Northern Colorado Anesthesia Professionals

HIPAA PRIVACY POLICIES & PROCEDURES

Effective as of January 1, 2022

TABLE OF CONTENTS

INTRODUCTION AND KEY DEFINITIONS

Index: P-01

1. PURPOSE

These Privacy Policies and Procedures summarize the permitted uses and disclosures of patient protected health information ("PHI") as permitted by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule" or the "HIPAA Privacy Rule"), as amended by the Health Information Technology for Economic and Clinical Health Act, which is at Section 13400, et seq. of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. § 17921, et seq., (the "HITECH Act") and any regulations promulgated thereunder, including the HIPAA omnibus final rule (the "HIPAA Final Rule").

2. SCOPE

These Policies and Procedures apply to all Company staff members.

3. PRIVACY POLICY STATEMENT

The Company is committed to complying with the Privacy Rule.
The Company recognizes the need to protect the privacy of PHI in order to facilitate the effective delivery of health care. These Privacy Policies and Procedures are designed and intended to ensure[1] the Company's compliance with the Privacy Rule. The Company adopts these Policies and Procedures to protect the PHI that it maintains from unauthorized use, disclosure, or access, and to maintain the confidentiality and integrity of that PHI. These Policies and Procedures also ensure that individuals have rights related to their PHI.

4. KEY DEFINITIONS

"**Company**" means Northern Colorado Anesthesia Professionals, PLLC and its affiliates and subsidiaries, as applicable.

"**Covered Entity**" means a health plan, a healthcare clearing house, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

"**Protected Health Information**" is information that (1) identifies (or could be reasonably used to identify) an individual, (2) is created or received by a HIPAA covered entity (a health care provider, health plan or health care clearinghouse) and (3) relates to the past, present or future physical or mental health of the individual, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual.

A "**Business Associate**" is a person or entity, other than a member of Company's workforce, that creates, receives, maintains or transmits PHI on behalf of a Covered Entity or Company for a function or activity regulated by HIPAA. The HIPAA Final Rule expands the definition of "business associate" to include subcontractors to a business associate that create, receive, maintain or transmit PHI on behalf of a business associate. Business associate functions or activities on behalf of a covered entity include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing.

These Policies and Procedures will be amended and/or supplemented as necessary and appropriate to comply with changes in the law or regulations or other interpretation of the Company's privacy-related

obligations, or to reflect changes related to the Company. The Company will document and implement changes to these Policies and Procedures whenever there is a change in the law, regulations or interpretation of the Company's privacy obligations and/or a material change to the uses or disclosures of PHI or other privacy practices that necessitate a change in these Policies and Procedures. These Policies and Procedures are effective as of January 1, 2022.

---

[1] The term "ensure," as used throughout these Policies and Procedures, is not meant to guarantee compliance with the Privacy Rule. Rather, "ensure" shall mean that Company and its employees and contractors, as applicable, will use their best efforts to comply with the Privacy Rule.

PERSONNEL DESIGNATIONS

Index: P-02

1. POLICY

The Company has designated a Privacy Officer.

2. PROCEDURE

2.1 **PRIVACY OFFICER DESIGNATION.** The Company has designated a Privacy Officer who is responsible for overseeing and directing the development and implementation of the Company's Privacy Policies and Procedures in compliance with the Privacy Rule.

(a) **Designated Privacy Officer.** The Company has designated the following Privacy Officer:

Anne C. Weddle, J.D.
3702 Automation Way, #103
Fort Collins, CO 80525
complianceofficer@ncaphealth.com
970.999.0278

(b) **Duties and Responsibilities.** The Privacy Officer is responsible, either directly or by his/her delegated authority, for monitoring and ensuring the Company's compliance with the Privacy Rule requirements and these Policies and Procedures.

The Privacy Officer:

(i) Oversees the development and implementation of HIPAA compliance processes, and supervises the day-to-day aspects of compliance with the Privacy Rule;

(ii) Coordinates with Company employees to identify HIPAA non-compliant processes and systems, and to develop and implement those changes necessary to ensure all processes and systems are HIPAA compliant;

(iii) Serves as central liaison for internal HIPAA systems and processes, and for external business partners and vendors involved in HIPAA systems and processes;

(iv) Communicates HIPAA compliance assessment findings, including cost and risk exposure, to the Company and impacted personnel;

(v) Tracks action items;

(vi) Prepares budgets for HIPAA compliance as necessary and appropriate;

(vii) Responds to inquiries from individuals, government officials and other third parties regarding uses and disclosures of PHI, and promptly renders determinations in response to such inquiries and requests;

(viii) Oversees workforce training on HIPAA compliance;

(ix) Maintains a current list of Business Associates;

(x) Responds to inquiries from individuals about the Company's privacy procedures;

(xi) Investigates any complaints that allege that any Company employee or a Business Associate has not complied with or has violated these Policies and Procedures;

(xii) Investigates and conducts risk assessments related to any breach of the Privacy Rule to determine whether notification of breach is required and, as appropriate and necessary, provides such notification;

(xiii) Oversees document maintenance and retention policies; and

(xiv) Reviews and revises Company's HIPAA Policies and Procedures as required or needed to ensure continued compliance with the Privacy Rule and any other applicable law.

2.2 **DOCUMENTATION.** Documentation related to these personnel designations will be retained for 6 years.

RESTRICTED INTERNAL ACCESS TO PROTECTED HEALTH INFORMATION

Index: P-03

1. POLICY

The Company has implemented reasonable safeguards, including appropriate administrative, technical and physical measures, to protect the privacy of protected health information ("PHI"), and to prevent impermissible uses and disclosures of PHI. The Company has limited access to PHI to only those Company employees who need to use or disclose PHI to carry out their duties.

2. PROCEDURE

2.1 **LIMITED EMPLOYEE ACCESS.** Access to PHI is limited to the following Company employees for the purpose(s) described herein.

(a) **IT Employees.** Information technology ("IT") employees provide technical support to Covered Entities performing functions that involves PHI.

(b) **Operations Department.** Operations Department employees provide patient and provider scheduling and service management.

(c) **Finance Department.** Finance Department employees provide analytical and data services related to provider services to patients.

(d) **Executive Leadership Team.** The executive leadership team oversees all Company operations, including various patient and patient care related issues.

2.2 **ACCESS CONTROLS AND PHYSICAL PROTECTIONS**

(a) **Physical Layout and How Hardcopy PHI is Handled**

(i) **"Clean Desk" Rule.** To the extent that Company employees maintain paper documents containing PHI, they will observe a "clean desk" rule with respect to such materials, including: (i) keeping such materials on their desktop only when in use; (ii) turning documents face-down on their desktop whenever possible; and (iii) at the end of each workday, putting all such materials away in their desk and locking the door to any office containing PHI. During any extended periods away from his or her desk, such as during a lunch break, an employee will place materials containing PHI in a locked drawer.

(ii) **Locked File Cabinets/Desk Drawers.** To the extent possible, hard copy PHI will be maintained in filing cabinets or desk drawers, which are locked when not in use.

(b) **Secure Equipment**.

(i) **Computer Security**

(1) **Email Security.** To the extent practicable, Company employees should avoid emailing or otherwise sharing PHI in electronic form, except as expressly authorized by their supervisor or by Company's policies and procedures. If a Company employee must send an email containing PHI, the email should contain the minimum amount of PHI necessary to accomplish the work task.

(2) **Password Protection**. All Company desktop computers and laptops will be password-protected, utilizing reasonably strong passwords (e.g., at least 8 characters with at least one capital letter and at least one symbol or numeral, etc.).

(3) **Screen-Savers and Automatic Log-off**. Company desktop computers and laptops will utilize screen-savers that will be activated, along with automatic log-off, when the computer is inactive after 20 minutes.

(4) **Device Encryption**. Company employees should never disable device encryption software used by the Company, and should enable all updates to such device encryption software provided by the Company.

(ii) **Portable Devices**.

(1) **Taking Laptops Home.** Company employees are permitted to take their laptops home, but must never leave laptops unattended at home or in transit. Employees should never leave a laptop in an unlocked room or car, nor should a laptop ever be left in plain sight in a locked car.

(2) **Securing Laptops.** Company employees must never leave their laptops unattended or unsecured. At the end of the workday, employees should ensure that their laptop is stored in a locked drawer or attached to a locked cable.

(3) **Fax Machines.** When practicable, Company employees will call ahead to make sure that the appropriate person is available to receive a fax containing PHI. Incoming faxes, particularly those containing PHI, will be picked up as soon as possible.

(4) **Printers**. Print jobs, and particularly those containing PHI, will be picked up as soon as possible.

(5) **Copiers**. Company employees will remove their copy jobs containing PHI from the machine when the job is completed.

(iii) **Secure Conversations**.

(1) **With Other Employees Who Have Access to PHI.** Company employees only discuss PHI with other employees who have access to PHI and only as required to perform their job responsibilities.

A. Conversations that involve PHI are conducted using moderate voice tones.

B. The IT employees only discuss PHI with the other Company employees to the extent necessary to provide technical support related to electronic PHI.

(2) **With Employees Who Do Not Have Access to PHI.** Company employees do not discuss PHI with other Company employees who do not have access to PHI, except as provided for in these Policies and Procedures.

(3) **With Individuals Who Are the Subject of PHI.** Company employees may receive communications from individuals who wish to discuss their own PHI.

A. Such conversations should be had in a private area where the PHI being discussed is unlikely to be overheard by a third party.

B. Conversations that involve PHI should be conducted using moderate voice tones.

C. If an individual orally contacts a Company employee to inquire about matters related to his/her PHI, the Company employee verifies the individual's identity by requesting the individual's date of birth and address.

IMPORTANT: UNLESS SPECIFICALLY AUTHORIZED AS ABOVE OR IN WRITING BY THE PRIVACY OFFICER, ALL OTHER EMPLOYEE ACCESS TO PHI IS UNAUTHORIZED, STRICTLY PROHIBITED AND MAY RESULT IN SANCTIONS.

USES AND DISCLOSURES OF PHI THAT ARE REQUIRED OR PERMITTED BY THE PRIVACY RULE, OR PERMITTED BY AUTHORIZATION

Index: P-04

1. POLICY

This Policy summarizes the uses and disclosures of patient protected health information ("PHI") that are required or permitted by the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, or permitted by authorization. Notwithstanding the following, if the Company's Notice of Privacy Practices, as revised from time to time, restricts the use of PHI beyond the terms of this policy, the Notice of Privacy Practice shall control.

2. PROCEDURES

2.1 **REQUIRED USES AND DISCLOSURES**. Company is required to use or disclose PHI in the following circumstances:

(a) **Individual Access**. To the individual who is the subject of the PHI contained in the designated record set, provided the individual's identity is reasonably verified by the Company employee, or if the request is to inspect and/or copy his/her PHI.

(b) **Access by Secretary of HHS.** To the Secretary of the Department of Health and Human Services ("HHS") when the Secretary is investigating a complaint or monitoring compliance. The Company will verify the identity of the HHS requester**.**

2.2 **DISCLOSURES TO FAMILY MEMBERS**.

(a) **Spousal Access**. A spouse must typically sign a HIPAA-compliant authorization releasing an individual's PHI to his or her spouse. A template HIPAA-compliance authorization Form is contained in the Appendix to these Privacy Policies and Procedures. Company employees should verify whether any personal representatives have been designated by the individual prior to disclosing PHI to a spouse.

(b) **Parental Access**. Parents or guardians ("parents") are generally considered the personal representatives of unemancipated minors. As such, the Company generally responds to parental inquiries and can provide parents with access to the minors' PHI. Company employees should verify whether any personal representatives have been designated by the individual prior to disclosing PHI to a parent.

2.3 **USES AND DISCLOSURES OF PHI PERMITTED WHEN THE PATIENT IS DECEASED.** Company may disclose PHI of a deceased patient to a family member, other relative, close personal friend or other person previously identified by the patient as someone involved in the patient's care or payment for health care prior to the patient's death. PHI disclosed will be limited to what is relevant to the person's involvement in the patient's care. NOTE: if the Company has knowledge that the disclosure of PHI would be inconsistent with a preference previously expressed by

the patient, the PHI requested will not be disclosed. Prior to disclosing a deceased patient's PHI at the direction of a personal representative, the Company will verify the individual's legal authority to act on behalf of the deceased patient or the deceased individual's estate. The PHI of a deceased patient is no longer considered to be PHI and is no longer subject to HIPAA after a period of 50 years following the death of the patient.

2.4 **USES AND DISCLOSURES PERMITTED FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS.** Company may use or disclose PHI for purposes of treatment, payment or health care operations *without* written authorization from the patient.

2.5 **USE AND DISCLOSURE OF PHI PERMITTED PURSUANT TO A VALID AUTHORIZATION**. Company will only use or disclose PHI to third parties for purposes other than treatment, payment or health care operations, or as permitted by the Privacy Rule or otherwise required by law, upon receipt of a valid, written authorization. Once a valid authorization is received, the Company will only use and disclose information consistent with the terms of the authorization. An individual may revoke, in writing, his or her signed authorization at any time, except to the extent that the Company has taken action in reliance on the authorization prior to revocation.

(a) **Authorization Forms**. Company should verify that an authorization is valid where an authorization is required. A template HIPAA authorization is contained in the Appendix to these Privacy Policies and Procedures. Valid HIPAA authorizations must contain the following information:

(i) A description of the information to be used or disclosed that describes the information in a specific and meaningful fashion**.**

(ii) The name or other specific identification of the person(s) or class of person(s) authorized to use or disclose the information from the Company**.**

(iii) The name or other specific identification of the person(s) or class of person(s) to whom the Company may use or disclose the information**.**

(iv) A description of each purpose of the requested use or disclosure**.** If the individual initiates the authorization, the purpose may be described as "At the request of the individual."

(v) A statement that the individual may revoke the authorization in writing, and how to do so**.**

(vi) A statement that the Covered Entity shall not condition treatment, payment or eligibility for benefits on the authorization (unless one of the conditional exception applies, in which case that exception must be explained)**.**

(vii) The potential for information disclosed under the authorization to be subject to redisclosure by the recipient, and the fact that once the information is disclosed (to a non-covered entity) it is no longer protected by HIPAA**.**

(viii) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure**.**

(ix) Signature of the individual who is the subject of the PHI and the date**.** If the authorization is executed by a personal representative, it must include a description of the representative's authority to act for the individual.

2.6 **OTHER PERMITTED USE WITHOUT AUTHORIZATION**. Company may use and disclose PHI for the proper management and administration of Company; provided that with respect to any disclosures of PHI, such disclosures are Required by Law or Company obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person agrees to notify the Company of any instances of which it is aware in which the confidentiality of the information has been breached. Company may, in accordance with the Privacy Rule, de-identify PHI and further use and disclose such de-identified health information without regard to HIPAA. Company may also provide data aggregation services relating to the Health Care Operations of the Covered Entity.

THE MINIMUM NECESSARY REQUIREMENT

Index: P-05

1. POLICY

The Company applies the minimum necessary standard whenever it uses or discloses PHI to a third party, or requests PHI from another Covered Entity. This means that the Company makes reasonable efforts to limit the use or disclosure, or request of PHI to the minimum necessary to accomplish its intended purposes.

2. PROCEDURE

2.1 **APPLICABILITY OF THE MINIMUM NECESSARY REQUIREMENT**. The Company will apply the minimum necessary standard to all uses and disclosures of PHI, except as follows:

(a) Disclosures to or requests by a health care provider for treatment purposes;

(b) Permitted and required disclosures to the individual who is the subject of the information;

(c) Uses or disclosures pursuant to a valid authorization executed by the individual;

(d) Disclosures made to the Secretary of HHS in accordance with the Privacy Rule; or

(e) Uses and disclosures required by law, and uses and disclosures that are required for compliance with the Privacy Rule**.**

2.2 **IDENTIFICATION OF EMPLOYEES**.

(a) **Identified Employees**. The Company employees who need access to PHI are identified in Company's Policies on Personnel Designations and Restricted Internal Access to Protected Health Information. No other Company employees may have access to PHI unless authorized by the Privacy Officer and/or as necessary for the performance of their job duties.

(b) **Restrictions on Employee Access**. The Company employees who need access to PHI only have access to the PHI necessary for their job duties, unless specifically authorized by the Privacy Officer.

2.3 **MINIMUM NECESSARY REQUIREMENT APPLIED TO USES AND DISCLOSURES OF PHI**.

(a) **Reliance on Scope of Request as Minimum Necessary**. Company may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(i) Making disclosures to public officials for purposes permitted under 45 CFR § 164**.**512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(ii) The information is requested by another Covered Entity owner of such PHI; or

(iii) The information is requested by a researcher with appropriate documentation from an Institutional Review Board**.**

2.4 **REQUESTS FOR PHI AND THE MINIMUM NECESSARY REQUIREMENT**. Requests for PHI initiated by the Company shall seek only the minimum necessary to accomplish the purpose for which the request is made.

2.5 **LIMITATION REGARDING USING, DISCLOSING OR REQUESTING ENTIRE MEDICAL RECORD**. For all uses, disclosures, or requests to which the minimum necessary requirements apply, the Company will not use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

BUSINESS ASSOCIATE RELATIONSHIPS

Index: P-08

1. POLICY

The Company ensures that its Business Associates, the entities that perform services for the Company and create, receive, maintain or transmit PHI that belongs to the Company in the course of providing such services, protect the privacy of the PHI and provide individuals with certain rights with respect to the PHI. After the Company obtains a Business Associate Agreement ("BAA") from a Business Associate, which provides that the Business Associate will protect the PHI and limit its use and disclosure of PHI, the Company will disclose PHI to the Business Associate only to the extent necessary for the Business Associate to carry out its contractual duties.

2. PROCEDURE

2.1 **BAA**. Before the Company discloses PHI to a Business Associate or permits a Business Associate to create, maintain or transmit PHI on its behalf, the Company enters into the required BAA. The Privacy Officer is responsible for assisting in identifying those vendors that require BAAs and ensuring that such BAAs are entered into. Upon execution, a copy of the BAA must be sent to the Privacy Officer.

2.2 **MONITORING AND NON-COMPLIANCE**. The Privacy Officer monitors Business Associates' compliance with their obligations only if they have a reasonable belief that a Business Associate has violated its BAA. Any Company employee or Business Associate or agent who becomes aware that a Business Associate may be violating its obligations to the Company must immediately report such alleged violation to the Privacy Officer, who may investigate the matter and, if warranted, take reasonable steps to cure the violation.

(a) **Investigation**. The Privacy Officer may take the following steps as appropriate if they become aware of a possible violation of a BAA: (1) interview Company employees who may have knowledge of the alleged violation; (2) interview the Business Associates' employees who may have knowledge of the alleged violation; (3) collect any documentation from the Company or the Business Associate that relates to the alleged violation; (4) contact the Business Associate to obtain information related to the alleged violation; (5) review the documents that pertain to the alleged violation; and (6) take any other actions that the Privacy Officer deems appropriate.

(b) **Response If Violation Has Occurred**. If the Privacy Officer determines that the Business Associate has violated the agreement, the Privacy Officer may:

(i) sanction any Company employee involved with the violation;

(ii) request that the Business Associate sanction any of its employees who were involved with the violation;

(iii) coordinate with the Business Associate to perform a risk assessment for potential notification of Breach purposes in accordance with Company's breach notification policy;

(iv) mitigate any harmful effect that the Company knows of resulting from the improper use or disclosure of the PHI;

(v) take any remedial steps provided for by the BAA; and/or

(vi) work with the Business Associate to cure the violation and ensure such violation will not occur again**.** But, if the reasonable steps taken to cure the violation are unsuccessful, the Company may terminate the contract with the Business Associate.

PERSONAL REPRESENTATIVES

Index: P-09

1. POLICY

For purposes of these Policies and Procedures, the Company will treat a person as a personal representative of the patient if, under applicable state law, that person has the authority to act on behalf of a patient, who is an adult or emancipated minor, in making decisions related to the patient's health care. The Company will also treat a person as a personal representative of a patient, if under applicable state law, that person is a parent, guardian or other person who has authority to act on behalf of a patient, who is an unemancipated minor, in making decision related to the patient's health care.

2. PROCEDURES

2.1 **GENERAL RULE**. Generally, the Company must grant a personal representative the same right to access, and control uses and disclosures of, PHI that would be allowed to the patient they represent.

(a) **Examples of Personal Representatives**.

- An adult who has legal authority over an individual with respect to health care decisions (*e.g*., a parent or guardian);
- An emancipated minor acting on behalf of the individual (*e.g*., an underage parent of a child);
- A legal representative of a deceased individual (*e.g*., an administrator or executor of an individual's estate);
- Any other person authorized under applicable state law to make decisions related to health care on behalf of the individual; and
- Any individual designated in accordance with HIPAA as a personal representative.

(b) **Exceptions**. If the Company is contacted directly by a patient and the patient expresses the desire to revoke a personal representative designation (where such is revocable under HIPAA), the Company will not share PHI with such personal representative.

INDIVIDUAL REQUESTS/RIGHTS UNDER HIPAA

Index: P-10

1. POLICY

Individuals have a right to make certain requests pertaining to their PHI as described below. The Company will accommodate such requests in accordance with the law.

1.1 RIGHT TO INSPECT AND COPY PHI

(a) **REQUESTS TO INSPECT AND/OR COPY PHI**. The Company may accommodate an individual's request to inspect and/or copy his/her PHI.

(b) **PROCEDURE**. The Company shall provide the requested access to PHI. If the Company does not hold the individual's medical record, it will direct the individual to the Covered Entity who holds the records and forward the request to such Covered Entity.

1.2 REQUESTS FOR CONFIDENTIAL COMMUNICATIONS OF PHI AND/OR ALTERNATIVE MEANS OF COMMUNICATIONS

(a) **STANDARD TO RECEIVE CONFIDENTIAL COMMUNICATIONS**. The Company may accommodate an individual's reasonable request to receive communications of PHI in a confidential manner or at an alternative location. If the individual clearly and reasonably states that the disclosure of all or part of that information could endanger the individual, the Company will accommodate the individual's request.

(b) **PROCEDURE**. The Company agrees to accommodate reasonable confidential communication requests from individuals. If the Company does not hold the individual's medical record, it will direct the individual to the Covered Entity who holds the records and forward the request to such Covered Entity.

1.3 REQUESTS TO RESTRICT USES AND DISCLOSURES OF PHI

(a) **STANDARD TO REQUEST RESTRICTION OF USES AND DISCLOSURES OF PHI**. The Company may accommodate an individual's reasonable request to restrict uses and disclosures of their PHI to carry out treatment, payment or health care operations or disclosures to a relative or individual identified by the patient.

(b) **PROCEDURE.** All requests shall be forwarded to the Privacy Officer for consideration. The Company may agree to accommodate reasonable requests to restrict uses and disclosures of PHI. If the Company does not hold the individual's medical record, it will direct the individual to the Covered Entity who holds the records and forward the request to such Covered Entity.

1.4 **REQUESTS FOR ACCOUNTING OF DISCLOSURES OF PHI**

(a) **STANDARD TO REQUEST AN ACCOUNTING**. Individuals have a right to receive an accounting from the Company that lists certain disclosures of their PHI made by the Company during the six (6) year period prior to the request.

(b) **PROCEDURE.** The Company shall provide such accounting. If the Company does not hold the individual's medical record, it will direct the individual to the Covered Entity who holds the records and forward the request to such Covered Entity.

(c) **CONTENTS OF THE ACCOUNTING**.

(i) **Accounting Requirements**. The accounting will be written and will contain the required information for an accounting under HIPAA.

(ii) **Items Excluded**. The accounting for disclosures will <u>not</u> include the following disclosures:

- Disclosures for carrying out treatment, payment or health care operations;
- Disclosures pursuant to a valid authorization executed by the individual;
- Disclosures of PHI to the individuals;
- Disclosures to persons involved in the individual's care, or for other notification purposes;
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials; or
- Disclosures that occurred before April 14, 2003.

(d) **ACCOUNTINGS INVOLVING BUSINESS ASSOCIATE DATA.** The Company shall obtain any necessary information held or maintained by a Company Business Associate required for an accounting.

1.5 AMENDMENT REQUESTS

(a) **STANDARD FOR AMENDMENT REQUESTS**. An individual has the right to request that the Company amend his/her PHI maintained in the designated record set.

(b) **PROCEDURE.** The Company will handle all requests for amendment in accordance with HIPAA regulations. If the Company does not hold the individual's medical record, it will direct the individual to the Covered Entity who holds the records and forward the request to such Covered Entity.

1.5 **DOCUMENTATION**. Information related to any individual requests will be retained for 10 years in accordance with Company's document and data retention policy.

COMPLAINTS

Index: P-11

1. POLICY

All individuals or parties who believe that privacy rights have been violated or who have a complaint arising under the Privacy Rule or these Policies and Procedures with regard to the Company have the right to make an inquiry or complaint with the Company or with the Secretary of Health and Human Services.

2. PROCEDURE TO FILE A COMPLAINT WITH THE COMPANY

2.1 **REPORTING**. Individuals may report a complaint to the Company as follows:

(a) An individual must make a complaint in writing to the Privacy Officer, and may elect to use the Privacy Rights Complaint Form, set forth in the Appendix to these Privacy Policies and Procedures. The complaint must include the individual's name, address and the date of birth, a description of the individual's complaint, and any documentation that supports his/her complaint. The Privacy Officer is available to discuss any questions the individual might have about the complaint procedure. An individual may contact the Privacy Officer at the following address and phone number:

Anne C. Weddle, J.D.
3702 Automation Way, #103
Fort Collins, CO 80525
complianceofficer@ncaphealth.com
970.999.0278

2.2 **INVESTIGATION**. When an individual makes a complaint, the Privacy Officer will promptly investigate the circumstances related to the report.

(a) **Reasonable Steps**. The Privacy Officer may take the following steps, as they deem appropriate, to investigate the alleged violation: (1) interview the individual complainant; and (2) interview the Company employees or Business Associates who may have knowledge of the alleged violation and review any relevant documents that pertain to the alleged violation. These procedures are not exclusive and the Privacy Officer may take any steps they deem necessary to investigate the complaint.

(b) **Confidentiality**. Confidentiality will be maintained throughout the investigative process to the extent practicable and consistent with the need to undertake a full investigation.

(c) **Results of Investigation**. If the Privacy Officer determines that a violation has occurred, they may take action as is necessary and supported by the facts, including:

- sanctioning the Company employees who have acted improperly, and requesting that any Business Associate employees who have acted improperly be sanctioned by the Business Associate;

- working with a Business Associate to cure any violation by the Business Associate, or terminating the Business Associate Agreement if no cure is possible;
- mitigating any harmful effect that the Company knows of resulting from the improper use or disclosure of PHI as per Company's mitigation policy.

(d) **Determination**. Upon completion of the investigation, appropriate action will be taken, as necessary and supported by the facts.

3. PROCEDURE TO FILE A COMPLAINT WITH SECRETARY OF HHS. To file a complaint with the Secretary of HHS, the individual should send a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, call 1.877.696.6775 or visit www.hhs.gov/ocr/privacy/hipaa/complaints.

4. DOCUMENTATION. Information related to each complaint received by the Company and the disposition of each complaint will be documented by the Company, and that documentation will be retained for 10 years.

MITIGATION

Index: P-12

1. POLICY

The Company, to the extent practicable, will mitigate any harmful effect that it knows of resulting from the use or disclosure of protected health information ("PHI") in violation of the Privacy Rule or these Policies and Procedures by the Company, any Company employees or its Business Associates.

2. PROCEDURE

2.1 **REPORTING REQUIREMENTS**. Any person, including Company employees or Business Associates, who becomes aware that an improper disclosure was made must immediately:

- Limit any further improper disclosure; and
- Report the matter to the Privacy Officer

2.2 **MITIGATION STRATEGY**.

(a) **Process**. In order to mitigate any harmful effects of an improper use or disclosure that the Company knows of, the Privacy Officer may take the following steps:

- immediately request the return or destruction of the PHI by the disclosing party and/or the party who received the PHI;
- create additional safeguards for protecting PHI;
- discipline the Company employees who have acted improperly;
- work with a Business Associate who may be involved to cure a violation, including requesting that the Business Associate discipline any involved employees; and
- terminate a Business Associate Agreement if the violation does not cease and/or consider all other possible remedial actions.

NOTE : The above steps are not mandatory or exclusive and the Privacy Officer may take any steps they deem necessary to mitigate the violation.

HIPAA WORKFORCE TRAINING

Index: P-13

---

1. PURPOSE

All employees and independent contractors who constitute the workforce of Company with access to Company PHI are to have initial and updated HIPAA training on the Policies and Procedures and applicable state and federal information privacy and security laws and regulations (See also HIPAA Security Policy S-04).

- **NEW EMPLOYEES**

The Privacy Officer shall, in cooperation with the Security Officer, relevant business heads, and the individual(s) responsible for hiring, implement and maintain a program to train all new hires (and new independent contractors with access to any Company PHI) on HIPAA issues and related policies and procedures (including, without limitation, these Policies and Procedures). The HIPAA training program shall include discussions regarding patient privacy rights, Company privacy rule obligations, security reminders, procedures for guarding against, detecting and reporting malicious software, procedures for monitoring log-in attempt and reporting discrepancies, and procedures for creating, changing and safeguarding passwords. The training program will also consist of an overview of the Company's HIPAA Privacy and Security Policies and Procedures, sanctions policies, individual security responsibilities, and common security threats and vulnerabilities.

Training of a new employee or independent contractor (the "trainee") must occur prior to the trainee being given unsupervised access to any Company PHI. Once training is completed, the trainee must sign a statement indicating that training was provided and that the trainee has a reasonable understanding of the information conveyed. New employees will be required to sign an acknowledgment of training acknowledging they have reviewed HIPAA laws and regulations and NCAP's privacy policies and procedures regarding permissible use of information technology systems containing electronic PHI.

- **CURRENT EMPLOYEES**

Current employees and independent contractors with access to PHI that have not received the training discussed above must receive that training within ninety (90) days after the effective date of these Policies and Procedures. Employees will be required to sign an acknowledgment of training acknowledging they have reviewed HIPAA laws and regulations and NCAP's privacy policies and procedures regarding permissible use of information technology systems containing electronic PHI.

- **ONGOING TRAINING AND ALERTS**

The Privacy Officer shall implement and maintain an ongoing training program for all Company employees and all independent contractors with access to PHI. The ongoing training program shall include, at a minimum, (a) frequent email alerts communicating new HIPAA developments; (b) periodic email reminders reinforcing HIPAA policies and procedures; and (c) yearly HIPAA Privacy and Security refresher courses.

- **DOCUMENTATION**

Company shall document compliance with this policy by maintaining records of all formal training sessions, including the statement referenced in Section 1, above, in the employee's personnel file. For contractors, such documentation shall be maintained in the relevant contractor file.

BREACH NOTIFICATION AND INVESTIGATION

Index: P-14

1. POLICY

The Company ensures that it investigates and notifies each individual whose unsecured protected health information ("PHI") has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of a breach by Company or one of its business associates, in accordance with the procedures for notifying individuals in 45 C.F.R §164.404. The Company also provides notification to the media as required by 45 C.F.R. §164.406 if a breach of unsecured PHI involves more than 500 residents of one state or jurisdiction, provides notification of all breaches of unsecured Personal Information in accordance with Colorado's Protections for Consumer Data Privacy ("CPCDP"), and provides notification of all breaches of unsecured PHI to the Secretary of Health and Human Services (the "Secretary") as required by 45 C.F.R. §164.408.

2. DEFINITIONS

2.1 Agent: Any person that is authorized to act on behalf of NCAP, including but not limited to NCAP's directors, officers, employees, contractors, subcontractors, service providers, and the employees, directors and officers of NCAP's contractors, subcontractors and service providers.

2.2 Prominent Media Outlets: The general interest newspaper(s), television station(s), and/or radio station(s) serving the state, county or city on a daily basis (or on the most frequent basis).

2.3 Personal Information: A Colorado resident's first name or first initial and last name in combination with any one of the following – (1) Social Security number, (2) Driver's License number or Identification Card number, (3) student, military, or passport identification number, (4) medical information, (5) health insurance identification number, or (5) biometric data. Personal Information also includes a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account and a Colorado resident's account number or credit or debit card number in combination with any required security codes, access code, or password that would permit access to that account. Personal Information does not include information that is lawfully made available to the general public from government records or widely distributed media.

3. PROCEDURE

3.1 **Investigation of Potential Breach**.

(a) Company workforce members will immediately report any suspected unauthorized use or disclosure of PHI or Personal Information to Company's Privacy Officer or Compliance Hotline at (970) 999-0278 or compliance@ncaphealth.com.

(b) Company's Privacy Officer will investigate all reported unauthorized uses or disclosures of PHI to determine whether a breach has occurred. An unauthorized use or disclosure of PHI is presumed to be a breach unless the Privacy Officer demonstrates

that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

(ii) The unauthorized person who use the PHI or to whom the disclosure was made;

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

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

(c) Company's Privacy Officer will investigate all reported unauthorized acquisition of Personal Information to determine the likelihood that the Personal Information has been or will be misused. Company will give notice as soon as possible to each affected Colorado resident, the state Attorney General, and/or consumer reporting agencies, in accordance with the process set forth below, unless the investigation determines that the misuse of information about the Colorado resident(s) has not occurred and is not reasonably likely to occur.

(d) If the Privacy Officer determines a breach of unsecured PHI has occurred, Company will notify patients, local media, the Secretary and/or state agencies as required by HIPAA or state laws in accordance with the process set forth below.

3.2 **NOTIFICATION OF BREACH**.

(a) **To Individuals**.

(i) Company will notify the individual in writing of the breach without unreasonable delay, and in no case later than 30 days after the date of discovery of the breach.

(ii) The date of discovery of the breach is the first day that Company knew about the breach, or would have known about the breach if Company had exercised reasonable diligence in implementing effective internal policies for discovering breaches of unsecured PHI or Personal Information.

(iii) Company will contact legal counsel if it is unsure of (i) the date of discovery of the breach or (ii) whether an individual who caused the breach is an employee or agent of Company.

(iv) The notice to the individual (whether in written or substitute form, as described below) will include the following elements, to the extent possible:

(1) A brief description of what happened, including the date of discovery of the breach, if known;

(2) A description of the types of unsecured PHI or Personal Information that were involved in the breach (such as whether the individual's full

name, social security number, date of birth, home address, diagnosis, disability code, or other types of information were involved);

(3) Any steps the individual should take to protect the individual from potential harm resulting from the breach;

(4) A brief description of what Company is doing to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and

(5) Contact procedures for the individual to ask questions or learn additional information, which will include a toll-free telephone number, e-mail address, website or postal address.

(v) Company will send the written notification by first-class mail to the individual at the last known address of the individual, or to the individual's email address, if the individual has previously agreed to electronic notice.

(vi) If the Individual is deceased, Company will send the written notification to the next of kin or personal representative of the individual, if Company has contact information for the next of kin or personal representative.

(vii) If the individual's contact information is unavailable or out-of-date such that the individual is unreachable by mail, Company will use a substitute form of notice that Company believes will reach the individuals.

(1) If there are fewer than ten individuals who cannot be reached by mailed written notice, Company will use an alternative form of notice, such as e-mail, telephone or other means.

(2) If there are ten or more individuals who cannot be reached by mailed written notice, Company will post the notice conspicuously on the home page of Company's website, or in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice will be posted for at least 90 consecutive days and will include a toll-free phone number that remains active for at least 90 days, which an individual can call to learn whether the individual's unsecured PHI may be involved in the breach.

(b) **To the Media.**

(i) Company will provide notice of a breach involving 500 or more individuals in any one state or jurisdiction to the prominent media outlets for that state or jurisdiction. The prominent media outlets would be the major television stations, newspapers and radio stations serving the residents of that area.

(ii) Company will provide the notice to the media without reasonable delay and in no case later than 60 calendar days after the date of discovery of the breach.

(iii) The notice to the media will include the same information that is required for the written notification to the individual, but without individual PHI involved in the breach. The notice may be in the form of a press release.

(c) **To the State Attorney General.**

(i) If a breach of Personal Information affects 500 or more individuals, Company will submit a notice of breach to the State Attorney General via email or postal service within 30 days from which Company determines that a security breach occurred. Notice to the Colorado State Attorney General should be sent to the Consumer Protection Program Manager at databreach@coag.gov.

(ii) The notification shall include the following information regarding each breach to the extent possible:

(1) Date of the breach;

(2) Date of discovery of the breach;

(3) Approximate number of individuals affected by the breach;

(4) Type of breach;

(5) Location of the breached Personal Information;

(6) Type of Personal Information involved in the breach;

(7) Brief description of the breach;

(8) Safeguards in place prior to the breach;

(9) Dates the individual notice was provided;

(10) Whether substitute notice was required;

(11) Whether media notice was required,

(12) Actions taken in response to the breach, and

(13) Whether they need to contact the federal trade commission or consumer protection agencies.

(iii) For more information regarding notification requirements to the Colorado State Attorney General's office go to https://coag.gov/resources/data-privacy-laws.

(d) **To the Consumer Reporting Agencies.**

(i) If a breach of Personal Information affects 1000 or more individuals, Company will notify Consumer Reporting Agencies that compile and maintain files on

consumers on a nationwide basis. Company shall not unreasonably delay notification and will notify the Consumer Reporting Agencies of anticipated date of notification to individuals.

(e) **To the Secretary of Health and Human Services.**

(i) Company shall maintain a log of all breaches of unsecured PHI involving less than 500 individuals.

(ii) The log shall include the following information regarding each breach to the extent possible:

(1) Date of the breach;

(2) Date of discovery of the breach;

(3) Approximate number of individuals affected by the breach;

(4) Type of breach;

(5) Location of the breached PHI;

(6) Type of PHI involved in the breach;

(7) Brief description of the breach;

(8) Safeguards in place prior to the breach;

(9) Dates the individual notice was provided;

(10) Whether substitute notice was required;

(11) Whether media notice was required, and

(12) Actions taken in response to the breach.

(iii) Within 60 days of the end of the calendar year in which the breaches were discovered, Company shall submit electronically a breach notification form for each breach on the Secretary's website: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/binstruction.html

(iv) If a breach affects 500 or more individuals, Company will submit electronically a breach notification form at the Secretary's website at the same time that Company notifies the affected individuals: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/binstruction.html.

APPENDIX: PRIVACY RIGHTS COMPLAINT FORM

See attached form.

Northern Colorado Anesthesia Professionals

PRIVACY RIGHTS COMPLAINT FORM

The Health Insurance Portability and Accountability Act of 1996 requires that **Northern Colorado Anesthesia Professionals ("NCAP")** protect the privacy of your Protected Health Information (PHI). If you are concerned that we have violated (a) your privacy rights, or (b) our policies and procedures implementing HIPAA compliance within NCAP, and/or you disagree with a decision we made about access to, or amendment of, your records, you may contact NCAP's Compliance and HIPAA Privacy Officer at the following:

Compliance Hotline at (970) 999-0278, or in writing to us at:

Compliance and Privacy Officer
Northern Colorado Anesthesia Professionals
3702 Automation Way, #103
Fort Collins, CO 80525
Email: compliance@ncaphealth.com

You also have the right to file a complaint with the Office for Civil Rights, Secretary of the Department of Health and Human Services (HHS). Directions for this process may be found at: www.hhs.gov/ocr/privacy/hipaa/complaints.

We will not retaliate against you for filing a complaint with NCAP or with the Secretary of HHS.

NCAP will investigate reported violations of any privacy policy and will develop and implement a corrective plan of action to deal with any discovered violations.

Please provide the following information so that we may properly address your complaint:

Details of your complaint: (Please be as specific as possible with respect to dates and times; include the name(s), if any, of anyone in NCAP with whom you discussed your complaint. Use the other side of this form if you need more space.)

_____

_____

_____

_____

_____ _____

Patient Signature **Date**

FOR INTERNAL USE ONLY

Date Received	**Date Reviewed**
Reviewed By	**Compliance Officer**

Comments (Specify the actions taken to address the Patient's complaint, state whether or not the Patient was satisfied with resolution, etc.):

APPENDIX: HIPAA AUTHORIZATION FORM

See attached form.

Northern Colorado
Anesthesia Professionals

HIPAA AUTHORIZATION TO RELEASE PROTECTED HEALTH INFORMATION

I, _____ (Patient Name), hereby authorize **Northern Colorado Anesthesia Professionals ("NCAP")** to release the following protected health information to the following individual(s) or entity for the stated purposes:

Name of Recipient(s):

_____

Address:

_____

Phone:

_____

Fax (PHI authorized to be sent via fax):

_____

Relationship to Patient:

_____

Information Authorized for Release:

_____

_____

_____

Purposes of the Release Authorized:

_____

_____

_____

This authorization shall remain in effect unless and until revoked by me or my personal representative. I understand I may revoke this authorization by providing written notice of such revocation to NCAP at any time. I understand that NCAP will not condition my treatment, payment or enrollment/eligibility for benefits on whether I sign this authorization. I understand that it is possible that information disclosed pursuant to this authorization may be subject to re-disclosure by individuals who see it, and such individuals may not be bound by HIPAA. I understand that I will receive a copy of this authorization for my personal records.

_____ _____

Patient/Personal Representative Signature Date

COPY MUST BE GIVEN TO PATIENT