HIPAA Privacy and Security Policy

April, 2020

Introduction

This Privacy Policy describes how Docademic, Inc. collects and uses Personal Data about you through the use of our websites, mobile applications, and through email, text, and other electronic communications between you and Docademic, Inc.

Docademic, Inc. ("Docademic" or "we," "our," or "us") is involved in the administration of telemedicine services, as described in the Terms of Use through the use of a digital medium (the "Platform"). Doc.com has adopted this policy to ensure compliance of the Platform under HIPAA.

This Privacy Policy (our "Privacy Policy") describes the types of information we may collect from you or that you may provide when you visit the https://docademic.com/, https://www.coolemotions.com/, https://MTC.Docademic.com, and https://www.doc.com websites (collectively, our "Website") and the associated Doc.com application ("Application") and our practices for collecting, using, maintaining, protecting, and disclosing that information.

This policy applies to information we collect:

- on our Website and Application;
- in email, text, and other electronic messages between you and our Website and Application;
- when you interact with our advertising and applications on third-party websites and services, if those applications or advertising include links to this policy.

It does not apply to information collected by:

- us offline or through any other means, including on any other website operated by Docademic or any third-party;
- any third party, including through any application or content (including advertising) that may link to or be accessible from or on the Website or Application.

Members of Docademic's workforce may have access to the "protected health information" (as described below) of Platform participants and dependents on behalf of the Platform or of Docademic in relation to its administrative functions. Docademic intends to fully comply with the HIPAA requirements, as administered by the United States Department of Health and Human Services (HHS), including HIPAA's Privacy Rule and Security Rule. HIPAA restricts Docademic's use and disclosure of protected health information relating to the Platform, including by the Platform's "business associates".

"Protected health information" ("PHI") means information that is created or received by the Platform and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information concerning persons living or deceased. The Security Rule governs electronically conveyed PHI, or "E-PHI." ("PHI" herein includes "E-PHI" unless "E-PHI" is specified.) Special aspects of Security Rule compliance are addressed at Article 2.12, below.

Docademic has adopted this Privacy Policy regarding the use and disclosure of PHI and individuals' rights relating to their PHI. All members of Docademic's workforce who have access to PHI must comply with this Privacy Policy. Individuals who would be considered part of Docademic's workforce under HIPAA are employees, independent contractors, volunteers, trainees, and other persons whose work performance is under the direct control of Docademic, whether or not they are paid by Docademic. The term "employee" herein includes all of these types of workers.

Note, Docademic is not a medical or psychological group. Any telepsychology or telemedicine consults obtained through our Website are provided by independent psychology or medical practitioners including, but not limited to, Docademic Provider Group P.A., an independent medical group with a network of United States based psychological or medical providers (each, a "Provider").

Please read this policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, your choice is not to use our Website and Applications. By accessing or using our Website and/or Application, you agree to this Privacy Policy. This Privacy Policy may change from time to time (see Changes to Our Privacy Policy). Your continued use of our Website or Application after we make changes is deemed to be acceptance of those changes, so please check this Privacy Policy periodically for updates.

Article I. CHILDREN UNDER THE AGE OF 18

Our Website and Application are not intended for children under the age of 18 and children under the age of 18 are not permitted to use our Website or our Application without parental or guardian consent. We will remove any information about a child under the age of 18 if we become aware of it.

Our Website and Application are not intended for children under 18 years of age. No one under age 18 may provide any information to or through the Website or Application. We do not knowingly collect Personal Data from children under 18. If you are under the age of 18 and wish to create an account with Docademic or receive services through our Website and Application, your parent or legal guardian must create the account, submit your personal information, agree to the Terms of Use and the Privacy Policy on your behalf. If we learn we have collected or received Personal Data from a child under 18 without verification of parental consent, we will delete that information. If you believe we might have any information from a child under 18, please contact us at support@doc.com.

Article II. PLATFORM RESPONSIBILITIES AS COVERED ENTITY.

II.1. **Privacy Official and Contact Person.** Christopher Parker will be the Privacy Official for the Platform. The Privacy Official will be responsible for the administration of policies and procedures relating to privacy, including but not limited to this Privacy Policy.

The Privacy Official has designated Christopher Parker Privacy Officer, as the contact person ("Contact Person") for all regular and routine matters, as set forth herein. The Contact Person will serve as the person available to participants who have questions, concerns, or complaints about their PHI.

II.2. **Security Official and Contact Person.** Christopher Parker, Privacy Officer, will be the Security Official. The Security Official will serve as the person available for any issues of a technical nature specific to the HIPAA Security implementation specifications.

Christopher Parker, Privacy Office, will serve as Contact Person for Privacy and Security Rule regular and routine matters.

II.3. **Persons with Access; Workforce Training.** It is Docademic's policy to limit access to PHI to those who have need and to train employees who have access to PHI on its privacy and security policies and procedures. The Privacy Official, Security Official and Contact Person will develop training schedules and programs so that employees who have access to PHI (including E-PHI) receive the training necessary and appropriate to permit them to carry out their functions within Platform.

II.4. **Technical and Physical Safeguards and Firewall.** An analysis of all Docademic's information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats—internal or external, natural or manmade, electronic and non-electronic—that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with *its collection, storage, dissemination and protection. From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined*. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

II.5. All computer equipment and network systems are assets of Docademic and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based on the following:

• **Installed Software:** All software packages that reside on computers and networks within Docademic must comply with applicable licensing agreements and restrictions and must comply with Docademic's acquisition of software policies.

• **Virus Protection:** Virus checking systems approved by the Security Official and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

- **Access Controls:** Physical and electronic access to PHI is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Security Official and approved by Docademic. Mechanisms to control access to PHI include (but are not limited to) the following methods:

(a) **Authorization:** Access will be user-based access whereby users of a system gain access based upon the identity of the user.

(b) **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PHI. Users will be held accountable for all actions performed on the system with their user id.

(1) Authentication shall be by **strictly** controlled passwords.

(2) The user must secure his/her authentication control (e.g. password) such that it is known only to that user and possibly a designated security manager.

(3) An automatic timeout re-authentication must be required after a certain period of no activity.

(4) The workstation must freeze after three unsuccessful attempts to gain access.

(5) The user must log off or secure the system when leaving it.

(c) **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features will be implemented:

(1) Encryption shall be utilized for emails where electronic PHI is transmitted.

(2) Benefits personnel shall use facsimile or telephone contact with the third-party administrator to the Platform when dealing with electronic PHI in claims assistance.

(d) **Remote Access:** Access into Docademic's network from outside will be granted using Docademic approved devices and pathways on an individual user and application basis. All remote access to systems which may access electronic PHI shall be made using a "virtual private network". All other network access options to these systems are strictly prohibited.

(e) **Physical Access:** Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

The following physical controls must be in place:

(1) Mainframe computer systems must be installed in an access-controlled area.

(2) File servers containing PHI must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

(3) Workstations or personal computers (PC) must be secured against use by unauthorized individuals. The following policies regarding workstation use and physical safeguards are instituted:

(i) Position workstations to minimize unauthorized viewing of protected health information.

(ii) Grant access to systems which may access electronic PHI only to those who need it in order to perform their job function.

(iii) Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to PHI.

(iv) Use automatic screen savers with passwords to protect unattended machines.

(4) Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

(i) Facility Security Platform—Procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(ii) Access Control and Validation—Procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iii) Maintenance records—Procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

(f) Employee Hiring and Departures:

(1) Docademic shall maintain its existing clearance procedures regarding the hiring of employees.

(2) Docademic shall maintain its existing procedures regarding departing employees, which include promptly deactivating system access and recovering ID cards, remote access devices and other access items.

(g) Security Updates: Docademic will provide periodic updates as appropriate, including security reminders regarding access security, virus protection and maintaining password protection.

Equipment and Media Controls: The disposal of PHI must ensure its continued protection. The receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility shall be documented by Information Services personnel. Docademic will maintain a record of the movements of hardware and electronic media and any person responsible therefor. PHI must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PCs, etc.) unless the devices have the following minimum security requirements implemented:

(1) Power-on passwords

(2) Auto logoff or screen saver with password

(3) Encryption of stored data or other acceptable safeguards approved by the Security Official

(4) Mobile computing devices must never be left unattended in unsecured areas

Data Transfer/Printing: PHI must be stored in a manner that is inaccessible to unauthorized individuals. PHI must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Oral Communications: Company staff should be aware of their surroundings when discussing PHI. This includes the use of cellular telephones in public areas. Company staff should not discuss PHI in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

Audit Controls: Logs that record and examine activity in information systems that contain or use PHI will be maintained. Records of information system activity will be reviewed weekly and available for review should a security incident have occurred or be suspected.

Evaluation: Docademic shall undertake periodic technical and non-technical evaluations in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

Contingency Platform: Controls must ensure that Docademic can recover from any damage to computer equipment or files within a reasonable period of time. Docademic will create and maintain, for a specific period of time, retrievable exact copies of information. Certain backup data must be stored in an off-site location and protected from physical damage.

II.6. **Privacy Notice.** The Privacy Official will maintain the Platform's Notice of the Privacy Practices that describes the uses and disclosures of PHI that may be made by the Platform; the individual's rights with respect to use and disclosure of PHI; and the Platform's legal duties with respect to the PHI.

The Notice informs participants that Docademic and certain third parties as described therein will have access to PHI in connection with Platform administrative functions. The Notice also provides details of Docademic's complaint procedures specifically for HIPAA Privacy and Security, the name and telephone number of the Privacy Official, Contact Person and Security Official for further information and assistance; and the date of the notice, among other elements.

II.7. **Complaints.** The Contact Person is responsible for administering a process for individuals to lodge complaints about the Platform's privacy and security procedures. A copy of the complaint procedure shall be provided to any participant upon request.

II.8. **Sanctions for Violations of Privacy and Security Policy.** Sanctions for using or disclosing PHI in violation of this HIPAA Privacy and Security Policy will be imposed in accordance with Docademic's discipline policy.

II.9. **Mitigation of Inadvertent Disclosures of Protected Health Information.** Docademic shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this

Policy. As a result, if an employee becomes aware of a disclosure of PHI that violates this Policy, either by an employee of the Platform or a third-party administrator or Provider, the employee may contact the Privacy Official so that the appropriate steps can be taken to mitigate the harm to the participant.

II.10. **Breach Notification Requirements.** The Platform will comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") and its implementing regulations with respect to notifications in the event of a breach of unsecured PHI. As a result, if an employee becomes aware of a potential breach of unsecured PHI, the employee shall contact the Privacy Official. Promptly after a report of suspected breach of unsecured PHI, the Privacy Official shall direct and undertake an investigation and risk assessment to determine if a breach of unsecured PHI occurred and the scope of such breach. There is a reportable breach only if all of the following have occurred, as determined by the Privacy Official:

- There is a violation of the HIPAA Privacy Rules involving "unsecured" PHI.
- The violation involved unauthorized access, use, acquisition, or disclosure of unsecured PHI.
- The violation resulted in a compromise of the security or privacy of the PHI.
- No exception applies under applicable law.

If the Privacy Official determines that there is a low probability that the PHI was compromised, the Platform will document the determination in writing and keep the documentation on file.

The Platform shall, following the discovery of a breach of unsecured PHI that is required to be reported, notify each individual whose unsecured PHI has been, or is reasonably believed by the Platform to have been, accessed, acquired, used, or disclosed as a result of such breach as well as the Secretary of HHS.

For a breach of unsecured PHI involving 500 or more residents of a state or jurisdiction, the Platform shall notify prominent media outlets serving the state or jurisdiction.

For a breach of unsecured PHI involving 500 or more individuals, the Platform shall notify the Secretary of HHS contemporaneously with the notice to affected individuals and in the manner specified on the HHS website.

The above notices shall be provided without unreasonable delay and in no case later than 60 days after discovery of the breach and shall comply with the requirements of the HITECH Act and its implementing regulations with respect to the content and method of notification.

A business associate is required to do the same.

II.11. **Breach Notification Definitions**

- *Breach*. The acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA and its implementing regulations which compromises the security or privacy of the PHI. If an unauthorized use or disclosure of PHI occurs, the security or privacy of PHI is presumed to have been compromised unless the Platform demonstrates that there

is a low probability that the PHI has been compromised. This determination is made through a risk assessment of at least the following factors:

(a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(b) The unauthorized person who used the PHI or to whom the disclosure was made;

(c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated.

A use or disclosure of PHI that does not include the identifiers listed at 45 CFR §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information. *Breach* excludes:

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

(b) Any inadvertent disclosure by a Person with Access and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA and its implementing regulations.

(c) A disclosure of PHI where the Platform has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

· *Unsecured PHI*. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS in the guidance issued under Section 13402(h)(2) of the HITECH Act on the HHS website.

I.2. **No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy and Security.** No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

I.3. **Documentation and Document Retention.** The Platform's and Docademic's privacy policies and procedures must be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must promptly be documented.

If a change in law impacts the Notice, the Notice must promptly be revised and made available to the necessary parties. Such change is effective only with respect to PHI created or received after the effective date of the Notice. The Platform and Docademic shall document certain events and actions (including authorizations, requests for information, sanctions, complaints) relating to an individual's privacy rights. The

documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Covered entities must maintain such documentation for at least six years, beginning with documents created on or after April 14, 2003.

Article II. INFORMATION WE COLLECT ABOUT YOU AND HOW WE COLLECT IT

We collect different types of information about you, including information that may directly identify you, information that is about you but individually does not personally identify you, and information that we combine with our other users. This includes information that we collect directly from you or through automated collection technologies.

II.1. We collect several types of information from and about users of our Website and Application, specifically information:

(a) by which you may be personally identified, such as name, e-mail address, date of birth, and address, (collectively, "Personal Data");

(b) that is about you but individually does not identify you, such as traffic data, location data, logs, referring/exit pages, date and time of your visit to our Website or use of our Application, error information, clickstream data, and other communication data and the resources that you access and use on the Website or through our Application; and/or

(c) about your internet connection, the equipment you use to access our Website or use our Application and usage details.

II.2. We collect this information:

(a) directly from you when you provide it to us;

(b) automatically as you navigate through the Website or use our Application. Information collected automatically may include usage details, IP addresses, and information collected through cookies, geo-location services, and other tracking technologies; and

(c) From third parties, for example, from Providers.

(d) Information You Provide to Us

II.3. The information we collect on or through our Website or through our Application are:

(a) information that you provide by filling in forms on our Website or the Application. This includes information provided at the time of registering to use our Application, using our Provider consultation services, or requesting further services. We may also ask you for information when you report a problem with our Website or Application;

(b) records and copies of your correspondence (including email addresses), if you contact us;

(c) your responses to surveys that we might ask you to complete;

(d) details of transactions you carry out through our Website or through the Application and of the fulfillment of your orders.

II.4. As you navigate through and interact with our Website and Application, we may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, specifically:

(a) details of your visits to our Website or Application, such as traffic data, location data, logs, referring/exit pages, date and time of your visit to our Website or use of our Application, error information, clickstream data, and other communication data and the resources that you access and use on the Website or in the Application; and,

(b) information about your computer, mobile device, and internet connection, specifically your IP address, operating system, browser type, and Application version information.

II.5. The information we collect automatically may include Personal Data or we may maintain it or associate it with Personal Data we collect in other ways or receive from third parties. It helps us to improve our Website and Application and to deliver a better and more personalized service by enabling us to:

(a) estimate our audience size and usage patterns;

(b) verify your location to ensure we can provide you with our services;

(c) store information about your preferences, allowing us to customize our Website and our Application according to your individual interests;

(d) recognize you when you return to our Website and our Application.

II.6. The technologies we use for this automatic data collection may include:

(a) Cookies (or browser cookies). A “cookie” is a small file placed on the hard drive of your computer or mobile device. On your computer, you may refuse to accept browser cookies by activating the appropriate setting on your browser, and you may have similar capabilities on your mobile device in the preferences for your operating system or browser. However, if you select this setting you may be unable to access certain parts of our Website or use certain parts of our Application. Unless you have adjusted your browser or operating system setting so that it will refuse cookies, our system will issue cookies when you direct your browser to our Website or use our Application.

(b) Google Analytics. We use Google Analytics, a web analytics service provided by Google, Inc. (“Google”) to collect certain information relating to your use of the Website. Google Analytics uses cookies to help the Website analyze how users use the site. You can find out more about how Google uses data when you visit our Website by visiting “How Google uses data when you use our partners' sites or apps”, (located at www.google.com/policies/privacy/partners/). We may also use Google Analytics Advertising Features or other advertising networks to provide you with interest-based advertising based on your online activity. For more information regarding Google Analytics please visit Google's website, and pages that describe Google Analytics, such as www.google.com/analytics/learn/privacy.html.

Article III. POLICIES ON USE AND DISCLOSURE OF PERSONAL DATA

We use your Personal Data for various purposes described below, including to:

- provide our Website or Application to you;
- provide products and services to you;
- provide you with information you request from us;
- enforce our rights arising from contracts;
- notify you about changes; and,
- provide you with notices about your account.

III.1. We use information that we collect about you or that you provide to us, including any Personal Data:

(a) to present our Website and their contents to you;

(b) to present our Application;

(c) to provide you with information, products, or services that you request from us;

(d) to process, fulfill, and administer transactions and orders for products and services ordered by you;

(e) for marketing, research, advertising, patient education, and/or similar activities;

(f) to contact you in response to a request;

(g) to fulfill any other purpose for which you provide it;

(h) to carry out our obligations and enforce our rights arising from any contracts entered into between you and us;

(i) to notify you about changes to our Website, our Application, or any services we offer or provide though them;

(j) in any other way we may describe when you provide the information;

(k) for any other purpose with your consent, including the rights to use your Personal Data.

III.2. We may disclose Personal Data that we collect or you provide as described in this privacy policy:

(a) to our subsidiaries and affiliates;

(b) to contractors, service providers, and other third parties we use to support our business. The services provided by these organizations include providing IT and infrastructure support services, and ordering, marketing, and other services;

(c) to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar

proceeding, in which Personal Data held by Docademic about our Website and Application users are among the assets transferred;

(d) to fulfill the purpose for which you provide it. For example, we may disclose your personal information to a Provider;

(e) for any other purpose disclosed by us when you provide the information;

(f) with your consent.

III.3. We may also disclose your Personal Data:

(a) to comply with any court order, law, or legal process, including to respond to any government or regulatory request;

(b) to affiliates to market their products or services to you if you have not opted out of these disclosures. For more information, see Choices About How We Use and Disclose Your Information;

(c) to enforce or apply our Terms of Use and other agreements; and

(d) if we believe disclosure is necessary or appropriate to protect the rights, property, or safety of Docademic, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

III.4. We may also use your information to contact you about goods and services that may be of interest to you, including through newsletters. If you wish to opt-out of receiving such communications, you may do so at any time by clicking unsubscribe at the bottom of these communications.

III.5. We may use how you browse and shop in order to show you ads for our advertising partners that are more relevant to your interests. We may use cookies and other information to provide relevant interest-based advertising to you. Interest-based ads are ads presented to you based on your browsing behavior in order to provide you with ads more tailored to your interests. These interest-based ads may be presented to you while you are browsing our site or third party sites not owned by Docademic.

III.6. We do not control the collection and use of your information collected by third parties described above in this Article IV. When possible, these organizations are under contractual obligations to use this data only for providing the services to us and to maintain this information strictly confidential. These third parties may, however, aggregate the information they collect with information from their other customers for their own purposes.

III.7. In addition, we strive to provide you with choices regarding the Personal Data you provide to us. We have created mechanisms to provide you with control over your Personal Data:

III.8. Tracking Technologies and Advertising. You can set your browser or operating to refuse all or some cookies, or to alert you when cookies are being sent. If you disable or refuse cookies, please note that some parts of our Website or Application may then be inaccessible or not function properly

III.9. Promotional Offers from Docademic. If you do not wish to have your email address used by Docademic to promote our own products and services, you can opt-out at any time by

clicking the unsubscribe link at the bottom of any email or other marketing communications you receive from us or logging onto your Background profile page. This opt out does not apply to information provided to Docademic as a result of a product purchase, or your use of our services.

III.10. Targeted Advertising. We belong to ad networks that may use your browsing activity across participating websites to show you interest-based advertisements on those websites. To learn more about interest-based advertisements and your opt-out rights and options, visit the Digital Advertising Alliance and the Network Advertising Initiative websites (www.aboutads.info and www.networkadvertising.org). Please note that if you choose to opt out, you will continue to see ads, but they will not be based on your online activity. We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide you with ways to choose not to have your information collected or used in this way. You can also opt out of receiving targeted ads from members of the NAI on its website.

Article IV. CALIFORNIA PRIVACY RIGHTS

IV.1. California Civil Code Section 1798.100 (The California Consumer Privacy Act ("CCPA")) provides California residents with the right to:

(a) Know what personal data is being collected about them.

(b) Know whether their personal data is sold or disclosed and to whom.

(c) Say no to the sale of personal data.

(d) Access their personal data.

(e) Request a business to delete any personal information about a consumer collected from that consumer.

(f) Not be discriminated against for exercising their privacy rights.

IV.2. The CCPA applies to any business, including any for-profit entity that collects consumers' personal data, which does business in California, and satisfies at least one of the following thresholds:

(a) Has annual gross revenues in excess of $25 million;

(b) Buys or sells the personal information of 50,000 or more consumers or households; or

(c) Earns more than half of its annual revenue from selling consumers' personal information.

IV.3. A "Do Not Sell My Personal Information" link on the home page of the website of Docademic, that will direct users to a web page enabling them, or someone they authorize, to opt out of the sale of the resident's personal information is available

Article V. POLICIES ON USE AND DISCLOSURE OF PHI.

V.1. **Use and Disclosure Defined.** Docademic and the Platform will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

• *Use*. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any Persons with Access of Docademic, by a Business Associate (defined below) of the Platform.

• *Disclosure*. For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons who are not Persons with Access of Docademic.

V.2. **Workforce Must Comply with Company's Policy and Procedures.**

V.3. **Access to PHI is Limited to Certain Employees.** As set forth in Article I, above, only the Persons with Access shall have regular and recurring access to and use of PHI.

Persons with Access may use and disclose PHI for Platform administrative functions, and they may disclose PHI to other Persons with Access for Platform administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the Platform administrative function). Persons with Access may not generally disclose PHI to employees (other than other Persons with Access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy.

V.4. **No Disclosure of PHI for Non-Health Platform Purposes. PHI** may only be disclosed to Providers for health care purposes only, unless you have provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

V.5. **Mandatory Disclosures of PHI to Individual and HHS.** A participant's PHI must be disclosed as required by HIPAA in two situations:

• The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Health Information and Requests for Amendment", below); and

• The disclosure is made to HHS for purposes of enforcing HIPAA.

V.6. **Permissive Disclosures of PHI for Legal and Public Policy Purposes.** PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The permissive disclosures are:

• about victims of abuse, neglect or domestic violence;

• for judicial and administrative proceedings;

• for law enforcement purposes;

• for public health activities;

• for health oversight activities;

• about decedents;

• for cadaveric organ, eye or tissue donation purposes;

• for certain limited research purposes;

• to avert a serious threat to health or safety; and

• for specialized government functions.

V.7. **Disclosures of PHI Pursuant to an Authorization.** PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. The Contact Person will have a supply of the authorization form.

V.8. **Complying with the "Minimum-Necessary" Standard.** HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure, as determined by the Privacy Official case-by-case, or, in the instance of routine and recurring disclosures, as set forth in the Uses and Disclosures Policy.

The "Minimum Necessary" Standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to the DOL;
- uses or disclosures required by law;
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For routine and recurring disclosures developing prospectively, the Privacy Official (or Contact Person if directed by the Privacy Official) will direct an analysis of such disclosures and further, specific standards will be developed.

All other disclosures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

V.9. **Disclosures of PHI to Business Associates.** Persons with Access may disclose PHI to the Platform's business associates and allow the Platform's business associates to create or receive PHI on its behalf. However, prior to doing so, the Platform must first obtain assurances from the business associate (in the form of business associate agreements) that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate", employees must contact the Contact Person and verify that a business associate agreement is in place.

A "Business Associate" is an entity or person who:

- performs or assists in performing a Platform function or activity involving the use and disclosure of protected health information (including claims processing or administration; data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services to the Platform, where the performance of such services involves giving the service provider access to protected health information.

V.10. **Disclosures of De-identified Information and Limited Data Sets.** The Platform may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis

to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers under HIPAA.

V.11. **Policies Specific to E-PHI/Security Rule.** Docademic has performed a risk analysis and assessment and developed a document called the HIPAA Security Risk Analysis and Assessment document, including recommended administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of electronic PHI Docademic creates, receives, maintains or transmits.

[List specific administrative, physical and technical safeguards as suggested by Security Rule Evaluation and Assessment document.]

Article VI. Policies on Individual Rights.

VI.1. **Access to Protected Health Information and Requests for Amendment.** HIPAA gives participants in the Platform the right to access and obtain copies of their PHI that the Platform (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Platform will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants as set forth in the Notice of Privacy Practices.

VI.2. **Accounting.** An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for national security or law enforcement purposes.

The Platform shall respond to an accounting request within 60 days. If the Platform is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Contact Person may impose reasonable production and mailing costs for subsequent accountings.

VI.3. **Requests for Requested Confidential Communications.** Participants may request to receive communications regarding their PHI by alternative means or at alternative

locations. Such requests shall be honored if, in the sole discretion of Docademic, the requests are reasonable.

However, Docademic shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Contact Person has responsibility for addressing requests for confidential communications.

VI.4. **Requests for Restrictions on Uses and Disclosures of PHI.** A participant may request restrictions on the use and disclosure of the participant's PHI. It is Docademic's policy to attempt to honor such requests if, in the sole discretion of Docademic, the requests are reasonable. The Contact Person is charged with responsibility for addressing requests for restrictions.

VI.5. **Requests for Amendment.** No third-party rights (including, but not limited to rights of Platform participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. Docademic reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon Docademic. This Policy does not address requirements under other Federal laws or under state laws.

Article VII. DO NOT TRACK SIGNALS

VII.1. We also may use automated data collection technologies to collect information about your online activities over time and across third party websites or other online services (behavioral tracking). Some web browsers permit you to broadcast a signal to websites and online services indicating a preference that they "do not track" your online activities. At this time, we do not honor such signals and we do not modify what information we collect or how we use that information based upon whether such signal is broadcast or received.

Article VIII. DATA SECURITY

VIII.1. We have implemented measures designed to secure your Personal Data from accidental loss and from unauthorized access, use, alteration, and disclosure. We use encryption technology for information sent and received by us.

VIII.2. The safety and security of your information also depends on you. Where you have chosen a password for the use of our Application, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

VIII.3. Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your Personal Data, we cannot guarantee the security of your Personal Data transmitted to our Website or on or through our Application. Any transmission of Personal Data is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the Website, in your operating system, or in the Application.

Article IX. LOCATION-ENABLED FEATURES

IX.1. Certain location-enabled functionality made available in the Website and Application is provided by Google, Apple Inc., and other third party providers. Your use of that functionality may be subject to additional privacy (and other) terms and conditions (as updated from time-to-time), including the terms that are accessible through: http://www.google.com/intl/en-US_US/help/terms_maps.html and https://www.apple.com/legal/internet-services/maps/terms-en.html. You must exercise your own judgment as to the adequacy and appropriateness of the sharing of this information with us.

Article X. CHANGES TO OUR PRIVACY POLICY

X.1. We may change this Privacy Policy at any time. It is our policy to post any changes we make to our Privacy Policy on this page with a notice that the Privacy Policy has been updated on the Website's home page or the Application's home screen. If we make material changes to how we treat our users' Personal Data, we will notify you by email to the email address specified in your account and/or through a notice on the Website's home page or the Application's home screen. The date this Privacy Policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable email address for you, and for periodically accessing the Application or visiting our Website and reviewing this Privacy Policy to check for any changes.

Article XI. CONTACT INFORMATION

XI.1. If you have any questions, concerns, complaints or suggestions regarding our Privacy Policy or otherwise need to contact us, you may contact us at the contact information below or through the "Contact" page on our Website or in the Application.

XI.2. How to Contact Us: Docademic, Inc., 800 SE 4th Avenue, Suite 710, Hallandale Beach, FL, 33009 Email: support@doc.com