participation in clinical research that includes genetic services by the individual or the individual's family member, and with respect to a pregnant woman (or a family member of a pregnant woman) genetic information about the fetus, and with respect to an individual using assisted reproductive technology, genetic information about the embryo. With the exception of disclosures required by the California Department of Health Care Services and by the California Department of Managed Health Care, all disclosures of genetic test results outside of Vivant require the Member's specific prior written authorization.

### **Documenting Disclosures and Accounting**

#### **37. Documenting Disclosures**

37.1 Privacy Officer will ensure that all uses and disclosures related to the confidentiality, integrity, and availability of PHI will be maintained for at least 50 years following the member's death (note, the authorization will identify an expiration deadline that could be longer than 50 years under California law), except that, upon the member's death, Vivant may disclose to a family member, close personal friend or representative, or other person involved in the member's medical care prior to death, or related payment, such PHI as is relevant to such person's involvement, unless doing so would be inconsistent with any prior expressed preference(s) of the Member that are known to Vivant based upon a reasonable inquiry. Upon request by Member, Vivant will provide an accounting of available disclosures except as specified below.

37.2 An accounting of disclosures will not be provided to Member when the disclosures are:

- (a) For the purpose of carrying out treatment, payment or health care operations (except to the extent required by Privacy Laws related to the use of PHI);
- (b) To Member regarding the member's own health information;
- (c) To individuals or entities involved in the member's care, or for the purpose of notifying the member's family or friends about the member's whereabouts;
- (d) For national security or intelligence purposes;
- (e) To correctional institutions or law enforcement officials who had the member in custody at the time of disclosure;
- (f) Upon Member's authorization;



## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (g) Part of a Limited Data Set (a Limited Data Set may contain the member's date of birth, date of death, dates of service, zip code, gender, but it may not contain the member's name, social security number, street address, etc.);

37.3 Member requests for an accounting of disclosures will be in writing and given to the Privacy Officer.

37.4 Upon receiving a written request for an accounting of disclosures, Privacy Officer will:

- (a) Contact all Business Associates and/or providers who have received PHI for the member in question and request a copy of the Business Associate's relevant disclosure accounting logs;
- (b) Within sixty (60) days of Member's request, review all relevant disclosure accounting logs and either provide the accounting requested or notify Member that an extension of time is needed, which extension may not be longer than thirty (30) days and which may only be utilized once per request; and
- (c) Provide the date that the disclosure accounting will be available, along with an explanation (including the reason(s) for any delay).

37.5 The disclosure accounting will include:

- (a) The disclosure date(s);
- (b) The recipients of the disclosure(s), and, if known, their address(es);
- (c) A brief description of the information disclosed; and
- (d) A brief statement detailing the purpose for the disclosure.

37.6 If multiple disclosures are made to the same individual or entity, a single reference to the first disclosure with the requisite information identified in this Policy followed by the date(s) of subsequent disclosures constitutes sufficient accounting.

37.7 In all instances, disclosure accountings need only include disclosures made during the preceding six (6) years.

37.8 Vivant will comply with any government agency requests to suspend a member's ability to receive a disclosure accounting.

- (a) If the agency makes the request orally, it is only effective for thirty (30) days and may not be renewed. The agency must specify that a disclosure accounting would likely impede its lawful activities. A Workforce Member will document the oral request and the identity of the government official making the request.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (b) During the thirty (30) day timeframe within which the oral request is valid, the agency must provide a written statement that a disclosure accounting would likely impede its lawful activities and provide an end date for the suspension.

37.9 The Privacy Officer will ensure that all communications regarding requests for disclosure accounting, including requests for suspensions of disclosure accounting, will be maintained for at least ten (10) years.

### **Requests for Modifications and/or Amendments to PHI**

#### **38. Modifications and/or Amendments to Medical and Billing Records**

38.1 Vivant's providers or another Covered Entity may request that Vivant modify and/or amend a member's PHI. In such an event, Vivant will modify and/or amend the PHI within a reasonable timeframe.

38.2 Vivant's Members may request that Vivant modify and/or amend their PHI. All such requests will be in writing and detail the reason(s) for the request.

- (a) The written request will:
  - (i) Be limited to 250 words per alleged incomplete or incorrect item; and
  - (ii) Indicate whether the Member wishes the modification/amendment would be made a part of the member's medical record.
- (b) Workforce Member will deliver the request to Privacy Officer, who will review the request and determine whether it will be made after consulting with appropriate health care providers, if necessary. Vivant will make reasonable efforts to grant or deny the request within sixty (60) days of receipt;
- (c) If Vivant is unable to grant or deny the request within sixty (60) days, Vivant will provide written notice to Member outlining the reasons for the delay and the anticipated determination date, which may not be extended by more than thirty (30) days;
- (d) If Privacy Officer grants the requested modification/amendment, or Vivant is notified that another Covered Entity has granted the request, Privacy Officer will:
  - (i) Modify and/or amend the PHI that is the subject of the request and append or provide a link to the modification/amendment;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (ii) Notify Member that the request was granted and obtain Member's agreement to notify any individuals or entities with whom the modification/amendment must be shared;
  - (iii) Provide the modified/amended PHI within a reasonable time to the individuals or entities identified by Member with whom the information must be shared;
  - (iv) Notify any Business Associates affected by the modification or amendment.
- (e) If Privacy Officer denies a request, which may only be done pursuant to applicable Privacy Laws, a written denial will be provided to Member that contains:
  - (i) the reason for the denial;
  - (ii) a statement that Member has the right to submit a written disagreement;
  - (iii) a statement that if Member does not submit a written disagreement, Member may request that Vivant provide the request for modification/amendment and the denial with future disclosures of the PHI; and
  - (iv) a description on how Member may file a complaint with Vivant, or the Secretary of HHS in the event of a denial.
- (f) If Member files a written statement disagreeing with Vivant's denial of the modification/amendment request:
  - (i) Privacy Officer will maintain a copy for at least ten (10) years;
  - (ii) Privacy Officer may prepare a written rebuttal and submit a copy to Member;
  - (iii) Privacy Officer will identify the PHI that is the subject of the disputed modification/amendment and attach or link the following to the member's medical record or the designated record:
    - (1) Member's request for a modification/amendment;
    - (2) Vivant's denial of the request;
    - (3) Member's statement of disagreement, if any; and
    - (4) Vivant's rebuttal, if any.
  - (iv) If Member files a statement of disagreement, Vivant will include it with any future disclosures of the PHI;
- (g) If Member does not submit a statement of disagreement, Vivant will, upon Member's request, include a copy of the request and a statement of denial with any future disclosures of the PHI;

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (h) If the disclosure does not allow additional material to be included, Vivant will transmit the request and denial information separately.

38.3 All correspondence regarding modification and/or amendment requests, including approvals or denials, will be maintained in the member's record for at least ten (10) years.

### **Disposal of PHI**

#### **39. Data Sanitization and Destruction**

39.1 Security Officer will ensure that all Vivant-Provided Devices and Personal Devices that have been used to store, duplicate, and/or transmit PHI, including without limitation, fax machines and copiers, will be reviewed for PHI (including any and all memory within the device or equipment) and sanitized using a method approved by the Secretary prior to being returned under a lease, disposed of, transferred or moved outside Vivant, and/or assigned/checked out/transferred to another Workforce Member, or when returned or provided to Vivant for maintenance or repairs. Any device or equipment that cannot be appropriately sanitized will be routed for secure disposal.

39.2 Preferred methods of sanitization before disposal include disintegration; pulverization; melting; incineration; and permanent deletion; or, if none of these are feasible, encryption.

39.3 Paper copies of PHI will be cross-cut shredded, or otherwise destroyed utilizing a NIST-approved standard.

### **Record Retention**

#### **40. Record Retention**

40.1 Vivant will retain records and documents required by applicable Privacy Laws, including Vivant Policies, written or electronic communications involving HIPAA processes such as Notice of Privacy Practices, appeals related to PHI, etc., for a minimum of ten (10) years from the date of the document's creation or the date last in effect, whichever is later, or as otherwise set forth in Vivant Policies. Such documents may include:

- (a) All substantive and material documents relating to Vivant Policies;
- (b) All substantive and material documents relating to Administrative Safeguards, including, but not limited to, Workforce job duties/classifications, authorization lists, training attendance, training materials, date and content of Workforce communications, access requests and authorizations, access terminations, Workforce sanctions,

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- signed confidentiality agreements, risk assessments, risk management strategies, procedures, plans, scanning, tests, and audits;
- (c) All substantive and material documents related to Physical Safeguards, including, but not limited to, logs, assessments, reports, inventories, policies, procedures, and authorized person lists;
  - (d) All substantive and material documents related to Technical Safeguards, including, but not limited to, password requirements, protocols, procedures, plans, designs, review, selection, installation, data scrubbing, and disposal;
  - (e) All necessary documents related to data entry and modifications including authorization procedures, tracking mechanisms, and data authentication methods;
  - (f) All substantive and material documents related to transmission and storage of PHI, including, but not limited to, electronic communications, Business Associate Agreements, confidentiality agreements, procedures, and reports;
  - (g) All necessary documents related to Security Incidents, including, but not limited to, reports, investigations, mitigations, and notifications regarding Security Incidents, suspected Breaches, or actual Breaches.

40.2 Vivant uses technologies to secure data meeting FIPS 140-2 compliance.

- (a) Vivant utilizes Microsoft Azure Storage.
  - (i) Data in Azure Storage is encrypted with SSE using 256-bit AES encryption.
  - (ii) Vivant utilizes Microsoft Azure encryption at rest with a platform managed key.

<https://docs.microsoft.com/en-us/azure/key-vault/general/overview>

### **Reports and Complaints**

#### **41. Reports**

41.1 Workforce Members who know or reasonably suspect that there has been a violation of Vivant Policies, including Vivant’s Compliance Plan, Privacy Laws, and/or the improper use or disclosure of PHI (collectively, “Reportable Incident”) will promptly report the suspected Reportable Incident.

41.2 Vivant will maintain a toll-free telephone number and e-mail address where Workforce Members may convey Reportable Incidents.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

- (a) Workforce Members will elect, at their discretion, to provide their contact information or remain anonymous when conveying Reportable Incidents.

41.3 The Workforce Member who discovers the Reportable Incident should also, where appropriate and prudent and in consultation with Privacy Officer and/or Security Officer, take steps to recover or destroy any PHI unlawfully disclosed or otherwise limit the potential risk or compromise of PHI.

41.4 The Privacy Officer will continually monitor the telephone messaging service and e-mail account where Workforce Members may convey Reportable Incidents.

41.5 Privacy Officer and Security Officer will take the following additional steps with respect to Reportable Incidents, and at the direction of General Counsel:

- (a) Communicate Reportable Incidents to the General Counsel within twenty-four (24) hours of discovery;
- (b) Reports related to Reportable Incidents will be in writing;
- (c) All Reportable Incidents will be initiated as quickly as possible and no later than two weeks after the date the potential noncompliance is identified
- (d) All Reportable Incidents will promptly and fully investigated; and will be reported to the Health Plans, if applicable
- (e) Conduct risk assessments if indicated;
- (f) Take any and all action necessary to ensure compliance with Privacy Laws and Vivant's Policies if applicable;
- (g) Take any and all action necessary for risk management and/or mitigation; Otherwise adhere to Vivant's Compliance Plan.

### 42. **Complaints**

42.1 Members and other individuals may submit complaints to Vivant regarding the use or disclosure of PHI relating to a member. Such complaints will be directed or submitted to the Privacy Officer.

42.2 The Privacy Officer will document the complaints, at the direction of General Counsel.

42.3 The Privacy Officer will review all applicable information related to the use or disclosure of the member's PHI that is the subject of the complaint(s), at the direction of General Counsel.

42.4 At the direction of General Counsel, the Privacy Officer, or Privacy Officer's designee, will review all complaints within fourteen (14) days of receipt. If the complaint requires a response, and contact information is provided, the Privacy Officer or designee will prepare and deliver a written response to the Member or individual who lodged the complaint. If the

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

complaint does not require a response, or contact information is not provided, the Privacy Officer or designee will prepare a written statement of any action taken and attach it to the filed complaint.

42.5 If a use or disclosure violation is confirmed, the Privacy Officer will sanction the Workforce Member responsible, if applicable, as set forth in this Policy, which sanctions can include being reprimanded up to and including termination. The Privacy Officer will document the actions taken and place all information relating to the complaint in Vivant's files.

42.6 If the Privacy Officer determines that the complaint has no merit, the investigation will be documented and placed in Vivant's file.

42.7 At no time will a Workforce Member who is the subject of a complaint be the same person responsible for investigating the complaint.

42.8 In the event that the complaint is about the Privacy Officer or Security Officer, the General Counsel will be notified and will investigate, or direct investigation of, the complaint.

### **43. No Intimidation or Retaliation**

43.1 Vivant will not intimidate, threaten, coerce, discriminate, retaliate, or withhold treatment from any Workforce Member or other individual for exercising any rights under Privacy Laws, including submitting complaints, filing reports, etc. Any violations of this non-intimidation or retaliation policy will be handled in accordance with Vivant Policies.

43.2 Training regarding Vivant Policies will include instructions that Workforce Members may not retaliate against any individual for exercising rights granted by the Privacy Laws and will be sanctioned for doing so.

43.3 Workforce Members will notify Privacy Officer or the General Counsel of any retaliatory act or intimidation.

43.4 Workforce Members who are determined to have retaliated against an individual for exercising rights granted by Privacy Laws will be sanctioned according to the severity of the violation and surrounding circumstances, consistent with Vivant Policies.

43.5 No sanctions will be imposed for actions constituting disclosures by whistleblowers or Workforce Member crime victims under 45 C.F.R. §164.502.

### **44. Reporting Security Incidents and/or Breaches to Third Parties**

44.1 Vivant will promptly report to third parties any incidents required to be reported under applicable Privacy Laws.

## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

44.2 The General Counsel will ensure that, where Vivant is required by Privacy Laws to give notice of any incident to Member, entities with whom the Vivant contracts, and/or a government agency, such notifications are made in the form and timeframe as required by Privacy Laws, and/or the Vivant's contracts, and in accordance with Vivant's Compliance Plan.

### **45. Risk Assessment and Risk/Issues Log**

45.1 Vivant will ensure Risk Assessments and/or Risk/Issues Log will be managed to mitigate risks or remediate issues when appropriate.

### **46. Foreign Corrupt Practices Act (FCPA)**

46.1 Title 15 of the United States Code § 78dd-1 prohibits bribery or corrupt practices by US issuers with foreign official.

46.2 This prohibition extends to any officer, director, employee, or agent or any stockholder of the issuer.

- (a) "Issuer" is defined as an entity that is registered with the US Securities and Exchange Commission and/or files reports with the SEC. In other words, Vivant is an "issuer", and its "agent" are contracted third parties, vendors, delegates, downstream entities, or subcontractors;
- (b) "Foreign official" includes any officer or employee of a foreign government or agency, or instrumentality of (such as government hospitals), and any officer or employee of a public international organization. This prohibition also extends to any foreign political party or official and any candidate for a foreign political office. This definition includes:
  - (i) Government agents or representatives;
  - (ii) Individuals in political office;
  - (iii) Representatives of a political party;
  - (iv) Officers or employees of government-owned business (such as employees of a state-own hospital);
  - (v) Officers or employees of quasi-government agencies or bodies;
  - (vi) Individuals with influence over a political body; and
  - (vii) Individuals with extensive experience or a history of dealing with foreign government

46.3 Vivant is committed to the prevention, detection, and elimination of all forms of corrupt business practices. Any form of bribery or corruption, whether in commercial dealings with private parties, or in dealings with officials of any state, local, federal, or foreign government is strictly prohibited.



## **PRIVACY AND SECURITY POLICIES AND PROCEDURES**

46.4 As a US company, Vivant is subject to the US Foreign Corrupt Practices Act (FCPA) which makes it a criminal offense for Vivant and/or its officers, directors, employees and any third party doing business with or for Vivant to offer, pay, or give any payment or other item of having value to any foreign official, political party, official or candidate of a political party, or public international organization, for the purpose of influencing any act or decision broadly designed to obtain, retain or direct business to Vivant.

### 47. **Pandemic Plan**

47.1 If Vivant experiences a significant loss of staff due to a pandemic, Vivant has well-established partnerships with staffing firms that Vivant utilizes to hire efficiently for support.

**PRIVACY AND SECURITY POLICIES AND PROCEDURES**

**Version History and Review**

<b>Version #</b>	<b>Date</b>	<b>Reviewed By</b>	<b>Description of Change</b>	<b>Updated Document ID</b>
1	01/26/2024	Kevin Lillywhite, Compliance Officer and RCMG Compliance Committee	Added Version History and Review table and conducted Annual Review	2024