ARIA INTEGRATIVE MEDICINE
3216 NE 45th Place, Suite 300
Seattle, WA 98105
Phone: (206) 588-1227
Fax: (206) 588-1387
www.AriaIntegrative.com

HIPAA Policy

Effective January 30th, 2013

Policy: General Policy Issues – Privacy of Patient Information

Purpose: To outline Aria Integrative Medicine's general position on implementation or compliance with HIPAA and other privacy laws.

Aria Integrative Medicine ("Aria") will implement the required elements of the HIPAA privacy rule on February 1, 2013. Continuing compliance with HIPAA will be achieved through ongoing assessment, oversight and informational training, as coordinated through the privacy officer.

Aria shall address all complaints received from patients, clients, employees or third parties in an expeditious and meaningful manner. Aria respects the rights of individuals, including employees, to make complaints, ask questions or inquire as to Aria's compliance with HIPAA and other privacy laws. No adverse action or retaliation shall be taken against any such individual or employee based on any legitimate complaint, question, or inquiry.

Aria must identify those members of its workforce that require access to protected health information to perform their duties, specify the protected health information to which they require access and make reasonable efforts to limit their access accordingly.

All employees will be trained in order that Aria will be HIPAA compliant. New employees will be trained on a regular basis to ensure continued compliance with new personnel. Personnel will be retrained if significant changes occur affecting HIPAA or privacy laws. Employees who fail to follow HIPAA requirements and/or the policies of Aria with respect to privacy rules, shall be sanctioned appropriately. Such sanctions may range from oral reprimand to termination. Any intentional breach of patient confidentiality, not permitted by law, shall be severely punished. All such sanctions shall be documented, in writing, by Aria.

To the extent practicable, Aria will mitigate the harmful effects of any known use or disclosure, by itself or its business associates, that is in violation of the privacy rule and/or Aria's policies and procedures.

The privacy officer shall implement necessary procedures or protocols to ensure that HIPAA compliance is maintained, including implementation and ongoing compliance with the rights set forth in Aria's published Notice of Privacy Practices. Such procedures and protocols may range from informal work processes to formal implementation policies. The privacy officer shall work with the governing body of Aria to implement major decisions.

Beginning February 1, 2013 Aria shall operate within the HIPAA requirements, and continued compliance shall be maintained with HIPAA, as amended from time to time.

Common abbreviations and terms used in the privacy policy manual for Aria includes:

- "PHI" means Protected Health Information, as that term is defined by HIPAA;
- "TPO" means Treatment, Payment, and Health Care Operations, as those terms are defined by HIPAA; and
- "Covered entity" means Aria Integrative Medicine.

Policy: Minors

Purpose: To describe the access rights of a minor and identify the circumstances under which he/she has a right to access their medical records.

The parent or legal guardian of a minor (someone 17 years old or **younger**), **not the minor**, has the right to access the minor's records by requesting access in writing and submitting the request to Aria. A minor does not have the right to access his/her medical records without parental authorization, except in limited circumstances (listed below).

A minor, and only the minor, may access his/her own records, without obtaining parental or legal guardian consent, in the following circumstances:

1. Examination or treatment for venereal diseases (for patients 13 years old and up);
2. HIV/AIDS testing, counseling and treatment if minor objects to parental involvement;
3. Family planning covered by Medicaid;
4. Abortion counseling and performance;
5. If the minor has been emancipated;
6. With respect to a child of the minor;
7. Drug and alcohol abuse treatment; and
8. Outpatient mental health if "sixth session" rule is met.

In these eight circumstances, a parent may not access the minor's records without the minor's consent.

In an outpatient mental health setting, where no drugs are being used as a treatment modality, a psychiatrist, psychologist, licensed social worker or licensed family and marital therapist may provide treatment to a minor without parental consent for six sessions. Upon the sixth session, the practitioner must tell the minor patient that, in order to continue treatment, the minor's parents must be notified – unless the practitioner believes such parental notification would be detrimental to the minor's well-being. At the end of every sixth session, the practitioner must make this assessment. If the minor refuses to agree to parental notification, the practitioner may end treatment, but may not inform the minor's parents of the care or any information about the minor. This is commonly referred to as the "sixth-session rule."

The "sixth-session rule" described above applies if all of the following are met:

1. informing the minor's parent would cause the minor to reject treatment;
2. treatment is clinically indicated;
3. failure to provide treatment would be seriously detrimental to the minor's well-being;
4. the minor knowingly and voluntarily sought treatment; and
5. the practitioner believes the minor is mature enough to participate in treatment productively.

The practitioner must document in the minor's record any determinations about parental notification, and obtain a written statement by the minor that:

- he/she is voluntarily seeking treatment, that he/she has discussed the possibility of involving his/her parents;
- that he/she has determined not to involve his/her parents; and
- that he/she has been given adequate opportunity to ask the practitioner questions about his/her treatment.

The parent of a minor who has not been notified of treatment of the minor under this section is not responsible for payment of services.

Policy: Privacy Officer Requirements

Purpose: To describe the role and responsibilities of the privacy officer.

HIPAA section 45 CFR 164.530 requires Aria to designate a privacy officer to oversee HIPAA compliance. The privacy officer is responsible for the implementation and development of Aria's privacy policies and procedures, and often acts as the final arbiter with regard to Aria's HIPAA decisions. The privacy officer must have a working knowledge of:

- The uses and disclosures permitted by the Notice of Privacy Practices;
- The internal Privacy Policy of Aria;
- What compromises protected health information (i.e., prohibited personal identifiers);
- Uses and disclosures not requiring an authorization or an opportunity to agree or object;
- Authorizations;
- The accounting process;
- The right to request confidential communications;
- The right to request a restriction;
- The amendment process;
- The procedures involved in providing an individual with access to his/her PHI;
- Aria's complaint process;
- Incidental disclosures;
- Business associate agreements;
- Data use agreements;
- Documentation requirements (i.e., retention schedules);
- Vendors; and
- Regulatory changes.

The identity of the privacy officer shall be logged by Aria in a manner that facilitates tracking of that information.

Policy: Privacy Contact Requirements

Purpose: To describe the role and responsibilities of the privacy contact.

The privacy contact is largely an administrative position. The privacy contact is responsible for receiving, logging, and informing the privacy officer of [45 CFR 164.530(a), 164.524(d), 164.526(d)]:

- Individual complaints alleging HIPAA violations;
- Individual inquiries regarding rights afforded by the Notice of Privacy Practices;
- Individual complaints regarding a denial of access to protected health information; and
- Individual complaints regarding the denial of a request for an amendment to protected health information contained in a designated record set.

The identity of the privacy contact shall be logged by the privacy officer or his/her designee in a manner that facilitates tracking of that information.

Policy: Acknowledgment of Notice of Privacy Practices

Purpose: To describe when an acknowledgment is required and the manner in which it should be obtained from the individual.

If Aria shares a direct treatment relationship with the patient, it must:

- Provide a Notice of Privacy Practices to the patient on his/her first visit, following February 1, 2013, or in an emergency treatment situation, provide the Notice of Privacy Practices to the patient as soon as reasonably practicable after the emergency has ended;

- Make a good faith effort to obtain a written acknowledgment from the patient that he/she has received a copy of the Notice of Privacy Practices, and if unable to obtain an acknowledgment from the individual, document its good faith efforts to obtain the acknowledgment and the reasons why an acknowledgment was not obtained. (If Aria presents the patient with a Notice of Privacy Practices and the patient refuses to sign an acknowledgment, there is no HIPAA violation as long as Aria documents its good faith effort to obtain an acknowledgment);

- Post the Notice of Privacy Practices in a clear and prominent location within the office where it is visible to all patients;

- Post the Notice of Privacy Practices on the website if Aria maintains a website and provide an individual receiving electronic Notice of Privacy Practices a paper copy upon request;

- Make Notice of Privacy Practices available at a physical service delivery site if Aria maintains such a service;

- Make the Notice of Privacy Practices available whenever the Notice of Privacy Practices is revised and the patient requests a revised copy.

The HIPAA acknowledgment is not a consent for treatment, but rather for use and disclosure of patient information in the course of treatment, payment or health care operations.

Policy: Authorization for the Use/Disclosure of Protected Health Information Determination

Purpose: To provide the circumstances under which an individual's authorization is or is not required for the use and/or disclosure of protected health information.

A HIPAA authorization is required for any disclosure Aria makes outside of the context of treatment, payment, or health care operations.

Outside of TPO, Aria should not disclose protected health information without an authorization, unless one of the following exceptions applies. An authorization is not required:

- To disclose psychotherapy notes to the extent that only the creator of the notes will access them for treatment purposes [164.508];
- To release patient information for use in a facility's directory. The information must be limited to patient name, patient location, and general condition. The patient must be given an opportunity to restrict or prohibit disclosure [164.510];
- To conduct limited discussions, involving health information, with the patient while family and close friends are present, if the patient agrees and has been given an opportunity to object. If the patient is not present or is unable to consent because of incapacity or an emergency situation, an Aria provider may make such a disclosure if in his/her professional judgment, it is in the best interests of the patient [164.510];
- To disclose PHI to the extent it is required by law (including disclosure to a local, state, or federal agency in compliance with a reporting duty) [164.512];
- To disclose PHI to a health oversight agency for activities authorized by law [164.512];
- To disclose PHI pursuant to a court order, or in limited circumstances, in response to a subpoena [164.512];
- To disclose PHI to law enforcement officials where the disclosure is necessary to report a crime [164.512];
- To disclose PHI to a coroner or medical examiner for the purpose of identifying the decedent or determining the cause of death [164.512];
- To disclose PHI to an organ procurement organization for the purposes of organ or tissue donation [164.512];
- To disclose PHI in an emergency treatment situation [164.512];
- To disclose PHI for specialized governmental functions (including disclosure to federal officials for national security and intelligence purposes, and disclosure to armed forces personnel for purposes of a military mission) [164.512];
- To disclose PHI for purposes of complying with laws pertaining to workers' compensation [164.512];
- To disclose information that is not PHI under HIPAA.

Policy: Accounting of Disclosures of Protected Health Information Determination and Requirements

Purpose: To identify the disclosures of protected health information that must be included within an accounting, and to describe the information that must be included within the accounting.

HIPAA requires Aria to account for any disclosure of PHI made by Aria itself or by one of its business associates. If multiple disclosures are made to the same person/entity, then Aria may meet the accounting requirement by fully accounting for the first disclosure, noting the frequency of subsequent disclosures, and including the date of the last disclosure. Provided below is a checklist designed to help Aria assess whether an accounting is required.

1. Has Aria or any of its business associates disclosed PHI?

2. If so, do any of the following exceptions apply, thereby eliminating the accounting requirement? Such exceptions may include [164.528]:

    - disclosure made to carry out TPO;
    - disclosure made directly to individual;
    - disclosure made for the facility's directory or to person's involved in the individual's care;
    - disclosure made to correctional institutions or law enforcement about an inmate in custody;
    - disclosure made for national security or intelligence purposes;
    - disclosure to or by a business associate that is for an exempt purpose (e.g., disclosure for TPO);
    - disclosure pursuant to an authorization;
    - disclosure pursuant to an authorization for psychotherapy notes;
    - disclosure of a limited data set[1];
    - incidental disclosure;
    - subsequent disclosure by an entity that receives information from Aria or its business associate.

1 A disclosure for research, public health, or health care operations, in which a limited data set is used/disclosed and a data use agreement is obtained from the recipient of the limited data set, is not subject to the HIPAA accounting rule. A limited data set includes no direct identifiers but can contain admission, discharge, and service dates, date of death, age, and 5 digit zip code.

3. If an exception does not apply, Aria must account for the disclosure of PHI. Examples include:

   - disclosure made for research purposes pursuant to board approval of a waiver of authorization;[2]
   - disclosure made to a public health authority;
   - disclosure required by law;
   - disclosure to a government entity;
   - disclosure to law enforcement;
   - disclosure to insurers for claims investigations;
   - disclosure made to child or adult protective services when referrals made for abuse or neglect.

4. The accounting must include[164.528(b)]:

   - Disclosures that occurred during the 6 years prior to the date of the request for an accounting;
   - The date of the each disclosure;
   - The name of the entity of person receiving the PHI and their address, if known;
   - A brief description of the PHI disclosed;
   - A brief statement of the purpose of the disclosure, or in lieu of such statement, a copy of the written request for disclosure under §§ 164.502(a)(2)(ii) (required disclosure to Secretary of HHS to investigate or determine Covered Entity's compliance) or 164.512 ("Uses and Disclosures for which an authorization or opportunity to agree or object is not requires.").

5. If Aria makes multiple disclosures of PHI to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.12, the accounting may include:

   - The information required in Section 4 of this part for the first disclosure;
   - The frequency with which the disclosure is made;
   - The date of the last disclosure.

2 If the research disclosure involves 50 or more records, the entity must only provide a simplified accounting. Rather than an individual accounting, the entity must disclose a list of all relevant protocols under which the individual's information may have been released, and the researcher's name and contact information.

Policy: Amending Protected Health Information Contained Within a Designated Record Set

Purpose: To identify the process involved in accepting and denying an individual's request for an amendment to protected health information.

Aria must permit a patient to request an amendment to his/her medical record. Aria may require that the patient request be in writing. Regardless of whether Aria agrees to the amendment, Aria must provide the patient with notice of its decision within 60 days of the request. Aria is eligible for a 30-day extension, if within the initial 60-day period it sends a written statement to the patient explaining the reasons for the delay and the date on which its decision will be provided.

Aria may deny the patient's request to amend the medical record only if:

- The portion of the medical record that the patient wishes to amend was not created by Aria and the originator of that portion is available. If the patient, however, provides a reasonable basis for believing that the originator of the PHI no longer exists, Aria must amend the medical record [164.526];

- The portion that the patient wishes to amend is not a part of the medical record, the billing record, or the record set that Aria maintains and uses to make decisions regarding the patient [164.526];

- The portion that the patient wishes to amend consists of information to which the patient does not have a right of access [164.526];

- The portion that the patient wishes to amend is accurate and complete [164.526].

If Aria agrees to the amendment, it must [164.526]:

- Notify the individual (preferably in writing) that the amendment has been accepted;

- Mark the portions to be amended with instructions on where the amendment can be found (the original record should not be destroyed or obliterated);

- Make reasonable efforts to inform business associates and other individuals known to Aria or identified by the patient as having the protected health information, of the amendment.

If Aria denies the request for the amendment, it must [164.526]:

- Notify the patient in writing of the basis for the denial;

- Notify the patient of his/her right to submit a statement of disagreement into the medical record and the procedure involved in filing such a statement. If the patient submits a statement of disagreement, Aria has the right to insert a rebuttal statement into the medical record. Aria must provide the patient with a copy of the rebuttal statement;

- Notify the patient that if he/she does not wish to submit a statement of disagreement, he/she may request that a copy of the request and a copy of the denial be included with any future disclosures;

- Notify the patient of his/her right to pursue a complaint process with Aria, and of his/her right to contact the Secretary of Health and Human Services to complain.

Policy: Minimum Necessary/Incidental Disclosure Determinations and Decision Tree

Purpose: To identify the difference between incidental and improper disclosures.

1. Was the disclosure a by-product of a use or disclosure otherwise permitted under the Privacy Rule?

    a. If no, the disclosure may require remediation and investigation by the privacy officer to limit any harm cause by the disclosure and to improve compliance.

    b. If yes, go to the next question.

2. If yes, has Aria applied reasonable safeguards and implemented the minimum necessary standard?

    The minimum necessary standard [164.514(d)] prescribes that PHI should not be used and/or disclosed when it is not reasonably necessary to accomplish a particular purpose or carry out a specific function.

    Aria must make a reasonable effort not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose.

    Aria must identify those members of its workforce that require access to PHI to perform their duties, specify the protected health information to which they require access and make reasonable efforts to limit their access accordingly.

    a. If no, then the incidental disclosure may require remediation and investigation by the privacy officer to limit any harm cause by the disclosure and to improve compliance.

    Example: Allowing an employee unimpeded access to patient files, where such access is not necessary for the employee to perform his/her job, is not a proper application of the minimum necessary standard, and any incidental disclosure would be a potential HIPAA violation.

    Example: Erroneous uses/disclosures or disclosures resulting from mistake or neglect (e.g., Aria mistakenly sends protected health information via e-mail to the wrong recipient, protected health information is erroneously made accessible through the entity's website).

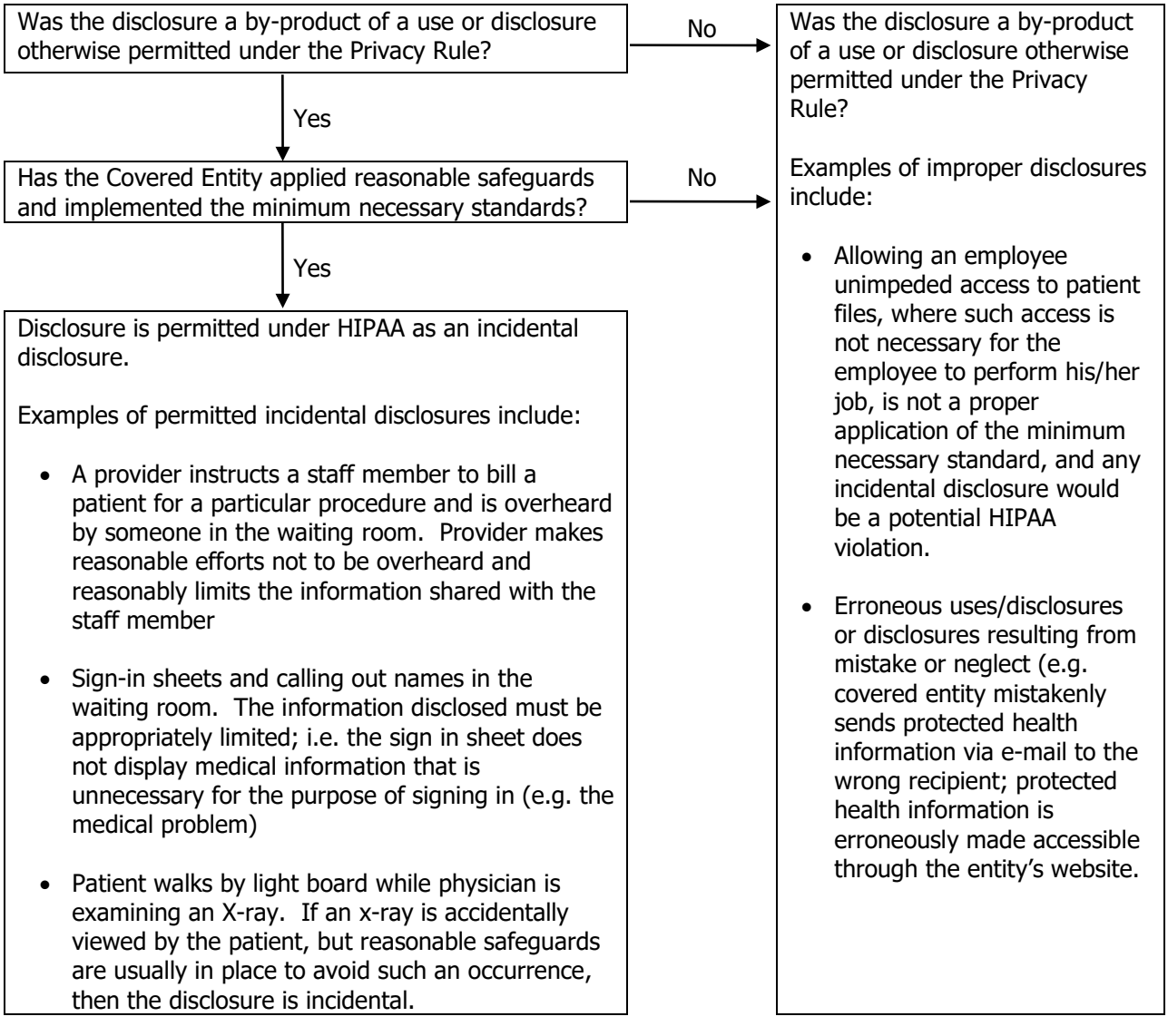
    b. If yes, then the disclosure is permitted under HIPAA as an incidental disclosure. The following are examples incidental disclosures, and are permitted:

    Example: An Aria provider instructs a staff member to bill a patient for a particular procedure and is overheard by someone in the waiting room. Aria provider makes reasonable efforts not to be overheard and reasonably limits the information shared with the staff member.

    Example: Sign-in sheets and calling out names in the waiting room. The information disclosed must be appropriately limited, i.e., the sign-in sheet does not display medical information that is unnecessary for the purpose of signing in (e.g., the medical problem).

Example: Patient walks by light board while Aria provider is examining an X-ray. If an X-ray is accidentally viewed by the patient, but reasonable safeguards are usually in place to avoid such an occurrence, then the disclosure is incidental.

Flow Chart of Preceding Information Concerning Incidental Disclosures



Policy: Marketing Disclosure Determination

Purpose: To identify what constitutes a marketing communication and when such disclosures require the authorization of the individual.

In making a marketing communication, HIPAA requires Aria to obtain an authorization for disclosure of protected health information [164.508(a)(3)]. There are exceptions for certain communications that are related to treatment or health care operations.

Under HIPAA, marketing means [164.501]:

- To make a communication about a product or service that encourages recipients of the communication to purchase or use the product; or

- An arrangement between Aria and another entity whereby Aria discloses PHI to any other entity for the other entity's marketing purposes, and in return, Aria receives direct/indirect remuneration.

Even if a communication would otherwise fall within the definition of marketing, Aria may be able to make the disclosure without an authorization, if the communication is made on behalf of Aria and it is related to the individual's treatment. HIPAA specifically excludes from marketing, communications that are made by Aria [164.501]:

- To describe a health-related product or service that it provides;

- To describe the participating providers in a network;

- For the treatment of the individual (i.e., recommending a specific brand-name or over the counter pharmaceutical or referrals of patients to other providers);

- For the case management or care coordination of the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual (i.e., appointment or prescription-refill reminders.)

If any of the four communications mentioned above occurs between Aria and one of its patients, no authorization is required.

Policy: Fundraising Disclosure Determination

Purpose: To identify the circumstances under which Aria may make a fundraising communication without the authorization of the individual.

HIPAA allows Aria to disclose certain PHI to a business associate or an institutionally related foundation, without an authorization, for fundraising purposes [164.514(f)].

Aria is limited to disclosing [164.514(f)]:

- demographic information pertaining to the individual;
- dates on which health services were provided to the individual.

To perform such fundraising functions, Aria is required to include [164.520(b)(1)(iii) and 164.514(f)(2)]:

- a separate statement within its Notice of Privacy Practices documenting its intentions to contact individuals to raise funds;
- a statement within its fundraising materials alerting individuals as to how they can opt-out of receiving any further fundraising communications.

Policy: Research Disclosure Determination

Purpose: To identify the processes involved in disclosing protected health information for research purposes.

HIPAA permits Aria to use/disclose PHI for research purposes with an individual authorization. Aria can avoid this requirement by obtaining a waiver, disclosing a limited data set, or de-identifying the information.

A waiver is permitted where [164.512(i)]:

- the PHI refers only to deceased individuals and the researcher asserts the necessity of access.
- an Institutional Review Board or Privacy Board determines that a waiver of individual authorization is appropriate and satisfies the following criteria:
    a. the use/disclosure of PHI involves a minimal risk to the individual;
    b. the waiver will not adversely affect the privacy rights and welfare of the individual;
    c. the research could not be conducted without the waiver;
    d. the privacy risks to individuals are reasonable in relation to the anticipated benefits to the individual or the knowledge resulting from the research;
    e. the presence of an adequate plan to protect identifiers from improper use/disclosure;
    f. the presence of an adequate plan to destroy all identifiers once they are no longer necessary to the research; and
    g. the presence of adequate written assurances that the PHI will not be reused or disclosed to any other person/entity, except as required by law.
- the PHI is utilized for preparatory research or the development of a protocol, where the PHI will not leave Aria and the researcher demonstrates that access is essential.

Disclosures made pursuant to a waiver are subject to the HIPAA accounting rule and the minimum necessary standard. If, however, the research disclosure involves 50 or more records, Aria must only provide a simplified accounting [164.528 (b)(4)]. Rather than an individual accounting, the simplified accounting requires Aria to disclose a list of all relevant protocols under which the individual's information may have been released, and the researcher's name and contact information.

Disclosures made pursuant to an individual authorization are not subject to the accounting or the minimum necessary standard. [164.528(a)(1)(iv) and 162.502(b)(2)(iii)]

Unlike the traditional HIPAA authorization, research-related authorizations

- do not require an expiration date, a notation indicating "end of research project" or "none" will suffice [164.508(c)(1)(v)];
- may be combined with any other legal permission related to the research study (including another authorization) [164.508(b)(3)(i)];

- may be a condition to the provision of research-related treatment [164.508(b)(4)(i)].

Research disclosures of de-identified information or a limited data set do not require an authorization or a waiver of authorization. Both are also exempt from the HIPAA accounting requirements [164.528(a)(1)(viii)].

A disclosure of a limited data set requires [164.514(e)]:

- a data use agreement with the recipient of the limited data set
- a limited data set including no direct identifiers but which can contain admission, discharge, and service dates, date of death, age, and 5 digit zip code

Information is not individually identifiable health information if it does not include any of the following information about a patient, the patient's relatives, the patient's employer, or the patient's household members:

- name
- all geographic subdivisions, including address and zip code
- all dates, except for year (including birth date, admission date, discharge date, and date of death)
- telephone number
- fax number
- email address
- social security number
- medical record number
- health plan beneficiary number
- account number
- certificate/license number
- vehicle identifier and serial number, including license plate number
- web universal resource locator (URL)
- internet protocol address number
- biometric identifier, including finger and voice prints
- full face photographic image and any comparable image
- any other unique identifying number, characteristic, or code

Policy: Business Associate Determination

Purpose: To provide a mechanism for determining if an outside entity is a business associate.

1. Does the person or entity perform, on behalf of Aria, any function that involves the use/disclosure of protected health information?

    a. If no, the person or entity is not a business associate under HIPAA and no further action is needed with respect to that person or entity.

    b. If yes, go to the next question.

2. Is the person a member of Aria's workforce?

    a. If yes, then the person is not a business associate under HIPAA and no business associate agreement is required.

    b. If no, go to the next question.

3. Do any of the following exceptions apply, thereby eliminating the need for a business associate agreement?

- Is the disclosure made by Aria to a health care provider for treatment purposes?
- Is the disclosure to a plan sponsor by a group health plan, a health insurance issuer, or an HMO?
- Is the collection and sharing of PHI by a health plan that is a public benefits program and an agency, other than the agency administering the plan, in order to determine eligibility or enrollment?

    a. If the answer is yes to any of the above questions, an exception applies, and no business associate agreement is required under HIPAA.

    b. If the answer is no to all of the above questions, an exception does not apply, the person or entity is a business associate, and HIPAA requires a business associate agreement between Aria and the person or entity.

Some examples of business associates are:

- claims processors/administrators
- data analysts
- data processors/administrators
- billing companies
- individuals/entities performing quality assurance or utilization review functions
- individuals/entities performing benefit management or practice management functions
- lawyers
- accountants
- consultants
- actuaries
- financial analysts
- individuals/entities performing accreditation functions

Disclaimer:

The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal and other professional advisors for individualized guidance regarding the application of the law to their particular questions or situations, and in connection with other compliance-related concerns.