0s
PRIVACY
SECURITY

HIPAA Privacy Rights and Operations Guide
HIPAA Security Summary

For the Practice of:

Rejuvenate Eye and Face Medspa

Publish Date: 11.1.2022

This guide has been created to serve Rejuvenate Eye and Face Medspa. It is intended to provide this organization and its workforce members with an overview of our daily operating policies and procedures and this organization's obligations relating to security and privacy standards for the use and disclosure of "protected health information" (PHI) under HIPAA, the Health Insurance Portability and Accountability Act of 1996.

This guide presents a simplified version of the fully detailed policies and procedures utilized to operate this Organization while maintaining the privacy and security of PHI. It should be used by workforce members and management as a quick reference to answer common questions about compliance operations and how to handle workplace situations so that HIPAA regulations are met and Patient Rights are upheld.

This document *is not* typically intended for outside distribution except as part of a wider investigation by regulators or other appropriate parties.

It is the responsibility of this Organization to conduct regular reviews of this document to incorporate updates as regulations change and/or to add more definition to the actual operational procedures utilized by this organization.

> If you have any questions—or if you need further guidance on HIPAA Privacy or Security requirements, please contact Diana L Fisher , RN, OD at 317-207-2868.

Section A: Privacy

Privacy, according to the HIPAA Privacy Rule, is an individual's right to control access and disclosure of their protected, "individually identifiable" health information. Besides giving individuals significant rights to understand and control how their health information is used, the Privacy Rule describes requirements for the use and disclosure of individuals' health information—protected health information (PHI)—by Covered Entity (CE) organizations subject to the Privacy Rule. PHI is considered "identifiable" if it contains any one or more of the 18 specific identifiers. <See policy *'8s – Minimum Necessary'* for a complete list of the 18 identifiers.>

1. Notice of Privacy Practices

Individuals have a right to receive a notice of the CE's privacy practices. The notice must be written in plain language and describe the ways in which the CE may use or disclose PHI. It also explains individual rights with respect to their health information, including the right to complain to Health and Human Services (HHS) and to the CE if they believe their privacy rights have been violated. <Our

Organization's Notice of Privacy Practices (NPP) is provided to new and existing patients through email or direct hard copy delivery. Our NPP is printed, posted in patient waiting areas and available upon request. We have translated our NPP into English and Spanish and ensure that each patient gets a copy when we being to treat them and they have access to them throughout their relationship with us.>

Our Organization creates record(s) of the care and services that patients receive from us. We need this record to provide them with quality care and to comply with certain legal requirements. Our NPP describes the ways in which we may use and disclose medical information about the patient. It also describes their rights and certain obligations we have regarding the use and disclosure of their medical information.

Our Organization always strives to follow all of the rules set down in our NPP. Any variation from our published practices that you notice should immediately be brought to the attention of the Organization's Security / Privacy Officer(s).

2. TPO (Treatment, Payment and Operations)

A CE may use or disclose PHI for its own treatment, payment or healthcare operations. Within our NPP, the following categories describe different ways that we may use and disclose patient PHI.

- **Treatment.** We may use medical information to provide a patient with medical treatment or services. We may disclose medical information about the patient to doctors, nurses, technicians, health care students, or other personnel who are involved in taking care of the patient within our Organization.

- **Payment.** We may use and disclose medical information about a patient so that the treatment and services received from the Organization may be appropriately billed and payment may be collected from the government, an insurance company or a third party.

- **Healthcare Operations.** We may use and disclose medical information about a patient for Organization operations. These uses and disclosures are necessary to run the Organization and make sure that all of our patients receive quality care.

3. Access, Use and Disclosure of PHI

General rules for access, use and disclosure of PHI are addressed within our NPP. *Minimum Necessary* principals are always applied to access, use or disclosure of PHI, meaning only the least amount of information needed to perform the permitted task is utilized. <Refer to '*Minimum Necessary'* policy for additional details.>

- **Appointment Reminders.** We may use and disclose medical information to contact a patient as a reminder that they have an appointment for treatment or medical care at the Provider location.

- **Treatment Alternatives.** We may use and disclose medical information to tell a patient about or recommend possible treatment options or alternatives that may be of interest to them.

- **Health & Related Benefits and Services.** We may use and disclose medical information to tell a patient about health and related benefits or services that may be of interest to them.

- **Fundraising Activities.** N/A.

- **Emergencies.** We may use or disclose a patient's medical information if they were to need emergency treatment or if we are required by law to treat them but are unable to obtain their consent. If this happens, we will try to obtain the patient's consent as soon as we reasonably can after treatment.

- **Communication Barriers.** We may use and disclose a patient's health information if we are unable to obtain their consent because of substantial communication barriers, and we believe they would want us to treat them if we could communicate with them.

- **Provider Directory.** N/A

- **Individuals Involved in the Patient's Care or Payment for Care.** We may release medical information about a patient to a friend or family member who is involved in their medical care and to whom the patient has agreed it is permissible. We may also give information to someone who helps pay for their care. In addition, we may disclose medical information about a patient to an entity assisting in a disaster relief effort so that the family can be notified about their condition, status and location.

- **Research.** N/ A

- **As Required By Law.** We will disclose medical information about a patient when required to do so by federal, state or local law.

- **To Avert a Serious Threat to Health or Safety.** We may use and disclose medical information about the patient when necessary to prevent a serious threat to their health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

- **Organ and Tissue Donation.** If a patient is an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

- **Military and Veterans.** If the patient is a member of the armed forces, we may release medical information about the patient as required by military command authorities.

- **Workers' Compensation.** We may release medical information about a patient for workers' compensation or similar programs.

- **Public Health Risks.** We may disclose medical information about a patient for public health activities. These activities generally include the following:
    - to prevent or control disease, injury or disability;
    - to report births and deaths;
    - to report child abuse or neglect;
    - to report reactions to medications or problems with products;
    - to notify people of recalls of products they may be using;
    - to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and
    - to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if the patient agrees or when required or authorized by law.

- **Health Oversight Activities.** We may disclose medical information to a health oversight agency for activities authorized by law. For example, audits, investigations, inspections, and licensure.

- **Lawsuits and Disputes.** If a patient is involved in a lawsuit or a dispute, we may disclose medical information about them in response to a court or administrative order. We may also disclose medical information about them in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell that patient about the request or to obtain an order protecting the information requested.

- **Law Enforcement.** We may release medical information if asked to do so by a law enforcement official:
    - in response to a court order, subpoena, warrant, summons or similar process;
    - to identify or locate a suspect, fugitive, material witness, or missing person;
    - about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
    - about a death we believe may be the result of criminal conduct;
    - about criminal conduct at the Provider; and
    - in emergency circumstances, to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

- **Coroners, Medical Examiners and Funeral Directors.** We may release medical information to a coroner or medical examiner. We may also release medical information about patients of the Practice to funeral directors as necessary to carry out their duties.

- **National Security and Intelligence Activities.** We may release medical information about a patient to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

- **Protective Services for the President and Others.** We may disclose medical information about a patient to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

- **Inmates.** If a patient is an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about them to the correctional institution or law enforcement official.

---

4. Individual (Patient) Rights

The HIPAA Privacy Rule grants the following ‘rights’ regarding a patient’s access to PHI and his/her right to control this information. A Covered Entity Organization typically ‘owns’ the records associated with the patient’s PHI, but has certain responsibilities for its maintenance. Individuals have the right to inspect and obtain a copy of their PHI in a designated record set for as long as the CE maintains the information. Generally, the Privacy Rule requires CEs to retain certain documentation for at least six (6) years. Most healthcare organizations keep medical records for a much longer time frame, and individuals have the right to access their records for as long as the CE keeps them. Regardless of time, every patient has rights to facilitate the confidentiality, security, accuracy and integrity of his/her information.

- **Right for Patient's to Access, Inspect, Receive Copies or Direct Copies be Sent of Patient Information**

  - This patient 'Right' is often referred to as a part of 'Release of Information'.

  - A patient has the right to access, inspect, get copies of and direct copies be sent to any third party of their medical information that is used to make decisions about his/her care. Usually, this includes medical and billing records, but does NOT include psychotherapy notes. <Refer to our *'Individual Access to PHI'* policy) for other important exceptions>. If the patient requests a copy of the information, our Organization may charge the HIPAA delineated fee for the costs of processing, copying, mailing or other supplies associated with the request. If a patient provides us with permission (using the Patient Access Request form, or similar, not an Authorization to disclose form) to use or disclose medical information about them, they may revoke that permission, in writing, at any time. If they revoke their permission, we will no longer use or disclose medical information about them for the reasons covered by their written authorization. They will need to understand that we are unable to take back any disclosures we have already made with their permission, and that we are required to retain our records of the care that we provided to them by law.

  - We may deny a patient request to inspect and receive or send copies of their medical information in certain very limited circumstances. If they are denied access to medical information, in some cases, they may request that the denial be reviewed. Another licensed health care professional chosen by the Organization will review the request and the denial. The person conducting the review will not be the person who denied the request. Our Organization will comply with the outcome of the review and document all of the processes included with the review.

Our Procedures for Inspection, Copying (for Receipt or Sending to Third Parties) for Disclosure of PHI

- *<Insert specifics for your Practice/Organization>.*

  - ***If the patient asks us to speak to another physician (or provider of care),*** use the *<'Patient Access Request* form (CCs)>, to gain signed authorization and documentation that we have permission to provide patient identifiable information to another healthcare provider. Note: If information provided is to another provider of care and is to be used for 'treatment' (the provision of healthcare) there is *not* a strict requirement under HIPAA to get an authorization or Patient Access Request form signed; but it is a good practice that we try to follow, especially if the other provider is unknown to the organization/practice. Any release of information that requires an accounting of disclosures should be logged on the *<'Release of Information and Patient's Rights Log'>* even if the patient does not sign an authorization for that disclosure.

  - ***If the patient asks us to disclose our written or copied patient information outside our organization***… the *<'Patient Access request* form (CCs)> is used to release information to a third party, which may or may not be another healthcare provider. If possible, get the patient to allow our practice to send the information directly to their provider of care, ensuring confidentiality and correct communications are observed. Depending on the purpose for the disclosure and type of third party (e.g., Adult Protective Services, Child Protective Services, Coroner/Medical Examiner, court order, employer, et

al.), releasing the entire medical record and tracking for Accounting of Disclosures MAY or MAY NOT be required. <Refer to specific guidelines or organization protocols for disclosure of PHI> *NOTE: The purpose behind a request for disclosure may also impact the fees we may charge for completing the request.*

- ***If the patient asks us to request written or copied patient information from another provider of care outside our practice/organization*** …use *<'Patient Access Request'* form (CCs)>, to authorize and request release of information. If written or copied patient information is to be used for 'treatment' (the provision of healthcare), there is not a strict requirement under HIPAA to get an authorization signed before we request the information; but it is a good practice that we try to follow, especially if the other provider is unknown to the organization/practice. Oftentimes, other providers of care will want the signed authorization, just for their own processing and protections.

- ***If a third party asks us for copied patient information…***use <Authorization to Disclose form Js>, which must be executed by the patient. These types of requests incur State Statute record copy fees.

As regulatory standards and organizational policy dictate:

- Record information disclosures in the <AAs '*Release of Information and Patient's Rights Log'*>.

- Be sure to calculate record copying fees according to HIPAA fee methodology if the request is initiated by a patient. Use State Statutes if the request is coming from a third party, not upon the direct request of the patient. There are instances where charges are not appropriate, such as in payment and healthcare oversight processes. Refer to the organization's *Release of Information* policies for additional guidelines on relevant scenarios and the appropriate fees.

- Be sure to validate and *if possible* get copies of the patient's or requestor's ID to store with the patient access form or authorization form. Some law enforcement agencies may not permit you to copy their ID or badges, and that is fine as long as you notate their ID number on the request, along with their affiliation, title, etc.

- Refer to and use <*Patient Access Request* form (CCs)> and/or *<'Authorization to Disclose PHI'* form (Js)> as often as needed; be sure to get signed authorizations to go with subpoenas.

- If a patient or third party requests **<u>electronic copies</u>** of their medical records, we need to disclosure them in that format if they are kept electronically. Electronic copies are produced by *<Insert details of EHR copy process>.*

- All of the above documentation must be kept for the minimum 6 year HIPAA retention.

- **Right to Amend.** If a patient feels that medical information we have about them is incorrect or incomplete, they may ask us to amend (correct or change) the information. They have the right to request an amendment for as long as the information is kept by or for our Organization.

- We may deny the request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny a request for amendment if the PHI:
  - Was not created by us (unless the originating person or entity that created the information is no longer available to make the amendment);
  - Is not part of the medical information (designated record set) kept by or for the Organization;
  - Is not part of the information which is available for inspection and copying; or
  - Is accurate and complete.

Our Organization Procedures for Amendments to PHI

- *<Insert specifics, including any of the bulleted items noted below as applicable>*
  - Use <*Request for Patient's Rights'* form Gs and '*Denial of Amendment or Correction Request'* form Hs> to document the patient's request and possible denial of the request.
  - Record the request in the 'AAs – ROI, Breach and Patient's Rights Log'.
  - If the amendment request escalates past a typical request and response, especially if there is a complaint or investigation use the <'Security or Privacy Event Report' form Bs> to document the entire process.
  - Process the request within 60 days.
- All of the above documentation must be kept for the minimum 6-year HIPAA documentation retention period.

- **Right to an Accounting of Disclosures (AOD).** Patients have the right to request an accounting of disclosures of their PHI by a Covered Entity or its Business Associates. Under HIPAA, a disclosure is a release, transfer, access to, or divulging of information outside of the Practice/Organization. In general, a patient has the right to know who has received his/her health information for reasons other than treatment, payment, and healthcare operations (commonly referred to as "TPO"), or disclosures specifically authorized by the patient. A request for an accounting cannot be earlier than the date the HIPAA Privacy Rule became effective which was April 14, 2003 for most CEs. Examples of disclosures that must be recorded and included in an accounting are: submission of reports required by law, this includes disclosure to Social Services or a protective service agency; responding to judicial or administrative proceedings, disclosures in response to warrants, court orders, subpoenas (unless the individual authorized the disclosure); notifying coroners, medical examiners and organ donation agencies of deaths; for law enforcement purposes, disclosures to report gunshot wounds. There are others, so if you are unsure whether a disclosure should be tracked, check with your supervisor.

Our Procedures for Accounting of Disclosures

- *<Insert specifics, including expected timeframe to perform and provide the AOD>*
  - Use <*'Request for Patient's Rights'* form Gs> to document the patient's request.

- Record the request in the 'AAs – ROI, Breach and Patient's Rights Log'.
- There is no charge for the first AOD request in a 12-month period; a <$15 fee> will be charged for each additional AOD request in the same 12-month period.

- All of the above documentation must be kept for the minimum 6-year HIPAA documentation retention period.

- **Right to Request Restrictions.** Patients have the right to request a restriction or limitation on the medical information we use or disclose about them for *payment or healthcare operations,* for disclosures to family members or someone who is (or may be) involved in their care and certain other permitted purposes. Covered entities are not required to agree with such requests, but if a covered entity does agree to the restriction, then the covered entity must abide by that restriction. It is this Organization's policy that we will not agree to any requests to restrict use or access of their medical information for treatment purposes.

  Patients also have the right to restrict use and disclosure of protected health information (PHI) if the PHI pertains solely to health care items or services for which the individual or another person on behalf of the individual (other than the health plan) has paid out-of-pocket, in full. We will not accept their request for this type of restriction until there is a zero balance for this item or service.

  General advice for restriction requests is to never accept them for treatment purposes and rarely, unless mandated by HIPAA, for payment or operations. Failure to comply with agreed to restrictions can lead to civil liabilities and fines.

  Our Procedures for Restrictions

  - Use <'*Request for Patient's Rights*' form Gs> and <'Denial of Amendment or Restriction of PHI' form Hs> to document the patient's request and possibly denial of the request.
  - Record the request in the 'AAs – ROI, Breach and Patient's Rights Log'.
  - Ensure payment for the item or service asking to be restricted carries a zero balance and was paid out-of-pocket, not by insurance. If the item or service is paid out-of-pocket and there is a $0 balance, the restriction request is not optional—it must be accepted and followed.
  - Be very careful in agreeing to any restrictions, there are many times when information that was requested for restriction may be present in histories or other encounters which would technically violate the restriction if allowed.
  - Set restriction flags or enter notes in the System (and on paper charts that contain the restricted PHI) to ensure workforce members who may be processing requests for disclosure in the future are aware of these restrictions.
  - Process the restriction request within 60 days.

- If the restriction request escalates past a typical request and response, especially if there is a complaint or investigation, use *'Security or Privacy or Event Report'* form Bs to document the entire process.

- All of the above documentation must be kept for the minimum 6-year HIPAA documentation retention period.

- **Right to Receive Notice of a Breach.** We are required to notify patients by First Class Mail or by email (if the individual has indicated a preference to receive information by email), of any breaches of UNSECURED Protected Health Information as soon as possible, but in any event, no later than <insert State requirements for notification> following the discovery of the breach. Our Organization will investigate any 'event' or incident' where a patient's PHI is known or thought to have been wrongfully disclosed. If it is determined that a breach has occurred both the patient, the Federal and State government will be notified within <insert number of days>. It is important to remember that PHI in Systems that are encrypted are not subject to breach (they are considered to be in the 'breach safe harbor'); however HIPAA violations can still occur, therefore all 'events or incidents must be investigated and corrective actions taken, even if a wrongful disclosure is not determined to be a breach.

  Our Procedures for Breach Determination and Notification

  - *<Insert specifics>*

  - Use the following forms to document the incident report, investigation and corrective actions related to investigating, remediating and notifying affected individuals in the case of a breach.

    - Use <*'Security or Privacy Event Reporting'* form Bs> to document the patient's report of a security or privacy event.

    - Use <*'Investigation and Corrective Actions for Security / Privacy Events'* form Cs> to document the investigation and corrective actions related to security or privacy events.

    - Use <*'Breach Reporting'* form Ns> to catalog the reportable information about a wrongful disclosure or breach.

    - Use the <*'Interim Final Rule Breach Assessment'* Excel form S1s> for breach determination under the Harm Standard (between September 23, 2009 and September 23, 2103) OR the <*'Omnibus Final Rule Breach Assessment'* Excel form Ss> for breach determination after September 23, 2013 in order to document the factors surrounding our determination of whether a HIPAA Violation is deemed a reportable breach.

    - Use <*'Breach Determination and Reporting'* policy 21s> to guide decisions as to whether an event is determined to a breach; upon determination, report to State and Federal government as necessary.

  - Record the request in the 'AAs – ROI, Breach and Patient's Rights Log'.

- Reporting timeframes: OCR (Federal Government) must be notified of a breach within 60 days (if over 500 patients). For breaches that affect fewer than 500 individuals, a covered entity must provide the Secretary with notice annually**.** All notifications of breaches occurring in a calendar year must be submitted within 60 days of the end of the calendar year in which the breaches occurred. <*Insert State requirements for breach reporting*>.

- All of the above documentation must be kept for the minimum 6-year HIPAA retention period.

- **Right to Request Confidential Communications.** Patients have the right to request that we communicate with them about medical matters in a certain way or at a certain location. For example, they can ask that we only contact them at work or by mail. We will not ask them the reason for their request and will accommodate all reasonable requests.

  Our Procedures for Confidential Communications

  - <*Insert specifics*>

  - Use <'*Request for Patient's Rights'* form Gs> to document the patient's request.

  - Record the request in the 'AAs – *Release of Information and Patient's Rights Log'*.

- **Right to a Copy of Our Notice of Privacy Practices (NPP).** If the patient or another party requests a copy of our NPP, be sure to provide it to them in whatever form they wish.

- **Handling Security or Privacy Complaints**

  If a patient, another party or one of the Organization's workforce members, Business Associates or contractors believes that privacy rights have been violated or that a HIPAA violation has occurred, they may file a complaint with the Organization or with the Secretary of the Department of Health and Human Services at the website URL shown below. Always advise the party of their rights and be supportive. Refer to our 'Handling Privacy Complaints Internal and External' policy 20s for guidance.

  http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

Section B: Security

This section of this guide is intended to give a general overview of the security compliance measures undertaken by this Organization. This summary *is not* intended to be an exhaustive list, rather an overview of the more common safeguards we employ. Please refer to our detailed polices, any written procedures and Risk Assessments for more information and statutory language or specific rules.

1. **Risk Assessment** – < Insert specifics, including the date of the last security risk assessment>. Risk Assessment to be updated routinely as the Organization's safeguards materially change, but not less than yearly.

2. **Workforce Clearance –** < Insert specifics of background steps undertaken, if there is ever staff turnover>

3. **Workforce Termination –** < Insert specifics: Workforce members who are terminated will have their access to computer systems and networks removed immediately according to policy timeframes and procedures>.

4. **Access to PHI** – < Insert specifics> All appropriate access to PHI is secured through the use of passwords which are changed routinely; of appropriate strength and unique to each user. All access to PHI is through formal logon. Remote access is via secured data in transit and no data is stored on mobile devices**.**

5. **Password Management –** < Insert specifics> Passwords expire and must be changed every 6 months. Use of more secure passwords, i.e. multiple digit letter number combinations is required**.**

6. **Auto Log-off –** < Insert specifics> Users are logged off of PCs and Servers after periods of inactivity.

7. **Back-up and Restoration –** < Insert specifics> Multiple levels of routine and remote back-ups are maintained. They are tested for restoration integrity and are encrypted data at rest and in transit**.**

8. **Encryption for Breach Safe Harbor –** < *Insert specifics,* tailor to site**;** all practice PHI in transit and at rest is encrypted. Emails should also be encrypted if used for PHI>**.**

9. **Malware Prevention –** Anti-virus, firewall(s), intrusion monitoring, detection and prevention and similar safeguards are all up to date and continually maintained**.**

10. **Physical Security –** The Organization has locks, alarms and segregated records and computers / monitors for patient areas, as practical. Maintenance records for all physical security items are kept for the 6-year HIPAA documentation retention period**.**

11. **Media and Devices –** <Insert details, tailor to site mobile devices are only used by only via secure connection and never store PHI>**.**

12. **Audit Controls –** <Insert EHR Name> maintains an audit log of all user activities which is monitored at least quarterly for inappropriate access, use or disclosure. We also monitor error and technical logs for inappropriate activity on a routine basis**.**

13. **Security and Privacy Training -** < Insert specifics> Workforce members are trained at new hire, at least annually thereafter and whenever there are material changes to the privacy / security rules or job roles which require a different level of training. Security and privacy reminders are discussed at staff meetings and other opportunities. Tests and documentation of the training is kept for the 6-year HIPAA documentation retention period.