PRIVACY AND SECURITY POLICY AND PROCEDURE

I. PURPOSE

The Health Insurance Portability and Accountability Act ("HIPAA") creates national standards to protect an individual's medical records and other personal health information. The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") amends the Rules (as defined below), which requires Covered Entities to implement appropriate administrative, technical, and physical safeguards to reasonably safeguard Protected Health Information ("PHI") (as defined below) and electronic Protected Health Information ("e-PHI") from any intentional or unintentional use or disclosure that violates the Rules. Dallas Anesthesiology Associates, P.A. ("DAA") is a Covered Entity (as defined below) under the HIPAA regulations and as such, must comply with all applicable HIPAA and HITECH Act requirements. The purpose of this policy is to establish guidelines for DAA and its physicians and employees (collectively referred to herein as "Members") to comply with the HIPAA and HITECH Act regulations.

II. POLICY

It is DAA's policy to comply with the HIPAA and HITECH Act regulations and to establish written policies and procedures to assist its Members in doing so. DAA Members shall take reasonable steps to safeguard PHI and e-PHI and to limit any use, disclosure, or request for PHI to the Minimum Necessary (as defined below) to accomplish the intended purpose.

III. PROCEDURE

A. Definitions

1. Covered Entity: Individuals or entities that are required to comply with the HIPAA regulations, including: health plans, healthcare clearinghouses, and healthcare providers who transmit any health information in electronic form, including but not limited to, the following types of information transmissions: (a) healthcare claims or equivalent encounter information; (b) healthcare payment and remittance advice; (c) healthcare claim status; (d) health plan premium payments; (e) health claims attachments; and/or (f) referral certification and authorization.

2. Business Associate: An individual who, or an entity that, on behalf of a Covered Entity:

    a. performs or assists in the performance of a function or activity involving the use or disclosure of Protected Health Information, or

    b. provides management, administrative, accreditation, billing or financial services to or for a Covered Entity where the provision of the service involves the disclosure of Protected Health Information from the Covered Entity, or from another Business Associate of such Covered Entity.

3. Minimum Necessary: The amount of information reasonably required for the performance of a given task or service, and no more. The Minimum Necessary

standard is not intended to impede essential treatment, payment, or healthcare operations activities of Covered Entities. The standard is intended to be consistent with, and not override, professional judgment and standards.

4. Organized Health Care Arrangements ("OHCA"): A clinically integrated care setting in which individuals typically receive healthcare from more than one healthcare provider; and an organized system of healthcare in which more than one covered entity participates, and in which the participating covered entities (a) hold themselves out to the public as participating in a joint arrangement; and (b) participate in joint activities that include at least one of the following (i) utilization review, (ii) quality assessment and improvement activities, or (iii) payment activities.

5. Privacy Rule and Security Rules ("Rules"): 42 CFR Parts 160 and 164. The regulations that set forth the federal standards for privacy and security of individually identifiable information and provide a "floor" of privacy protection.

6. Protected Health Information ("PHI"): Any information created or received by a Covered Entity that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, which identifies the individual or, with respect to which, there is a reasonable basis to believe the information can be used to identify the individual. **Exhibit A** contains some examples of PHI.

B. Uses and Disclosures of PHI

1. Minimum Necessary

a. When using or disclosing PHI or when requesting PHI from another Covered Entity, a Covered Entity must make reasonable efforts to limit PHI to the Minimum Necessary to accomplish the intended use, disclosure, or request.

b. The Privacy Rule permits a Covered Entity to make its own assessment of what the Minimum Necessary PHI is for a particular purpose given the characteristics of its business and workforce. All DAA disclosures of or requests for PHI for payment or operations will be limited to the Minimum Necessary amount of PHI needed to accomplish the purpose of the disclosure or request. In addition, disclosure by DAA will be limited to those with "a need to know" to carry out their duties.

c. A Covered Entity is permitted to reasonably rely on the request of another Covered Entity for PHI because the requesting Covered Entity is itself subject to the Minimum Necessary standard, and, therefore, required to limit the request to only that information that is reasonably necessary for the intended purpose. In addition, and in accordance with 42 CFR §164.514(d)(3)(iii), DAA may reasonably rely on a requested use or disclosure as the Minimum Necessary when:

i. making disclosure to public officials that are permitted under 42 CFR

§164.512; or

ii. the information is requested by a DAA Business Associate.

d. The Minimum Necessary rule does not apply when disclosures are made to or requested by a healthcare provider for treatment.

2. Disclosure Accounting

DAA will track all PHI disclosures that must be accounted for under the Privacy Rule. An accounting of these disclosures will be given to individuals upon their request, in accordance with 42 CFR §164.528. Disclosures subject to the accounting rule include: (a) incidental disclosures due to a breach of the Minimum Necessary rules, or the administrative, technical, or physical safeguards set forth in 45 CFR §164.530; (b) disclosures to report information to a public health or health oversight agency; (c) disclosures as required by law; (d) disclosures for judicial or administrative proceedings, including pursuant to a subpoena; (e) disclosures made in compliance with workers' compensation laws and proceedings; and (f) disclosures made pursuant to a defective authorization.

3. Authorizations

It is DAA's policy that a valid authorization, as defined in 45 CFR §164.508, will be obtained for all disclosures by DAA, except for disclosures made:

a. for treatment, payment, or healthcare operations;

b. to the individual or their personal representative;

c. to persons involved with the individual's care;

d. to Business Associates in performance of their legitimate duties; or

e. as required for public health activities and set forth in 45 CFR § 164.512.

Any authorization requests that are generated outside of DAA will be checked to ensure they contain the required core elements and statements as defined by 42 CFR §164.508(b)(1), including an expiration date or event and a statement that the authorization is revocable.

4. Marketing Activities

DAA does not use or disclose PHI for marketing purposes. For the purpose of this policy, marketing is defined as any communication from DAA to purchase or use a product or service in exchange for direct or indirect remuneration, or where DAA encourages purchase or use of a product or services. DAA does not consider the communication of alternate forms of treatment, or the use of products and services in treatment, to be marketing.

DAA does not disclose PHI in exchange for financial remuneration, except as specifically allowed by law (e.g. when collecting a reasonable, cost-based fee for providing copies of medical records to the individual or to a third party pursuant to the individual's authorization). DAA does not use or disclose PHI for fundraising purposes.

5. Judicial and Administrative Proceedings

   DAA discloses PHI for the purposes of a judicial or governmental administrative proceeding only when: (a) requested pursuant to a court or administrative order or grand jury subpoena; (b) requested pursuant to a subpoena or discovery request; or, (c) pursuant to a qualified protective order issued by a court. Further, it is DAA's policy that PHI be disclosed only when requested by any of the above-listed means, if such request includes either: (i) the authorization of the individual to whom the information applies; or, (ii) documented assurances that good faith effort has been made to adequately notify the individual of the request for their information; or, (iii) the applicable time for objection to such request for PHI has reasonably expired.

C. Notice of Privacy Practices

DAA physicians participate in one or more OHCA at the facilities where they practice and, accordingly, meet the HIPAA Notice of Privacy Practices ("Notice") requirements through the use of a joint Notice. Nevertheless, DAA maintains a Notice that describes the way in which it uses and discloses PHI. DAA distributes its Notice to patients upon their request. Should a situation arise where DAA physicians are not covered by a facility's Notice, DAA will work with the facility to establish a process for distribution and tracking of DAA's Notice.

D. Individual Access to PHI and Restrictions on Disclosure and Amendments

1. Individual Requests

   a. Restriction on Uses and Disclosures of PHI. The Privacy Rule grants each individual the right to request restriction of the uses and disclosures of his or her PHI to carry out treatment, payment, or healthcare operations, although DAA is not required to grant this request. For instance, a patient may request that certain medical information not be included on the billing ticket sent to the billing company. DAA may deny this request if the information is necessary for payment purposes. If DAA agrees to the restriction, the restriction must be appropriately documented and DAA's billing company must be notified of the restriction.

   b. Restriction on Uses and Disclosures of PHI (Out-of-Pocket Paid Items and Services). The Privacy Rule requires that a Covered Entity restrict disclosures of PHI to an individual's health plan if: (i) the disclosure is for the purpose of carrying out payment or healthcare operations (and is not otherwise required by law); and, (b) the information pertains only to a healthcare item or service for which the individual (or a person other than the health plan) paid the Covered Entity in full. DAA will abide by such requests for disclosure restriction.

c. Confidential Communications of PHI. The Privacy Rule grants individuals the right to request communication of PHI by alternative means or to an alternative location. DAA will accommodate reasonable requests. For example, if a patient requests that the DAA physician make his or her follow-up phone call to the patient's cell phone, rather than a home phone, the physician should honor that request.

If a DAA physician agrees to a request, he or she will make every effort to abide by this agreement, unless unable to do so in case of emergency. When appropriate, the DAA physician should document any requests agreed to in the comments section of the DAA charge ticket, so the billing company can also comply with the requests.

2. Access by Personal Representatives

It is DAA's policy that access to PHI must be granted to personal representatives of individuals as though they were the individuals themselves, except in cases of abuse where granting such access might endanger the individual or another person. DAA will conform to the relevant custody status and the strictures of state, local, case, and other applicable law when disclosing information about minors to their parents.

3. Individual Access to Records

As DAA does not physically possess medical or billing records, it is the group's policy to inform the individual requesting access regarding the location of the PHI if DAA has knowledge of the location.

4. Requests for Amendment of Incomplete or Incorrect PHI

a. Amendment of Incomplete or Incorrect PHI - Individual Request. The Privacy Rules permits individuals to request the amendment of incorrect PHI. As DAA does not physically possess patient medical or billing records, the patient should be directed to make these requests to the healthcare facility or DAA's billing company, as applicable, based on whichever entity is in possession of the pertinent records. If the patient's request pertains to the amendment of a record or document owned and under the control of DAA, then DAA will review and respond to the request and make revisions to the applicable record or document, as appropriate.

b. Amendment of Incomplete or Incorrect PHI - Hospital Request. DAA physicians will review a patient amendment request if asked to do so by the hospital and make recommendations or amendments, as appropriate.

5. PHI of Deceased Individuals

DAA may disclose to a family member, other relative, or a close personal friend who was involved in the patient's care or payment for healthcare prior to the patient's death, PHI that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the patient that is known to DAA. DAA will comply with this requirement as well as the other requirements set forth in

this policy with respect to disclosure of PHI.

E. DAA Operations

DAA ensures that appropriate physical safeguards are in place to (a) reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the Privacy Rule; (b) ensure the confidentiality, integrity and availability of e-PHI it creates, receives, maintains or transmits; and (c) protect against reasonably anticipated uses or disclosures that violate the Rules. These safeguards include technical protection (i.e. password protection and encryption) of PHI maintained electronically, and also apply to PHI that is removed from a healthcare facility, such as anesthesia records, billing reports, and billing tickets. DAA Members will adhere to the "Practical Guidance for Protecting PHI" as outlined in **Exhibit A**.

1. DAA Member Access to PHI

DAA access to PHI, for operations or payment purposes, is granted to each DAA Member and officer based on the assigned job functions of the individual. These access privileges will not exceed those necessary for the job function or task.

2. Training and Awareness

DAA requires all its Members complete annual HIPAA compliance training. Members who fail to fulfill this training requirement are subject to disciplinary action, in accordance with DAA's Compliance Plan and/or Employment Contract. New DAA Members will receive HIPAA training as a component of their initial orientation.

3. Physical Safeguards

DAA ensures that appropriate physical safeguards are in place to reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the Privacy Rule. These safeguards include both physical and electronic protection of PHI, and also apply to PHI that is removed from a healthcare facility, such as anesthesia records, or an administrative office or billing company.

Oral communication must also be appropriately safeguarded. When Members engage in conversations where PHI is discussed, they should take appropriate precautions to minimize the possibility of being overheard. **Exhibit A** contains examples of PHI that are relevant to DAA Members.

4. Removal and Transport of Hardware and Electronic Media Containing e-PHI

Members shall limit to the extent reasonable, the removal of tablets, cell phones, laptops, USB drives, CD's/DVD's, and storage/backup drives from its offices and facilities, and in the case of removal, the Member will ensure safety measures are utilized, such as encryption and password protection. Each Member shall limit the use of cell phones and tablets that contain PHI and implement safeguards as set forth herein.

Each Member may maintain their personal laptops, tablets, cell phones to use for work related to DAA. All laptops, tablets, cell phones, USB drives, storage drives, CD's, DVD's, or other electronic media that is used to store PHI shall be encrypted, if possible, or, at a minimum, password protected if the software program does not support encryption.

In the event of loss or theft, the Member shall either wipe or lock the device immediately, or immediately contact the service with which it is registered and instruct that service to lock or wipe the device if possible. Additionally, if the device allows it, the Member shall establish settings on the cell phone or tablet that wipe all data from the device after a specified number failed log-in attempts.

Any loss or theft of any electronic devices or media containing e-PHI must be immediately reported to the DAA's Privacy and Security Officer ("Privacy Officer") or Compliance Officer.

5. Safeguard e-PHI in the Event of Remote Access

   Members shall not remote access into a facility or other entity, which maintains e-PHI for any reason other than treatment, payment, or healthcare operations.

   For any home computers or devices that access e-PHI at work, two passwords shall be required that are not divulged to anyone else. The first password shall be a log-in and password into the computer that is separate and distinct from any other log-in password for all other users of the home device.

   Upon exiting any remote session, the user will terminate the remote session so that it does not remain open. Upon leaving the computer or electronic access device, the user will log out of the computer, so no one else can access the user's access device.

6. Secure e-PHI Transmitted via Email and Other Web-based Services

   Web-based services such as Gmail, Yahoo mail, Hotmail, and AOL, may not be secure, and therefore, Members shall not use non-office, web-based services to send or receive e-PHI related emails that are not encrypted. Emails containing e-PHI are unsecure unless encrypted.

   Each Member who sends or receives e-PHI from abeo Management Corporation ("abeo") will do so using approved secure email encryption software. This will ensure protection of e-PHI by using the secure network provided by abeo. If such account is not accessible, the Member may use an unsecure email account only if the communication is encrypted. For example, if the email contains a pdf attachment with PHI, the Member must use Adobe Acrobat to encrypt the attachment with a password, in which case, the password will be sent to the recipient via a separate email from the email containing the encrypted pdf.

7. Prohibited Activities

DAA and its Members are prohibited from engaging in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA regulations.

8. Document Retention and Destruction

   DAA documents all policies and procedures adopted to protect the privacy of PHI. Policies and procedures, and any other information required by 42 CFR § 164.530(j)(1) to be maintained in writing or electronically, will be retained in accordance with DAA's record retention policy. DAA destroys documents containing PHI through shredding or other means which safeguards their confidentiality.

9. Business Associates

   The Privacy Rule does not require DAA to actively monitor the actions of its Business Associates. Rather, it requires that, where a Covered Entity knows of a pattern of activity or practice that constitutes a material breach or violation of the Business Associate's obligations under its contract with the Covered Entity, the Covered Entity take steps to cure the breach or end the violation. Accordingly, DAA requires its Business Associates to be contractually bound to safeguard PHI. Business Associates who violate their agreement will be required first to correct the problem. If the Business Associate is unable to cure the breach or end the violation, DAA will terminate the agreement (if feasible) and report the privacy breach to the Department of Health and Human Services, as required by 42 CFR § 164.504(e)(1)(ii).

10. Cooperation with Privacy Oversight Authorities

    DAA will cooperate with oversight agencies, such as the Office for Civil Rights, in their efforts to ensure the protection of health information within DAA. DAA Members will cooperate with all privacy compliance reviews and investigations, which should be directed to DAA's Privacy Officer.

11. Sanctions

    DAA may impose disciplinary action, up to and including termination, upon Members who intentionally or unintentionally violate the requirements outlined in this or any of DAA's other related policies. **Exhibit A** contains a list of general practices that Members should follow in order to comply with the HIPAA regulations.

12. Privacy Officer

    DAA has designated one of its Members as its Privacy Officer. **Exhibit B** contains contact information for the Privacy Officer or his/her designee(s).

13. Audits

    As a Covered Entity, DAA may be subject to a HIPAA audit by the Secretary of the Department of Health and Human Services (or his/her designee). It is DAA's policy to cooperate with such HIPAA audits. DAA members should immediately report receipt

of any documents related to a HIPAA audit of DAA to the Privacy Officer.

III. EXCEPTIONS and LIMITATIONS

A. A Covered Entity may disclose PHI to a family member or other person involved in the individual's care. Where the individual is present during a disclosure, the Covered Entity may disclose PHI if it is reasonable to infer from the circumstances that the individual does not object to the disclosure.

B. The Privacy Rule permits certain incidental uses and disclosures that occur as a result of a use or disclosure otherwise permitted by the Rules. The incidental use or disclosure is permissible only to the extent that the Covered Entity has applied reasonable safeguards to PHI, and implemented Minimum Necessary standards. For example, two physicians who are conferring about a patient at a nurses' station do not have to fear violating the Privacy Rule if they are overheard by a passerby, as long as the physicians make reasonable efforts to avoid being overhead and reasonably limit the information shared.

C. State laws that are more stringent than the Privacy Rule take precedence over the federal regulations.

D. The Privacy Rule does not apply to employers, nor does it apply to the employment functions of Covered Entities, namely, when they are acting in their role as employers. Employment records are exempt from the definition of PHI. For example, information in a DAA Member's personnel file about a leave of absence due to illness is not PHI under the Rules. Similarly, drug-screening test results sent to DAA and placed in the Member's personnel file are not considered PHI.

IV. REFERENCE

A. 45 CFR Part 160 and 164

Exhibit A

Examples of Protected Health Information

1. Conversations about a patient's health
2. Patient dictation on tape
3. Charge Ticket/Patient Bill
4. Anesthesia record
5. Emails with patient name (or other identifiers, such as date of birth, address, phone number or email) and health information
6. Electronic equipment or digital media (if patient data is stored). Some examples include, cell phones, laptops, tablets, thumb drives and recordable discs.

Practical Guidance for Protecting PHI

1. Disclose only the minimum necessary information for people to do their jobs.
2. Avoid discussions about patients in public places.
3. Avoid placing PHI in view of other patients or family members.
4. Password protect your mobile electronic devices ("PDAs"), laptops, and home computers if PHI is stored there.
5. Don't leave your PDAs or laptops unattended in the hospital and don't leave PHI visible on your computer screen.
6. Be certain that your papers and computer equipment are physically secure in your home, car, or other "off-site" locations. Do not leave your briefcase in plain sight within your car; secure it in the truck of the car and remove it from the car (to a more secure location) as soon as possible.
7. Don't send emails with PHI unless they are encrypted or you are using a secure network.
8. Don't put PHI in trash or recycle bins; use only shredding or other document destruction receptacles.
9. Verify fax numbers before you send faxes with PHI. Verify mailing address before mailing or shipping documents or devices with PHI.
10. Report any privacy or security breaches by DAA Members or DAA business associates to the DAA's Privacy Officer.

Exhibit B

Privacy and Security Contacts Sheet

DAA COMPLIANCE OFFICER

Amy Ripley, M.D., Compliance and Privacy Officer
E-mail: amy.ripley@daadoctors.com