

## DATA PRIVACY AND SECURITY POLICY

### 1.0 Introduction

In the course of application, examination, certification, recertification, and Maintenance of Certification processes (collectively, "Certification Processes"), the American Board of Anesthesiology, Inc. (ABA) must collect and utilize personal and professional information pertaining to its applicants and diplomates. The ABA has issued the following Data Privacy and Security Policy to govern the collection, use, and disclosure of such information, and the ABA's policies and practices regarding the privacy of information during the Certification Processes. The goal of establishing this privacy policy is to assure all persons disclosing information to the ABA of the sensitivity and care utilized in protecting this information. The Chief Information Officer is responsible for reviewing, maintaining and monitoring the compliance of the data privacy and security procedures.

### 2.0 Use and Disclosure of Personal Information

In order to determine the qualifications of applicants during the application and certification processes, the ABA requires that applicants and diplomates provide personal contact and identifying information, as well as personal, educational, and professional background information. This information is used by the ABA to identify and determine an applicant's or diplomate's appropriate status with the ABA.

In connection with the registration and administration of its examinations, the ABA requires an applicant's or diplomate's personal information, including name, mailing address, and social security number. Social security numbers are used only as an individual identifier. The ABA restricts access to such personal information to ABA employees and contractors who need this information to conduct the registration, administration, and scoring of examinations, and for the verification of certification by the ABA.

The ABA does not disclose any personal information regarding its applicants or diplomates to non-ABA employees and contractors, except when required by law (such as complying with a subpoena or court order) or as described below for the American Board of Medical Specialties (ABMS). The ABA does not share personal information about its applicants or diplomates with companies or other third parties outside of the ABA for marketing purposes. The ABA considers only the certification, recertification, or Maintenance of Certification status of applicants and diplomates to be public information and regards all other information about applicants and diplomates as private and confidential.

Upon certification and recertification, the ABA provides basic biographical and demographic data on diplomates to the ABMS, which publishes The Official ABMS Directory of Board Certified Medical Specialists. The ABMS will directly contact diplomates regarding the publication of diplomate information in its directory. ABA diplomates will communicate directly to the ABMS the personal information that they wish to appear in the directory.

The ABA provides residency program directors with the results of their residents' performance on specific ABA examinations. Individual examination results are not provided to any other person or institution. The ABA will use performance on examinations and other information for research purposes and may

publish these studies. In these instances, however, the ABA will not identify specific individuals, hospitals, or practice affiliations.

The ABA provides summary information for specific residency programs regarding the collective performance of residents on ABA examinations to the Residency Review Committee for Anesthesiology. In the interests of better informing medical students regarding anesthesiology training, this information will be provided to the public via the ABA website.

The ABA reserves the right to disclose information in its possession regarding any individual whom it determines, in its sole and absolute discretion, is involved in a violation of ABA rules or procedures or engaged in misrepresentation or unprofessional behavior or any other illegal activity. Such determinations may include statistical analyses of examination responses.

### **3.0 Protection of Personal Information**

The ABA maintains physical, electronic, and procedural safeguards to protect and secure all personal information in its possession. The ABA's security measures protect the confidentiality of online communication, examination results, and data related to the application or certification processes. The ABA uses encrypted technology for the sensitive communications performed. Examination results and sensitive applicant and diplomate data transmissions are encrypted and stored in secure areas of ABA systems accessible only by authorized ABA personnel with a unique ID and password.

ABA database servers used for transactions and communication with applicants and diplomates are stored in a restricted, secure area accessible only to authorized personnel. Firewalls and monitoring devices are installed that are designed to prevent unauthorized network access via the Internet.

### **4.0 HIPAA Privacy Rules**

The U.S. Department of Health and Human Services finalized regulations regarding privacy protections for certain health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As part of the certification process, the ABA may require an applicant to submit patient information that could be governed by HIPAA and its regulations.

The ABA requires that all patient information that is forwarded as part of the application or certification processes be "de-identified" in accordance with the HIPAA privacy regulations so that all identifying information and markers that could be used to reasonably identify a patient are removed before it is forwarded to the ABA. The ABA will not accept any patient information that has not been de-identified in accordance with the HIPAA privacy regulations. It is the applicant or diplomate's responsibility to de-identify the patient's health information before it is submitted to the ABA. If the ABA receives any information that is not de-identified as part of the application or certification processes, the ABA will return such information to the applicant so that it can be appropriately de-identified. This may delay ABA consideration of that applicant or diplomate during the application and certification processes. The ABA cannot and will not be responsible for the applicant's violation of HIPAA and its regulations. If you have questions regarding de-identification or would like more information regarding de-identification requirements, please contact the ABA.

The ABA is committed to the privacy of patient information submitted by its applicants and diplomates during the application and certification processes. The ABA is not a "covered entity" under HIPAA and is not subject to the HIPAA regulations. Because the ABA will not accept patient information that has not been de-identified, the ABA is not a "business associate" of an applicant or diplomate and the ABA will not execute a business associate agreement with an applicant or diplomate.

## 5.0 Notification

The ABA takes all reasonable precautions to ensure that personal information is never exposed to any unauthorized person. In the unlikely event that an unauthorized party gains access to personal information stored in the ABA's computer systems, the ABA will notify the affected person(s) without unreasonable delay and consistent with the legitimate needs of law enforcement, pursuant to North Carolina law 75-65 "Protection from security breaches". In this event, the ABA will take all necessary steps to determine the scope of the breach and restore our systems to a reasonable level of security.

See [here](#) for more information on North Carolina General Statute 75-65.

Updated: February, 2011