HIPAA Manual

HIPAA Manual for Inspirit Therapy Associates

Revision date: 7/25/2025 • 71 pages

Section VI: HIPAA

1.000: HIPAA Program (the Program) Guidances

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

HIPAA Program Processes

All employees and agents will be educated regarding the content of Inspirit Therapy Associates's HIPAA Program upon employment or engagement and annually thereafter. The Program, in its entirety, is organized in policy and procedure modules supported by authenticated resources. Employees and agents acknowledge their education and understanding of the Program by signing the ***HIPAA Training Signature Sheet Form, HIPAA-139.***

All employees and agents of Inspirit Therapy Associates must carry out their duties in accordance with the Program. Any violations of applicable laws and/or deviations from appropriate ethical and professional standards will result in disciplinary action, including dismissal, for the employee or agent. Any supervisor who directs or approves improper actions or is aware of those actions but fails to take appropriate corrective action is subject to the same extent of disciplinary action.

If at any time any employee or agent becomes aware of an apparent violation of the Inspirit Therapy Associates's HIPAA Program, he/she must report it to the HIPAA Officer, his/her supervisor, or the owner or designee. Any person making a report is assured that this report will be treated as confidential and that it will be shared only on a bona fide need-to-know basis.

Inspirit Therapy Associates will take no adverse action against a person making such a report, whether or not the report ultimately proves to be well-founded. Inspirit Therapy Associates will not take any disciplinary action against an employee or agent for reporting a violation of the law to his/her supervisor or any other manager. Failure to report known or apparent violations by an employee or agent, however, could subject them to disciplinary action, up to and including dismissal.

Program Reporting Mechanisms

Any employee/agent who knows of or suspects that a violation of the HIPAA program has occurred is obligated to report the incident within ten (10) working days or sooner to the HIPAA Officer, his/her manager, or the owner or designee.

In the event that an employee/agent is uncomfortable with directly reporting a violation, he/she may provide a written anonymous report of the incident to the HIPAA Officer, his/her supervisor, or the owner or designee.

Program Monitors

1. Inspirit Therapy Associates's HIPAA Officer will maintain a ***Compliance Investigation Log Form, FM 103.*** This log will list:
    a. The violation
    b. The date of the report
    c. The investigation status
        i. Open—facility investigation
        ii. Open—outsourced investigation
        iii. Closed—with corrective action taken and date
        iv. Closed—inconclusive—no corrective action required
2. All report details, including the names of individuals under investigation, are considered confidential material and/or protected under attorney/client privilege and will be managed accordingly. Employees/agents wishing to review the Investigation Log must obtain the HIPAA Officer's authorization.
3. The HIPAA Officer for Inspirit Therapy Associates will provide its executive board, as applicable, with an annual report that includes, but is not limited to, any Program violations and associated actions.
4. A summary of any compliance violation and action taken to correct or prevent compliance problems must be documented and secured under the attorney/client privilege as needed.
5. The ***HIPAA Training Signature Sheet Form, HIPAA 139,*** must be signed by each employee/agent upon initial orientation and annually thereafter.

1.001: Use, Disclosure, Authorization & Release of PHI

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

POLICY:

Inspirit Therapy Associates will comply with all Federal, State, and professional standards and regulations relating to the use and disclosure of protected health information, regardless of the

medium in which it exists. We have a Notice of Privacy Practices that details our procedures in complying with legal and ethical mandates that guide us.

DEFINITIONS & ACRONYMS:

Business Associate (BA): A business associate is a person or entity that performs certain functions or services for or on behalf of a HIPAA-covered entity (e.g., healthcare provider, health plan, or healthcare clearinghouse) that involves the use or disclosure of Protected Health Information (PHI).

Covered Entity (CE): A covered entity is:

1. Health Plan
2. Provider
3. Clearinghouse

Disclosure: Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Electronic Protected Health Information (EPHI): EPHI is PHI maintained (at rest) or transmitted (in transit) in electronic form. Examples of EPHI at rest include patient information stored on magnetic tapes, optical discs, hard drives (both internal and external), DVDs, USB thumb drives, and servers. EPHI transmission occurs when EPHI is being sent between computer systems. The risks are generally more significant when EPHI is being transmitted outside of an organization's internal network, including Internet and extranet technology, leased lines, and private networks; however, insiders pose significant risks, and study results show that most breaches (confidentiality breaches) are from authorized users.

Notice of Privacy Practices (NPP)

The NPP is a document provided by healthcare providers, health plans, or other entities covered under the Health Insurance Portability and Accountability Act (HIPAA). It informs patients or clients about how their protected health information (PHI) may be used, disclosed, and safeguarded, as well as their rights regarding their health information.

Protected Health Information (PHI): This means individually identifiable information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity) that can be linked to a specific individual.

PHI does not include educational records covered by the Family Educational Rights and Privacy Act, employment records held by a covered entity in its role as an employer, and information regarding a person who has been deceased for more than fifty (50) years.

Treatment, Payment & Operations (T-P-O): Treatment, Payment, and Healthcare Operations (TPO) are key categories that describe permissible uses and disclosures of Protected Health Information (PHI) by covered entities (e.g., healthcare providers, health plans, and healthcare clearinghouses) without requiring patient authorization.

1. Treatment: The provision, coordination, or management of healthcare and related services for an individual, including consultations and referrals between providers.

2. Payment: Activities undertaken by a healthcare provider or health plan to obtain payment or be reimbursed for services or to determine eligibility for coverage.

3. Healthcare Operations: Administrative, financial, legal, and quality improvement activities necessary to run a covered entity's business and support treatment and payment functions.

Use: Means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not the covered entity or business associate pays them.

CONDITIONS FOR USE, DISCLOSURE & AUTHORIZATION:

We are required by federal and state laws, as well as ethical standards, to protect the privacy of our patients' health information. For example, federal health information privacy regulations require us to protect patient information in the manner described in our Privacy Notice. Certain types of health information may specifically identify the patient. Because we must protect this health information, we refer to it as Protected Health Information—or "PHI." In our Privacy Notice, we describe:

1. How we use PHI.

2. When we may disclose protected health information (PHI) to others.

3. The Patient's Privacy Rights and How to Exercise Them.

4. Our privacy duties.

5. Who to contact for more information and/or complaints.

Inspirit Therapy Associates Uses, Discloses, and Releases Protected Health Information in the following manner and under the following conditions:

1. Use and Disclosures for Treatment, Payment & Healthcare Operations

    a. Treatment

        We use and disclose PHI in the course of a patient's treatment. For instance, once we have completed an evaluation or re-evaluation, we send a copy or summary of our report to the patient's referring practitioner, if applicable. We also maintain records detailing the care and services that patients receive at our facility, ensuring accuracy and consistency in the delivery of that care in an optimal manner. That record also helps us meet certain other professional and legal requirements. These records may be used and/or disclosed by members of our workforce to ensure that proper care is rendered. Inspirit Therapy Associates will adhere to the 'minimal necessary' stipulations as noted

in PHI-E-PHI & Proprietary Data: Confidentiality, Use, Disclosure & Access, HIPAA Policy 1.007.

b. Payment

After treating a patient, we typically bill a third party for the services provided. We will collect the treatment information, enter the data into our computer system, and then process the claim either on paper or electronically. The claim will note the patient's health problem and the treatments rendered, and it will include other relevant information, such as the patient's social security number, insurance policy number, and other identifying details. If a Social Security number is required, the first five digits will be redacted. The third-party payer may request a copy of the patient's treatment records to help determine that the services were medically necessary.

If a patient chooses to pay for services in full without involving a third party (such as an insurer or employer), he/she may request that we not disclose any information regarding the services for payment purposes. The patient will be provided with a Good Faith Estimate (GFE) for all self-pay visits or treatments, regardless of the reason. Exception: You will not receive a GFE if you are enrolled in Medicare Part A, B, or C, Medicaid, TRICARE, Veterans Affairs, or Indian Health Services.

c. Health Care Operations

We also use and disclose PHI in our healthcare operations. For example, our therapists meet periodically to review clinical records and monitor the quality of care at our facility. Patient records and PHI could be part of these quality assessments. Sometimes, we offer student internship programs and utilize the PHI of actual patients to assess their skills and knowledge. Other healthcare data (PHI) may be involved in business planning, compliance monitoring, or even the investigation and/or resolution of a complaint.

d. Special Uses and Disclosures

We may also use or disclose PHI to assist us in carrying out specific responsibilities to our patients, such as:

i. Remind patients of appointments

ii. Release equipment and/or supplies to a patient's designee

iii. Carry out follow-ups on home programs or discharge planning

iv. Advise patients of new or updated services or home supplies via telecommunication or a newsletter

v. Update the patient's workers' compensation case worker or employer

vi. Carry out research that does not directly identify the patient

vii. Carry out marketing functions, such as providing nominal promotional gifts

viii. Notify the patient of fundraising functions

Prior to implementing any of the above Special Uses and Disclosures, this facility will provide the patient with the opportunity to decline our implementation of all of the above, with the exception of V (Update patient's workers' compensation case worker or employer).

We will obtain written authorization before using PHI for marketing purposes when required by law. Additionally, all other electronic communication will be conducted based on the patient's request or authorization. This facility will use only secure transmissions to mitigate the risk of unauthorized access. We recommend that our patients utilize secure communications for all sensitive information.

2. Uses and Disclosures that are Permitted and/or Required

Many laws and regulations govern our interactions with patients, affecting the disclosure of their PHI; they may either require or permit us to disclose it. The following is a list from the federal health information privacy regulations describing required or permitted uses and disclosures without patient authorization:

a. Permitted:

   i. We may share PHI with a family member or friend if he/she is clearly involved with the patient's care and if the patient does or has not objected (verbally);

   ii. We may use PHI in an emergency if the patient is unable to express him or herself;

   iii. We may use or disclose a patient's PHI for research if we receive specific assurances that protect the privacy of the individual;

   iv. We may update the patient's workers' compensation case worker or employer.

b. Required:

   i. We must release PHI when required by law, i.e., ordered by a court;

   ii. We must report communicable diseases or adverse reactions to drugs to the appropriate public health, federal department, or agency;

   iii. We must report neglect, abuse, or domestic violence;

   iv. We must allow access to and disclosure of PHI to government regulators for compliance audits and surveys;

   v. We must allow access to or provide PHI as a response to a judicial or administrative proceeding, such as a valid subpoena or protective order;

   vi. We must report and/or respond to legal requests of law enforcement officials or other legal entities relating to criminal activities, such as gunshot wounds;

   vii. We must disclose PHI to avert a health hazard or to respond to a public health threat, such as an imminent crime against another person;

viii. We must release the PHI of a member of the armed forces upon request of the appropriate military command authorities;

ix. We must release PHI in connection with certain types of organ donor programs;

x. We must comply with state regulations that are more stringent than federal laws;

Note: The Reproductive Healthcare Rule per Purl v HHS declared major portions of the 2024 RHC Rule to be unlawful, and it vacated those provisions. Under the Administrative Procedure Act (5 U.S.C. § 706(2)), when a court "sets aside" an unlawful agency action, the regulation ceases to exist, with OCR treating the RHC Rule and attestation requirements as void.

Unless a state passes legislation that is more stringent than HIPAA's Use and Disclosure provisions, providers are not required to comply with the 2024 RHC Rule unless reinstated on appeal or by new rulemaking. Providers should apply HIPAA Privacy Rule standards for Use and Disclosure as stipulated above.

3. Authorization for the Release of Protected Health Information

Only under the conditions noted above (Sections 1 & 2) do we have the right to use and disclose a patient's protected health information without a patient's authorization. If a patient desires to provide access to his/her PHI, for instance, to his/her PHI to designees or participate in a research project, we will provide an authorization form for his/her completion.

In certain circumstances, this facility may need or desire to use and/or disclose a patient's PHI. In such situations, we must obtain the patient's permission and provide him/her with an authorization form for completion to ensure his/her consent. An example is that an authorization would be required by law to allow Inspirit Therapy Associates to directly or indirectly receive compensation in exchange for disclosing a patient's PHI.

Inspirit Therapy Associates has a HIPAA compliant ***Authorization for Release of PHI Form HIPAA-143,*** which we provide to our patients. A patient may revoke his/her authorization at any time with a written notice (see Protected Health Information (PHI) & Patient Rights under HIPAA, HIPAA Policy 1.003) using the ***Authorization Revocation Request Form HIPAA-152,*** or its equivalent.

4. Procedure for Authorization and Release of Information

{{Policy_R001001_01A}}

{{Policy_R001001_02A}}

Authorization for Release of PHI Form HIPAA-143

a. The Business Office staff will be the first-line source for answering questions about the Authorization Form; however, the HIPAA Officer will be the individual to handle non-routine questions and/or complaints.

b. Once the patient fills out the authorization form, he/she will give it to the business office staff member, who will review it for completion. If the form is complete, the Business Office staff member will make one copy of the form, the original form will be placed in the patient's chart, and the copy will be provided to the patient.

c. If an incidental request for access (e.g., a request to speak to or give a message to a patient) is received by the Business Office, the person accepting the request will check the patient's chart for the requestor's authorized access and then will proceed to validate the identity of the requestor. The Business Office staff member will then release or decline to release the information based on the authorization permits and identity validation. Authorized disclosures of PHI are exempt from disclosure accounting.

d. If a request is mailed or faxed to the Business Office, the staff designee will verify the patient's chart for the requestor's authorized access, validate the person's identity, and release or decline to release the information based on their findings. If the release is permitted and/or required per "HIPAA's Required Listed noted in 2b (i-ix) and HIPAA Policy 1.002 and is substantiated as 'required' the subject, date, and purpose of the release will be logged on the ***Accounting for Disclosures Log Form HIPAA 155,*** or its equivalent and the release of the PHI will occur.

e. All validated requests for the release of PHI are subject to reproduction and labor cost fees, with the exception of those from healthcare providers, workers' compensation case workers/employers, etc., schools, and not-for-profit organizations.

f. All requests for release of PHI, in any medium, will be honored within thirty (30) days of receipt of a valid authorization from the patient and a written request from the requesting party.

g. If a requestor is denied access to any PHI, including but not limited to the presence of the patient in the clinic, the requestor will be told that Inspirit Therapy Associates is restricted from releasing any information without proper authorization. He/she will be advised to contact the patient directly to obtain that authorization.

1.002: HIPAA Authorization for Release of Protected Health Information

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

POLICY:

It is the policy of Inspirit Therapy Associates to comply with the HIPAA Privacy Rule regarding the use and/or disclosure of protected health information (PHI). This facility requires a valid and written authorization for the release of PHI as described below.

The HIPAA Officer or his/her designee will determine whether an authorization is required when a request for disclosure is received. A valid authorization will be requested from the patient or his/her legal representative if the HIPAA Officer or designee determines that the request for information is outside the parameters of treatment, payment, or healthcare operations. The

relationship and legal authority of the patient's representative will be assessed and must be documented on the authorization form.

Authorizations are never required for the release of PHI under the following conditions:

1. Requests made by the patient or his/her legal representative.
2. Requests for treatment information.
3. Requests for billing and payment purposes.
4. Requests needed for the Inspirit Therapy Associates's healthcare operations, such as clinical or billing audits.
5. Requests by the Secretary of the U. S. Department of Health and Human Services when determining HIPAA compliance.
6. Requests by other state or federal agents pursuant to other regulations.
7. Requests for the release of PHI are required by law, i.e., they are ordered by a court.

This facility does not need authorization from the patient to release PHI when we:

1. Must report communicable diseases or adverse reactions to drugs to the appropriate public health or federal department or agency.
2. Must report neglect, abuse, or domestic violence.
3. Must allow access to and disclosure of PHI to government regulators for compliance audits and surveys.
4. Must allow access to or provide PHI as a response to a judicial or administrative proceeding, such as a valid subpoena or protective order.
5. Must report and/or respond to legal requests of law enforcement officials or other legal entities relating to criminal activities, such as gunshot wounds.
6. Must disclose PHI to avert a health hazard or to respond to a public health threat, such as an imminent crime against another person.
7. Must release the PHI of a member of the armed forces upon request of the appropriate military command authorities.
8. Must release PHI in connection with certain types of organ donor programs.

Refer to Use, Disclosure, Authorization & Release of PHI HIPAA Policy 1.001 for the Authorization Procedure.

Refer to the ***HIPAA Authorization Content Form HIPAA, 100.***

1.003: Protected Health Information (PHI) & Patient Rights under HIPAA

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

DEFINITIONS:

Implementation Specifications: These are specifications that provide direction as to how Security Standards should be executed.

Required Implementation Specifications: These are specifications that “must” be implemented, i.e., they are not optional procedures.

Addressable Implementation Specifications: These are specifications that must be implemented as stated in the rule or in an alternative manner that better meets the organization's needs while still adhering to the intent of the implementation specification. Addressable implementation offers some flexibility to organizations in implementing the standard; however, the standards are not optional, and all must be addressed. Organizations must maintain formal documentation about why and how the implementation specification in the security rule was implemented. The decision can be based on a variety of factors, such as the entity's risk analysis, risk mitigation strategy, existing security measures, and the cost of implementation.

POLICY:

Inspirit Therapy Associates will comply to the fullest extent with all provisions of the Healthcare Insurance Portability & Accountability Act (HIPAA) relating to Transaction & Code Sets Standards, Privacy and Security Rules, and Health Information Technology for Economic and Clinical Health (HITECH) as per the American Recovery and Reinvestment Act (ARRA). The security rules ‘required’ implementation specifications will be carried out as stipulated, and the ‘addressable’ implementation specifications will be continually reviewed and implemented using ‘sizable’ procedures and processes.

Inspirit Therapy Associates’s Notice of Privacy Practices (NPP) serves as the foundation for privacy behavior within the facility, guiding the day-to-day management of Protected Health Information (PHI) and serving as a communication vehicle with its patients. The Patient Rights, mandated by HIPAA and reiterated in the NPP, have been thoroughly reviewed by Inspirit Therapy Associates’s workforce. HIPAA education is provided upon hiring, and updates will be provided as needed and/or when new regulations and/or guidelines are published.

Patient Rights as reflected in Inspirit Therapy Associates’s Notice of Privacy Practices and as required by HIPAA and HITECH are summarized below:

Note: This facility will provide patients with a written notice of the risks of transmitting protected health information (PHI) via unsecured email or messaging platforms. Patient authorization will be obtained before initiating or responding to any such electronic communication.

1. The Patient Has the Right to Request Limited Use or Disclosure

   The patient has the right to request that we not use or disclose his/her PHI in a particular

way, and we will grant that request whenever possible. However, we are not required to abide by his/her request and do not have to provide a reason. If we agree to his/her request, we must comply with the agreement. We have the right to request that the request be in writing, and we will exercise that right, preferably on the ***Request for Confidential Communication Form HIPAA 150.*** Unless otherwise directed by the patient or his/her representative, Inspirit Therapy Associates will disclose PHI to:

a. Remind patients of appointments;

b. Release equipment and/or supplies to the patient's designated representative;

c. Carry out follow-ups on home programs or discharge planning;

d. Advise patients of new or updated services or home supplies via telecommunication or a newsletter;

e. Update the patient's workers' compensation case worker or employer;

f. Carry out research that does not directly identify the patient;

g. Carry out marketing functions such as providing nominal promotional gifts or advertising services.

h. Notify the patient of fundraising events.

Note: A patient may opt out of notification and/or engagement in all of the above, except for letter (e) above, as it is required per HIPAA unless restricted by state law. If we receive direct or indirect financial remuneration from a third party for marketing a product or item or for any fundraising we are engaged in, we will offer you the opportunity to opt out of receiving any of these materials. We will obtain written authorization before using PHI for marketing purposes when required by law.

2. Objection and Exception:

a. An objection to release or a request to limit PHI for payment purposes will not be honored by this facility if a third party makes a payment. We will promptly advise the patient of this rejection. Inspirit Therapy Associates reserves the legal right to decline to provide treatment should the patient persist in restricting the release of PHI for payment when a third party is utilized for payment.

b. Exception: Requests to restrict disclosure for items and/or services received that are personally paid for (no third-party payment) will be honored for all situations outside of treatment, which will not have restrictions other than under the 'minimal necessary' provision. This Patient Right does not supersede Medicare's Mandatory Claim Submission requirements unless the provider is enrolled in Medicare, the provision was requested by the patient, and the covered entity did not initiate it. ***Cash-based payments to Medicare & Non-Medicare Patients, BOM-207*** should be utilized, and the patient's signature should be obtained.

3. The Patient Has the Right to Confidential Communication

The patient has the right to receive confidential communications from us at a location or phone number that he/she specifies. We reserve the right to request that the request be submitted in writing. We will exercise that right, preferably on the ***Request for Confidential Communication Form HIPAA 150.*** Compliance with this request will include the stipulation that this alternative mode of communication should not hinder or defer payment or collection notices.

a. Procedure: A request may be submitted in person, by mail, or by e-mail

   i. Mailed requests should be addressed to:

      Inspirit Therapy Associates
      c/o {{Name_of_Owner_or_Designated_HIPAA_Officer}}
      {{Street}}
      {{City}}, {{State}}, {{Zip_Code}}

   ii. Faxed requests should be addressed to:

      Inspirit Therapy Associates
      c/o {{Name_of_Owner_or_Designated_HIPAA_Officer}}
      {{Fax_Number}}
      feelbetter@inspiritpt.com

b. Procedure: If the patient requests confidential communication, he/she will be asked to put it in writing, preferably on the ***Request for Confidential Communication Form HIPAA 150***, with the following information:

   i. The type of information being managed confidentially includes specific conditions, treatments, dates of services, and other relevant details.

   ii. The period for which the request applies

   iii. The manner in which the patient wishes to receive confidential communications

   iv. The manner in which payment will be received if the confidential communication involves an alternate address

c. Procedure: If the patient requests an alternate phone number, contact Inspirit Therapy Associates will note it as the primary/preferred number and record the other phone number as an emergency number. The data screen and/or intake form should be flagged/highlighted to emphasize the preferred phone number.

d. Procedure: If the patient requests an alternate address for statement mailing, Inspirit Therapy Associates will first confirm and obtain assurance that payment consent will not be compromised. This facility will enter the alternate address as the primary/preferred mailing address and record the home address as the emergency contact site. The data screen and/or intake form should be flagged/highlighted to emphasize the preferred address.

3. The Patient Has the Right to Access, Inspect, and Copy His/Her PHI

The patient has the right to access, inspect, and copy his/her PHI. Should we decline, we must provide him/her with a resource person to assist in reviewing our refusal decision. We

must respond to the patient's request within thirty (30) days. We may charge reasonable fees for supervised inspection time, copying, and/or labor time related to copying. We reserve the right to require an appointment for record inspection. We also reserve the right to request written confirmation of the patient's request. We will exercise this right, preferably using the ***HIPAA 193 Request for Access to PHI Form.***

Procedure for Patients:

Patient Access to PHI

Patients may request access to their PHI by submitting a written request to Inspirit Therapy Associates's HIPAA Officer or designee. The patient will be asked to use the ***HIPAA-193 Request for Access to PHI Form***, if possible. The form specifies that access will be granted within thirty (30) days of its receipt unless otherwise notified. It identifies the fees that will be charged for the supervised inspection, copying, or summarizing of the record, and it details the access requirements listed below, requiring that the patient:

a. State the type of access request (inspection, copy of all or specified records, or a summary of the records).

b. Specify the dates and specific information.

c. Sign and date the request and provide proper identification upon accessing the records.

Methods of Inspecting and Copying:

a. Inspect: Patients may inspect/read their clinical and billing records and associated documents under the supervision of a staff member (an inspection fee may be charged if the access is more frequent than once annually or if the inspection duration exceeds thirty (30) minutes.

b. Copy: Patients may obtain a copy of all or a portion of their clinical and billing records, including associated documents in paper or electronic format (if such records are maintained electronically). A copying/duplication fee, including labor costs, may be charged.

Procedure: Business Office Staff

a. The Business Office staff member refers all Access Requests to the HIPAA Officer after verifying the request, confirming that all of the prerequisite information has been provided by the patient, including, but not limited to, an authentic signature;

b. If the request is incomplete, the Business Office staff designee will forward the request to the patient, noting any deficiencies. If the request is complete but the records have deficiencies, the chart will be forwarded to the appropriate person(s) for completion when necessary and in accordance with the law. If the request and the chart are complete and the patient has requested a PHI inspection, the Business Office designee will set an appointment for the patient with the HIPAA Officer or his/her designee, who will be present during the inspection. The patient will not be allowed to remove any documents from the file or make any entries;

c. If the patient wishes to amend the record, he/she will be advised of the amendment procedure;

d. If the patient has questions about billing information, the HIPAA Officer may address them during the inspection appointment or at a later date if further research is required;

e. If the patient has a question about his/her clinical record, he/she will need to make an appointment to meet with the appropriate therapist;

f. If the request form and chart are complete and the patient has requested PHI copying, then the Business Office staff designee will make the specified copies and distribute them to the patient in the format specified by the patient (paper or electronic).

g. If there is a delay in allowing access, the patient will be provided with a written extension statement specifying an access date, not to exceed an additional thirty (30) days;

h. If the HIPAA Officer has preliminarily denied access, it must be based on either Unreviewable Grounds (e.g., civil, criminal, or administrative action or proceedings) or Reviewable Grounds (e.g., safety or life endangerment). The HIPAA Officer will forward all potential denials to the owner or designee;

i. The HIPAA Officer will review the request and approve or deny the access based on all of the above conditions;

j. The ***Authorization for Release of PHI Form HIPAA-143*** and all supporting data will be filed in the patient's clinical file;

k. Any patient requests for records not created by this facility will be returned to the patient; if the location of the requested information is known, it should be included in the communication to the patient.

4. The Patient Has the Right to Revoke His/Her Authorization

If the patient has authorized us to use or disclose his/her PHI, he/she may revoke it at any time in writing. The patient must understand that we relied on the authority of his/her authorization prior to the revocation and used or disclosed his/her PHI within its scope.

a. Procedure: The Business Office designee forwards any patient request to revoke authorization to the HIPAA Officer. The HIPAA Officer will carry out the revocation if the request is in writing and provides sufficient information to facilitate the revocation. The HIPAA Officer will sign off on the revocation and inform the designated Business Office staff member; the designated Business Office staff member will document the change and insert the signed revocation in the patient's chart. The HIPAA Officer will contact the patient if the requested revocation is incomplete and will initiate the proper procedures to facilitate the revocation for the patient;

b. The Patient Has the Right to Amend His/Her PHI;

The patient has the right to request an amendment of his/her record. We reserve the right to request the request in writing. We will exercise that right, Inspirit Therapy Associates prefers that its Request To Amend the ***Designated Record Set (DRS) Amendment Request Form HIPAA 153*** be utilized. We may deny that request if the

record is accurate and/or if the record was not created by Inspirit Therapy Associates. If we accept the amendment, we must notify the patient and make an effort to inform others who have the original record.

5. The Patient Has the Right to Know Who Else Sees His/Her PHI (Hardcopy)

   The patient has the right to request an accounting of certain disclosures that we or our business associates have made over the previous six years. We do not have to account for all disclosures, including those made directly to the patient, those involving treatment, payment, or healthcare operations, those to family/friends involved in their care, and those involving national security. The patient has the right to request an accounting annually; we have the right to ask for the request in writing and to charge for any accounting requests that occur more than once per year; we must advise the patient of any charge, and the patient has the right to withdraw his/her request or to pay to proceed. Inspirit Therapy Associates prefers that the ***Disclosure Accounting Request Form HIPAA 154*** be utilized, if possible.

6. The Patient Has a Right to be Informed of a Breach of His/Her Privacy

   We are required to notify the patient by first-class mail or by e-mail (if 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 sixty (60) days following the discovery of the breach, unless otherwise required by state law. “Unsecured Protected Health Information” is information that is not secured through the use of a technology or methodology identified by the Secretary of the U.S. Department of Health and Human Services to render the Protected Health Information unusable, unreadable, and undecipherable to unauthorized users. The notice is required to include the following information:

   a. A description of the breach, including the date of the breach and the date of its discovery, if known;

   b. A description of the type of unsecured protected health information involved in the breach;

   c. Instructions regarding the measures the patient should take to protect him/her from potential harm resulting from the breach;

   d. Correction action Inspirit Therapy Associates has/will take to investigate the breach, mitigate losses, and protect the patient from further breaches;

   e. Inspirit Therapy Associates 's contact information, including a toll-free telephone number, email address, website, or postal address, to facilitate additional questions. (See Breach Notification Requirements, HIPAA Policy 1.021 for full details).

7. The Patient Has the Right to Complain

   The patient has the right to complain if he/she feel his/her privacy rights have been violated. The patient may complain directly to us or the Secretary of Health and Human Services/Office of Civil Rights (OCR). We will not retaliate against a patient if he/she file a complaint about us. All complainants should provide a reasonable amount of detail to enable us to investigate the concern. Inspirit Therapy Associates prefers that the ***HIPAA Complaint***

Form, HIPAA 156, be utilized, if possible. To file a complaint with us, the patient should contact:

Name:	{{Name_of_Owner_or_Designated_HIPAA_Officer}}
Address:	{{Street}} {{City}}, {{State}} {{Zip_Code}}
Phone:	(920) 338-9670
Fax:	{{Fax_Number}}
Email:	feelbetter@inspiritpt.com

Note: In order for the Office of Civil Rights to investigate a complaint, it must be filed within one hundred and eight days (180) of the violation.

8. The Patient Has the Right to Receive a Copy of the Privacy Notice (NOTICE)

   Inspirit Therapy Associates is obligated to provide patients with a copy of its Notice of Privacy Practices and to post the Notice in a conspicuous place for patients to access, as well as on its website. We reserve the right to modify the Notice to comply with policy, rules, or regulatory changes. We are obligated to provide new notices to current and subsequent patients as changes are made. We are required to maintain each version of a Privacy Notice for a minimum of six (6) years, along with the signed NPP receipts. HHS discontinued the requirement for providers to obtain a signed NPP receipt to reduce administrative burdens in the HHS 2024 Final Rules.

9. The Patient Has the Right to Expect Protection of Any Substance Use Disorder or Treatment Records According to 42 CFR Part 2 (Substance Use Disorder Records)

   Inspirit Therapy Associates is required by federal law to protect the privacy of a patient's substance use disorder (SUD) treatment records. These records are protected by 42 CFR Part 2, which provides additional confidentiality safeguards beyond those required by HIPAA. Part 2 protects any information that identifies the patient as having a substance use disorder or receiving SUD treatment services, including the patient's diagnosis, treatments, medications for SUD, appointment information, billing records, and any other information that could identify the patient. We may not use or disclose SUD treatment records without the patient's written consent unless federal law allows it. Part 2 permits disclosure without the patient's consent in limited circumstances, such as:

   a. Medical emergencies
   b. Scientific research under strict safeguards

   c. Audits or program evaluations
   d. Court orders that meet specific legal requirements
   e. Reporting suspected child abuse or neglect as required by law
   f. Crimes committed on program premises or against program staff

   The patient may authorize us to disclose SUD treatment information to others, including for treatment, payment, or healthcare operations. Authorization must meet the requirements of 42 CFR Part 2. An authorization may be revoked at any time. If we disclosed SUD information per the patient's valid authorization, we will cease any further disclosures from the effective date of the revocation.

Any recipient of a patient's SUD treatment or program information is prohibited from redisclosing it unless the patient gives written permission or the disclosure is otherwise permitted by Part 2. Federal law does not protect information if the patient voluntarily discloses it to others who are not covered by HIPAA or bound by Part 2.

Patient Rights Related to SUD Information: The patient has the right to:

a. Request restrictions on how the SUD information is used or disclosed.

b. Request an accounting of disclosures of his/her Part 2–protected information.

c. Receive a copy of this Notice and any updates.

d. File a complaint if he/she believes their privacy rights have been violated; we are prohibited from retaliation against the patient for filing a complaint.

1.004: Electronic Communication: Computer, Internet & E-mail Utilization

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

This policy does not require modification except for names

POLICY:

Computers and associated hardware and software provided to access and utilize the internet and e-mail are intended solely for business use and are at all times the property of Inspirit Therapy Associates. All documents composed, transmitted, or received via the company's server/network, whether on or off company time, are considered the company's official records and property.

Strict adherence to Use, Disclosure, Authorization & Release of PHI, HIPAA Policy 1.001, HIPAA Performance Feedback, HIPAA Policy 1.027, HIPAA Positive Corrective Action & Sanctions, HIPAA Policy 1.029, and Court Ordered Subpoena & Legal Counsel Request for Records, HIPAA Policy 1.031 is expected of all employees under all conditions, but also, specifically, as they relate to electronic communication.

PROCEDURE:

Each employee will be provided with this policy as part of orientation and as an inclusion in his/her Employee Handbook. Each employee will have the opportunity to clarify any questions regarding proper and permitted electronic communication during orientation and throughout his/her employment. All questions and concerns should be directed to the Business Office Manager, HIPAA Officer, or Compliance Officer, as outlined in the Code of Conduct Standards & the Compliance Program Requirements (located in the HR Manual).

Any related or observed policy violation, whether suspected or confirmed, will be investigated and pursued with expediency. If confirmed, it will be managed to the fullest extent of the disciplinary policy.

Inspirit Therapy Associates reserves the right to monitor computer access and utilization and to take action to ensure compliance with this and related policies.

1.005: Record, Electronic Media & Device Retention &/or Disposal Guidelines

Effective/Revision Date: {{Policy_DATE1005}}

Policy Classification(s): HIPAA

Content items must be addressed and can be customized to fit the practice, but core elements are required. Retention schedules for non-PHI-E-PHI may be revised per state statute.

Policy:

It is the policy of Inspirit Therapy Associates to comply with all Federal, State, and industry standards relating to record/data/document and device retention and disposal as noted in the retention and disposal schedule of this policy. This includes, but is not limited to, Protected Health Information and any of the facility's proprietary materials, whether maintained on paper, electronic media, or cloud-based systems.

All records/data/documents and devices, including the electronic media on which it is stored, are maintained or destroyed in accordance with prevailing regulations. At no time will the disposal schedule supersede the company's policy to retain all ongoing investigational reports, documents, notes, memoranda, and other relevant materials. This retention and disposal policy complies with both the HIPAA privacy and security rules and other regulatory bodies that enforce retention schedules.

Paper PHI

{{Policy_R001005_01A}}

{{Policy_R001005_02A}}

All PHI waiting for shredding will be:

1. Bagged and tagged PHI -"Shredding Required", or
2. Secured in the shredder vendor's container

Electronic Media and Data

To HIPAA-compliantly remove specific files and folders containing protected health information (PHI) from electronic media and storage devices, you must ensure that the data is securely and permanently deleted to prevent unauthorized access or recovery. Below is a step-by-step guide to achieve this:

1. Understand HIPAA Requirements

a. HIPAA requires that PHI be disposed of in a way that renders it "unreadable, indecipherable, and unable to be reconstructed" (see 45 CFR § 164.310(d)(2)(i)).

b. Simply deleting files or formatting a drive does not meet HIPAA standards, as data can often be recovered unless properly overwritten.

2. Identify Files and Folders Containing PHI

a. Locate all files and folders on your device that contain PHI. This may include documents, spreadsheets, databases, emails, or backups.

b. Check common locations such as the Desktop, Documents, Downloads, and email clients.

c. Ensure you include temporary files, cached data, or cloud-synced folders (e.g., Google Drive, Dropbox) that may contain PHI.

3. Use Secure Deletion Tools

a. To permanently delete files and folders, use software that overwrites the data multiple times to prevent recovery. Examples of HIPAA-compliant secure deletion tools include:

i. Eraser (Windows-free software): Overwrites files with multiple passes.

ii. CCleaner (Windows/Mac-Home version is free): Offers secure file deletion options.

iii. Shred (Linux/Mac): A command-line tool for overwriting files.

iv. Secure Eraser (Windows): Supports multiple overwriting standards.

v. FileVault or Disk Utility (Mac): For secure erasure of files or entire drives.

4. Steps for Secure Deletion:

a. Install and configure the secure deletion tool.

b. Select the specific files or folders containing PHI.

c. Choose a deletion method that complies with standards like DoD 5220.22-M (3-7 passes of overwriting) or NIST 800-88 (guidelines for media sanitization).

d. Run the tool to overwrite and delete the files.

5. Clear Temporary Files and Cache

a. PHI may reside in temporary files, browser caches, or system logs. Use tools like CCleaner or manually clear:

i. Browser history and cache.

ii. Recycle Bin (Windows) or Trash (Mac).

iii. Temporary folders (e.g., %temp% on Windows or /tmp on Linux/Mac).

iv. Ensure these are also securely overwritten using the tools mentioned above.

6. Remove PHI from Cloud Sync Services

   a. If PHI was synced to cloud services (e.g., OneDrive, Google Drive, etc.), log in to the service and securely delete the files from the cloud.

   b. Empty the cloud service's trash or recycle bin.

   c. Verify that no local synced copies remain on the laptop.

7. Verify Deletion

   a. Use data recovery software to attempt to recover the deleted files and confirm they are unrecoverable. If any PHI is still recoverable, repeat the secure deletion process. Examples of recovery software include:

      i. Recuva

      ii. TestDisk

8. Document the Process

   a. HIPAA requires documentation of data disposal processes (45 CFR § 164.310(d)(2)(i)). Document the following:

      i. The files/folders that were deleted.

      ii. The secure deletion method used (e.g., software, number of overwrite passes).

      iii. The date and time of deletion.

      iv. Verification steps were taken to ensure that the data was unrecoverable.

      v. Maintain a personal copy of the deletion documentation.

      vi. Send a copy of the deletion documentation to the HIPAA Officer or IT Manager.

If an electronic device is being decommissioned, disposed of, or repurposed, the NIST 800-88 guidelines for media sanitization, which may include physical destruction of the hard drive, must be followed to ensure unauthorized access is accomplished by rendering the E-PHI unrecognizable or beyond reconstruction.

The three sanitization methods for all electronic media containing PHI, as outlined in the NIST Framework, are:

1. Clear: Overwrites data in user-addressable storage to prevent simple, non-invasive recovery.

2. Purge: Uses advanced techniques (e.g., cryptographic erasure or degaussing) to make data recovery infeasible, even with sophisticated tools.

3. Destroy: Physically destroys the media to render data irretrievable, making the device unusable.

When this facility performs the destruction/disposal internally, it maintains documentation of the destruction of PHI, EPHI, and electronic media, which includes:

- The patient's name and account record number.
- The patient's date of birth (cross-check for age of minority).
- The date of destruction.
- The method of destruction.
- Description of the software and hardware destroyed (if applicable).
- The signatures of the individuals supervising or witnessing the destruction.

When this facility outsources destruction/disposal services, all of the above requirements, as well as the following requirements, must be met:

1. Documentation: Generate a Certificate of Sanitization or Certificate of Destruction for each device (by serial number) to demonstrate compliance.
2. Verification: Confirm the effectiveness of Clear or Purge (e.g., checking that the device boots to a setup screen or that encryption keys were deleted).
3. Chain of Custody: Maintain secure transport to third parties (e.g., for destruction or recycling).
4. Business Associate Agreements: Required for third-party vendors handling sanitization or destruction.

Resources containing the Guidelines from NIST on non-paper data and media sanitization, destruction, and methodologies are located in the Compliance Bubble under HIPAA Forms and Resources.

Portable and Removable Media

PHI sensitivity will be assessed, and the disposal method for portable or removable media will be based on the level of sensitivity and encryption status.

USB Drive Sanitation Methods

1. Clear technology will be used to overwrite non-sensitive data on storage devices that will be reused within the organization. This method protects against simple recovery techniques.
2. Purge technology uses advanced techniques to render sensitive data recovery infeasible. This method will be used for data that leaves the organization.
3. Destruction technology will be used to destroy media, ensuring that highly sensitive data is irretrievable, regardless of organizational control.

Compact Disk Sanitation Methods

- Destruction technology will be used to destroy the media on CDs, ensuring the data is irretrievable.

Other Portable Media (floppy disks, memory cards, external hard drives, tape cartridges, and other removable storage) Sanitation Methods.

- Purge or Destruction technologies are the preferred methods for making data recovery infeasible for all of these media.

All references to "indefinite retention" should be considered equivalent to meeting federal or state statutory mandates if the business were to terminate or archiving is no longer feasible.

The retention schedule listed below is the 'best' practice standard. State retention policies vary widely and change frequently. We encourage you to query a reliable source to verify state-specific retention regulations. Please note that Medicare Advantage providers are required to retain all patient records for a minimum of ten (10) years, regardless of state law, unless state law is more stringent.

Patient-Related AHIMA's Recommended Retention Standards	**Retention Period –**Recommendation—Monitor State/Fed Statutes
Appointment Book/Electronic Schedule	Indefinite/10 years
Patient Log	Indefinite/10 years
Audits	Indefinite/10 years
Patient Clinical Charts ● Referral(s) ● Evaluation(s)/Re-evaluations/MD Letters ● Daily Notes ● Progress & Discharge Report(s) ● Pain & Functional Activities Forms ● Home Programs/Instructions ● Test/Surgical & Medication Reports ● Treatment/Instruction Flow Sheets ● Patient Intake Form ● Patient ID Information ● Authorizations & Notices ● Claims, Statements, RAN/MRN ● Correspondence & Acknowledgements	Indefinite/10 years after the most recent encounter– adults Indefinite/ age of majority plus statute of limitations
HIPAA Record Keeping ● Notice of Privacy Practices ● Patient Authorizations ● Patient Consents ● HIPAA Policies & Procedures	Indefinite/6 years from the date created
Cont. HIPAA Record Keeping	
Charge & Billing Records	Indefinite/1 year or until AR Summary
AR Summary with PHI	Indefinite/6 years
Clinical Forms with PHI	Indefinite/6 years
HIPAA Security Audits	Indefinite/6 years
HIPAA Breach Notices	Indefinite/6 years
HIPAA Incidents	Indefinite/6 years

Employee/Agent Related	Retention Period – Indefinite/Minimum Required
Employee/Agent Personnel Files	Indefinite/7 years
Employee/Agent Medical Files	Indefinite/Employment Duration + 3 yrs. Work Injury or Exposure 30+
Applications/Resumes of Non-Hired People	Indefinite/1 year
Employment Verification I-9 Form	Indefinite/Employment Duration + 3 yrs.

Operational Related	Retention Period – Indefinite/Minimum Required
Policy & Procedure Manuals	Indefinite//6
Inventory Listing	Indefinite/6 years
Equipment Maintenance/Inspection Manual	Indefinite/6 years
Payroll Book	Indefinite/6 years
Minutes of Staff Meetings/In-services/CPE	Indefinite/6 years
Operational Forms	N/A
Financial Statements	Indefinite
Cancelled Checks for Taxes, C.E., Contracts	Indefinite
Contracts For Leases, etc.	Indefinite
Copyrights	Indefinite
Correspondence on Legal & Tax Matters	Indefinite
General Ledger, Journals	Indefinite
Insurance Records	Indefinite/6 years
Property Appraisals	Indefinite/3 years
Tax Returns & Work Papers w/Support Records	Indefinite
Cancelled Checks (operational)	Indefinite/3 years
Expense Reports	Indefinite/3 years
AP/AR Ledger	Indefinite/6 years
Expired Contracts/Leases	Indefinite/3 years
Purchase Orders	Indefinite/2 years
Invoices/Sales Records	Indefinite/2 years
Employee Withholding Statement	Indefinite/3 years
Employee Benefit Plans	Indefinite/3 years
Bank Reconciliation	Indefinite/3 years
Petty Cash Vouchers	Indefinite/3 years
Expired Insurance Policies w/No Res. Value	Indefinite/3 years
General Correspondence	Indefinite/2 years
Requisitions	Indefinite/2 years

It is the intention of the owner or designee of Inspirit Therapy Associates to continue operations indefinitely. However, the owner or designee retains the right to interpret all references to “indefinite retention” as equivalent to meeting statutory mandates if the business were to terminate or archiving is no longer feasible. Ownership of records, with the exception of those related to non-assumed employees and compliance records, is automatically transferred to the new owner or their designee in the event of the sale of Inspirit Therapy Associates.

In the event of termination of operations, all records, including patient records, that meet the statutory retention limit will be either disposed of in a manner that does not breach confidentiality or maintained by the current owner or designee of Inspirit Therapy Associates. Patient, operational, and compliance records that do not meet the statutory limit will be maintained until the statutory limit is reached. All of the retained records will be securely stored

{{Policy_R001005_03}}

{{Policy_R001005_04}}

that meets protected healthcare information/e-phi storage criteria and is under a Business Associate Agreement.

Additionally, if the business is terminated, all active patients will be provided with a referral list of practices to choose from, and record transfer will be facilitated to ensure that no disruption of care or access to records occurs. While not required by law, as a courtesy to its patients, Inspirit Therapy Associates may choose to publish a notice regarding business cessation in the local paper, stating the disposition of the records and including an action deadline.

Workstation privacy and security are compliant with HIPAA regulations guiding covered entities. For the purposes of this policy, as defined by the Security Rule, a “workstation” includes all electronic computing devices, such as desktops, laptops, tablets, cellular phones, PDAs, portable USB drives, or any other device that performs similar functions, as well as all electronic media stored in its immediate environment.

This facility will consider any device that permits user access to electronic health information to be included in the definition and ‘use’ requirements for workstations. All workstations (hardware, software, and any E-PHI medium) are inventoried by item, location, serial number/model number, or version.

{{Policy_R001005_05}}

T{{Policy_R001005_06}}

Paper clinical records may not be removed from the premises for routine documentation purposes, and electronic documents may not be accessed on devices that the HIPAA Officer has not authorized. Paper records may be relocated for archiving and or emergency security purposes as approved by the owner or his/her designee and/or the Office Manager. A ‘by year’ alpha list will be maintained for all records relocated or stored off-site. Access to archived clinical records must be approved by the HIPAA Officer or the owner or designee and is permitted only for clinical management by authorized staff members, clinical record review for quality management or other compliance mandates, judicial compliance by subpoena, patient authorization per his/her designation and as permitted and/or required by HIPAA rules and regulations. Access to electronic clinical records is subject to the same restrictions and prerogatives as those noted for paper records.

Every effort to protect patient, patient-related, and operational records from physical damage or confidentiality breaches is guaranteed. The physical safeguard of PHI and E-PHI is addressed in PHI-EPHI & Proprietary Data: Confidentiality, Use, Disclosure & Access HIPAA Policy 1.007.

The Business Office staff designee, under the direction of the HIPAA Officer, is the individual responsible for obtaining authorized releases of PHI or E-PHI from Inspirit Therapy Associates's patients. The HIPAA Officer or the Business Office Manager would typically be the individual authorized to release PHI or E-PHI in response to subpoenas, protective orders, and affidavits.

1.007: PHI-EPHI & Proprietary Data: Confidentiality, Use, Disclosure & Access

Effective/Revision Date: {{Policy_DATE1007}}

Policy Classification(s): HIPAA

POLICY:

All information, whether written, spoken, or electronically transmitted, relating to a patient that is outside of the "need to know' for treatment, billing, healthcare operations purposes, or required or permitted by law must have the patient's or the patient's representative's valid HIPAA authorization. All uses and disclosures of PHI/E-PHI (Protected Health Information and/or Electronic Protected Health Information) will be carried out in total accordance with prevailing HIPAA, HITECH, Affordable Care Act (ACA), and state regulations that yield the most protective ordinance.

All facility operational information is considered proprietary. This information will also be used and disclosed by employees and/or agents according to facility policy as authorized by the owner or designee or as noted in a position description or by specific duty designation.

GENERAL PROCEDURES & PROCESSES TO ENSURE COMPLIANCE

Minimum Necessary Determination

1. Each position description and individual's role will be reviewed for PHI and E-PHI use, disclosure, and access opportunities and functions, and will be reassessed upon role or position description modification, operational or system changes that could impact his/her 'minimum necessary' status

    a. **Privacy "Minimum Necessary" Determination:**

        i. For this policy, all employees at Inspirit Therapy Associates, due to the size of the staff and the need for duty cross-training and job sharing, have been deemed as 'authorized to access' all paper PHI relating to treatment and payment information to ensure that efficient and effective duty execution may occur.

    b. **Security "Minimum Necessary" Determination:**

        For the purpose of this policy:

        i. All managerial, licensed clinical staff, and business office staff at Inspirit Therapy Associates have been deemed as 'authorized to access' all E-PHI to ensure that efficient and effective duty execution may occur;

ii. Access levels are controlled based on duties and responsibilities. Currently, only the owner or designee and the Compliance and HIPAA Officers have full access to read, write, and delete E-PHI;

iii. All other staff members or Business Associates (users) are limited to read-only and/or read/write access as stipulated on the Staff & Business Associates Rosters, per position description. However, licensed staff have the prerogative to delete entry errors prior to closing and signing an electronic document, as per the software's procedures;

iv. The System Administrator has read, write, and delete privileges when authorized by the owner or designee or the HIPAA Officer.

Patient Records & other Protected Healthcare Information (PHI)

For PHI management, see the Clinical Documentation, COM Policy 5.001, the Use, Disclosure, Authorization & Release of PHI, HIPAA Policy 1.001, and the Record, Electronic Media and Device Retention and Disposal Guidelines, HIPAA Policy 1.005.

Operational Information

Inspirit Therapy Associates's operational information ascertained by personnel is considered confidential and may only be used and/or disclosed with the permission of the owner or designee or his/her designee. Any operational materials acquired while at Inspirit Therapy Associates are considered proprietary and must be returned prior to or during the exit interview in the event of employment separation. The operational data referenced includes, but is not limited to:

1. All Protected Health Information, including but not limited to patient records, claims (in any medium), or other confidential material as classified by HIPAA.
2. Educational Information, Training Manuals, and Instruments.
3. Safety, Clinical, Financial & Operational Policies, Procedures & Forms.
4. Clients and Business Associates Lists.
5. Finances (both budgeted and actual).
6. Marketing Strategies.
7. Projects and Proposals (both in development and pending).
8. Employee Handbook—Policies, Procedures & Forms.
9. Compliance Reports and Resource or Investigational Materials.

Personnel Information

All personnel information is considered confidential and is managed in a manner that ensures its confidentiality. The owner or designee will securely maintain personnel files, and access to those files is restricted to personnel who require it on a 'need-to-know' basis.

Work history reference checks will be released in accordance with work separation procedures and to the extent allowed by state/federal law. Medical files are maintained separately for each employee, and access to them is restricted to the owner or his/her designee, the Compliance Officer, the HR Manager, regulatory agents, and others authorized by the employee. The staff call roster is to be shared with the company's staff only and will not be posted or be openly accessible. Any personnel's personal information, whether in paper or electronic form, must be destroyed by shredding or, according to Electronic Media & Device Retention &/or Disposal Guidelines, HIPAA Policy 1.005***.***

Compliance & Audit Reports and Documents

All compliance reports and documents are considered strictly confidential. Report details, parties named or reporting, and investigation proceedings are managed solely by the owner or designee or the Compliance and/or HIPAA Officer (s). Release of any of the above information is on an absolute "need to know" basis for fact discovery, investigation, and/or incident resolution. Active or closed compliance documents, including, but not limited to, reports, notes, audits, databases, logs, and disciplinary action, are to be managed by the owner or designee or the Compliance or HIPAA Officer as "secured materials" under lock and key and/or password access and in accordance with the Record, Electronic Media & Device Retention &/or Disposal Guidelines Policy, HIPAA Policy 1.005***.*** Strong consideration will be given to retaining an attorney for audit process consultation by Inspirit Therapy Associates.

Billing Information

All patient billing information is managed confidentially at all times. Access to patient billing files, A/R, and/or billing reports is restricted to employees and agents in compliance with prevailing regulations relating to the 'minimal necessary' provision.

Safeguard Provisions

Every measure to safeguard E-PHI data 'at rest' and data 'in transmission' and PHI uses and disclosure will be taken; these measures will include, but not be limited to, the information below.

Information Access & Management

1. Information access authorization will be determined for each employee, agent, and Business Associate based on his/her role, job description, and/or contractual agreement. Additionally, access needs will be reassessed in response to environmental or operational changes, including system or software changes or upgrades.

2. Inspirit Therapy Associates's computer system and all associated E-PHI require a unique identifier to access them. This safeguard is also a required procedure for accessing all personnel and proprietary data files.

3. Unique identifiers are required for each device (personal, network, and/or server) that could permit user access to E-PHI. Each person has their unique identifier, which includes their password and ID.

   Applicable passwords will be changed immediately in the event of employee separation, any suspected or known security risk, or breach. The IT Consultant/Administrator & HIPAA Officer maintains a master copy of all passwords and IDs to ensure access in the event of

an emergency and for audit purposes. Password selection will be based on NIST's Digital Identity Guidelines for creating strong passwords utilizing the following criteria:

a. Select Length Over Complexity:

    i. Twelve to sixteen (12-16) characters up to sixty-four (64) characters;

b. Avoid Common or Predictable Patterns:

    i. No guessable passwords like "password123", "qwerty," or repetitive sequences "aaaa";

c. Use Passphrases:

    i. Long and combined unrelated words, including all letters, spaces, and punctuation;

d. Do Not Force Arbitrary Complexity Rules:

    i. No required special character types (uppercase, numbers, symbols);

e. Check Against Breached Password Lists:

    i. Verify that passwords are not on the lists of commonly used or compromised passwords, or use a password checker;

f. Do not require Password Resets:

    i. Only require resets when breached or compromised;

g. Use Multi-Factor Authentication (MFA):

    i. Use MFA or a hardware token to enhance security;

h. Educate Users:

    i. Prohibit sharing passwords or writing them down in insecure locations;

    ii. Guided users in creating strong, memorable passwords or passphrases.

4. Inspirit Therapy Associates's software support company's access is software-specific and carried out via a Third-Party Remote Program. Their access is typically limited to correcting problems, performing updates, and conducting tutorial sessions; access authorization from the HIPAA Officer, the owner, or their designee is required, and the process is password-protected. Verification and authentication include password recognition. Access purposes are documented in the Business Associate's Agreement and its contractual agreement. The HIPAA Officer or designee will conduct access audits to ensure proper access authorization and activities.

5. Inspirit Therapy Associates's IT Consultant/Administrator has full access to the system but is required to obtain permission from the owner or the HIPAA Officer prior to accessing the system. All accesses will be logged by the HIPAA Officer or his/her designee, and a random audit will be conducted to ensure compliance with access requirements. The IT Consultant/ Administrator's password is changed every ninety days or sooner if indicated, unless otherwise stipulated in the IT Consultant/Administrator Agreement.

Medicare's remote software/system (Direct Data Entry) requires users to change passwords at regular intervals, often every thirty (30) or sixty (60) days.

6. A user (facility staff) must have an active ID and password to sign onto the computer. Access is predefined and limited in scope per the 'minimum necessary' provision of the prevailing regulations. User access is terminated on the day of the exit interview unless otherwise deemed appropriate by the owner or designee.

7. Monitor or device screens must use a timed screen saver to shield the viewing of E-PHI and proprietary data when inactive for 2-5 minutes, based on workstation location. An automatic log-off should occur after a minimum of (10) minutes of inactivity, regardless of workstation location; all data screens must be closed out at the end of each working day.

8. All Electronic Medical Record users will use role-based access controls determined by job functions. These individuals will save E-PHI to the EMR Portal. Temporary storage on another drive or any other electronic medium requires prior authorization from the owner or designee. It must comply with HIPAA security guidelines for "data at rest" and data "in transmission."

9. All hardcopy files and/or reports are stored/filed in an 'access restricted area' such as a locked or attended office when not being utilized. All charts, reports, billing information, and other PHI in paper form must be locked in the file room, a closed and secured office, or a desk at the end of each day. At no time will any patient PHI or E-PHI be left in an open access area, either in the clinic or off-site teleworkers' offices, without the authorized individual's oversight.

10. System Back-Ups include, but are not limited to, the operating systems, practice management data, clinical records, Claims Data, and Electronic Medical Records Software.

    {{Policy_R001007_02A}}

    {{Policy_R001007_03A}}.

    Security Software—Firewalls (internal and external), virus and anti-malware software, and access audit software are maintained and upgraded to prevent contamination and detect unauthorized access or disclosure. All users are oriented to the purpose of this software, as well as how to quarantine and/or report security incidents or problems.

11. Should the clinic use email to communicate with patients or access e-PHI, it must be certain that all correspondence is executed via the EMR secure portal or encrypted via the email software and that all documents are transferred off the email server and onto a secured file and/or hardcopy.

Electronically 'At Rest' and 'In Transit' Documents/Data

1. Electronic data will be safeguarded by employing credible virus and anti-malware detection and firewall software, complying with all recommended system and software updates, and ensuring routine virus and malware scanning as per the manufacturer's recommendations and OIG's guidance.

2. Electronic data "'at rest" will be safeguarded via encryption/firewall standards and other access safeguard procedures in accordance with the OIG's guidances.

3. Electronic data “in transmission,” including but not limited to clinical records, claims, and associated billing information, will meet at least the 256-bit encryption recommendations for safeguarding data and will comply with reimbursement coding and transaction standards and code sets per prevailing regulations.

4. Security systems with cross-checks will be maintained, monitored, and updated in accordance with prevailing regulations. Access monitors and audits will be conducted to ensure compliance with security standards.

5. Audits performed will or could include, but not be limited to:

    a. Workstation access (passwords, access attempts, access level compliance, etc.);

    b. Network/Server, EMR access;

    c. Application access;

    d. Internet & email destinations or sites;

    e. Back-up capabilities, reports, and access;

Telephonically Communicated PHI/E-PHI(Protected Health Information-Electronic Protected Health Information)

1. Any PH/E-PHI disclosed telephonically to any requesting party must first be determined as ‘in compliance with’ the patient’s authorization per Patient Rights and/or prevailing Treatment, Payment, or Healthcare Operations regulations and, additionally, must be identified explicitly with ‘minimal necessary’ privileges.

2. Careful verification of the ‘requesting’ party’s identification must be made prior to the release of PHI/E-PHI. Secondary verification may be necessary to ensure that the requesting party has the necessary authorization to access PHI/E-PHI. The methods for verification may be telephonic by requesting specific information about the patient (SS#, birth date, etc.); accessing a known and authorized agent of the entity, or by requesting fax or email on official letterhead; PHI/E-PHI released outside of T-P-O, and patient authorization must be logged.

3. Inquiries made to other covered entities or business associates regarding a patient’s PHI/E-PHI must be directed to a specific person and comply with the ‘minimal necessary’ guidelines for both parties.

US Mail & Express Delivery Services

1. All claims, reports, and associated PHI must be inserted into an appropriately sized and posted sealable envelope.

2. All addresses will be verified prior to mailing.

3. All envelopes will bear return addresses and “return to sender” requests if undeliverable.

4. All mail will be deposited directly into a certified US mail drop, given directly to a US mail carrier, or deposited with a reputable express mail carrier.

Faxed Documents/Data

All faxes must:

1. Include the sender's name, contact information, and fax number.
2. Include the recipient's name, contact information, and fax number.
3. Verify that the recipient's fax number is correct.
4. Include the date and time the fax was sent.
5. Indicate the total number of pages in the fax.
6. Include a statement that the information is protected under HIPAA if it includes PHI.
7. Include the following general-use confidential statement:

   “This message is confidential and intended only for the use of the individual or entity to whom it is addressed. Any unauthorized viewing, copying, or distribution of this information is strictly prohibited. If you are not the intended recipient, please notify the sender and arrange for the return or destruction of this fax.”

8. Include the following, or a similar confidential message, if PHI is included in the fax:

   “This fax contains confidential health information that is protected by the Health Insurance Portability and Accountability Act (HIPAA). It is intended only for the recipient(s) listed on this cover sheet and should not be viewed by anyone else. Unauthorized disclosure or distribution of this information is prohibited. If you are not the intended receiver, please notify the sender and arrange for the return or destruction of this fax”.

{{Policy_R001007_04A}}

{{Policy_R001007_05A}}

1.008: Video Surveillance (Disregard or Delete if not applicable)

Effective/Revision Date: {{Policy_DATEFINAL}}

Policy Classification(s): HIPAA

POLICY:

This facility's policy is to limit surveillance to video technology; audio surveillance is prohibited. Our video monitoring system has two primary goals: the first is to protect employees, patients, and visitors, and the second is to mitigate liability risks. We fully comply with all relevant federal and state laws, including the HIPAA Protected Health Information laws under the Privacy and Security Rules, as well as the *Electronic Communications Privacy Act (ECPA)*. Additionally, this facility will comply with state and local ordinances regarding camera surveillance of the public and employees. We post notices regarding the use of security cameras in the reception area, common areas, and parking area, as applicable. Postings will comply with federal, state, and local requirements. Security cameras are prohibited in areas where privacy is expected, including but not limited to enclosed treatment rooms, restrooms, break rooms, and changing areas.

PROCEDURE:

The following factors will be considered when determining the location of video equipment and its intended use. These are based on best practices and are conventionally accepted standards for placing surveillance equipment in a workplace.

1. Surveillance devices will only be located in public areas, i.e., devices will only be operational where there is no 'reasonable expectation of privacy' (e.g., not in bathrooms, locker rooms, dressing rooms, employee lounges, breakrooms, and other private areas).

2. Cameras will be situated so they do not have visual access to PHI. Take extra precautions to ensure camera placement is proximal to computer monitors displaying personal information, and never point at the screens.

3. Video footage viewing will be carried out in a secure area. It will be limited to authorized personnel as determined by the HIPAA or Compliance Officer.

4. The surveillance system will have end-to-end encryption and all other required security safeguards. The HIPAA Officer will audit the system for potential vulnerabilities, including, but not limited to, unauthorized access or the capturing of personal or protected health information.

HIPAA Considerations

Video surveillance can be a crucial part of the 'physical safeguards' component of the HIPAA Security Rule. Security footage is one way to document and audit who accessed PHI, especially when the platform incorporates Artificial Intelligence (AI) features such as facial recognition. If AI is used, it will be compatible with all federal, state, and local laws and requirements.

If our video surveillance records PHI (including but not limited to facial photographic images, license plate numbers, or other personally identifying health information), it will be HIPAA compliant. The recorded video footage will be protected in accordance with HIPAA and the Security Rule regulations. These regulations include, but are not limited to, the following:

1. Utilize permissions-based role management to tailor system access levels for various users. Control access to PHI by sharing and restricting access to different cameras on an individual or role-based basis; for example, permission might be limited to access the lobby camera but not the interior cameras.

2. Ensure the video security system has documented security practices and incorporates robust security safeguards, including end-to-end encryption, secure system access controls, and regular security audits to identify potential vulnerabilities.

3. Obtain and maintain current Business Associate Agreements with surveillance system vendors or HIPAA third-party auditors.

1.009: Security Risk Management: Risk Analysis, Risk Mitigation & Program Evaluation & Assessment

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

POLICY:

Inspirit Therapy Associates has established sound business risk management processes and has incorporated the HIPAA Security Risk Management requirement within this framework. For the purpose of this policy, security risk management is the process of identifying risk, assessing risk, taking steps to reduce risk to an acceptable level, evaluating the program's effectiveness, and ultimately making changes to maintain compliance.

This facility considers the security risk management responsibility of the security management team, which consists of:

1. Owner or designee
2. HIPAA Officer
3. IT Consultant/Administrator
4. Compliance Officer

Risk Management

Inspirit Therapy Associates is committed to complying with HIPAA's security regulations not just because it is required or because it makes good business sense but primarily because it is the right thing to do to protect both the patient and the organization.

While the Risk Management Team is responsible for planning, developing, implementing, monitoring, evaluating, and improving, as necessary, its security program, all personnel and business associates of Inspirit Therapy Associates are expected to be active participants in promoting and ensuring HIPAA Privacy and Security compliance daily.

Risk Identification & Analysis

To mitigate its risk related to HIPAA, Inspirit Therapy Associates initially conducted a security risk analysis using the most current National Institute of Standards and Technology (NIST) guidelines and the Office of Civil Rights/HHS-recommended tools. The analysis was documented on a variety of Risk Analysis Survey/Checklist tools (from reputable sources), which now serve as a baseline for subsequent analyses, which will be performed periodically as regulations, operations, and/or systems change, but no less than annually.

The analysis identified assets, system characteristics, threats and risks, existing controls, vulnerabilities (including types, ratings, and impacts), and current policies and procedures. The findings of the risk analysis provided a basis for strengthening the facility's security infrastructure and overall security operations.

Risk Mitigation

Because the elimination of all risks is usually impossible, the Risk Management Team will use the least-cost approach and implement the most appropriate controls to decrease risk to an

acceptable level with minimal adverse impact on the facility's resources and mission. Risks will be ranked as identified in the initial Risk Analysis and re-ranked as needed following subsequent Risk Analyses; implementation activities will be prioritized based on these rankings. Required resources, including but not limited to human resources, will be documented, as will target start and completion dates for control implementation. These activities will be documented and retained in accordance with the HIPAA Retention Policy 1.005.

Privacy & Security 'Working' Manual.

Controls implemented will be a combination of both technical and non-technical methods. Technical controls are safeguards that are incorporated into computer hardware and/or software (e.g., access controls, identification mechanisms, encryption methods, etc.). Non-technical controls are typically management and operational controls (e.g., policies, procedures, personnel, physical and environmental security processes, and audits). The first five controls are proactive, non-technical controls, and the sixth (audit) is a combination of reactive, technical, and non-technical controls. The types of audits employed at Inspirit Therapy Associates are noted in PHI-EPHI & Proprietary Data: Confidentiality, Use, Disclosure & Access, as outlined in HIPAA Policy 1.007 (2e).

Evaluation & Assessment

The evaluation and assessment responsibilities are assigned to the Security Risk Management Team.

While aspects of the program will be routinely reviewed for effectiveness, a comprehensive Risk Assessment will occur at least annually. Additionally, a Security Risk Assessment may be conducted more frequently based on changes to and/or an expansion of the system and its processing environment, as related to new technologies, new regulations, or guidelines.

Security Awareness Program

Per HIPAA, a security awareness and training program is a required administrative safeguard. Our program educates all personnel on security responsibilities and best practices, ensuring a comprehensive understanding of both basic requirements and individual security responsibilities. Four main areas of our program include, but are not limited to, the following:

1. Security Reminders—Regularly distribute security reminders on various topics, including, but not limited to, access controls, incident response, data protection, on-site visitor monitoring, malware protection, mobile device security, social media best practices, and other relevant information.

2. Protection from Malicious Software—Personnel should be trained to identify symptoms of malicious software (e.g., phishing, malware) and understand procedures for reporting and mitigating these issues.

3. Log-In Monitoring—Personnel should be trained to recognize log-in discrepancies and identify when their accounts may have been accessed without their knowledge or consent. Routine monitoring of login activity should be performed. Personnel should report any suspected discrepancies to the HIPAA Officer.

4. Password Management – Personnel should be trained in creating, managing, and changing secure passwords.

5. Encryption and Two-factor Authentication Education.

The focus of this program is to develop awareness so that all personnel realize the consequences of their actions/decisions, moving beyond training. For example, all personnel need to be aware that opening an unrecognized email may create a malware infection versus just training to report an incident if something happens.

This program is intended to be ongoing and may include presentations, web-based learning, screen-saver messages, break-room postings, and other activities. Documentation of the program and staff participation, when appropriate, should be filed in the Annual Compliance Manual.

Examples of Problems and Mitigation Interventions

Possible Risks For Accessed E-PHI	Sample Risk Management Strategies
Lost or stolen login/ password information resulting in potential unauthorized or improper access to or inappropriate viewing or modification of E-PHI.	Implement two-factor authentication to grant remote access to systems that contain e-protected health information (E-PHI). This process requires factors beyond general usernames and passwords to gain access to systems (e.g., requiring users to answer a security question such as “Favorite Pet’s Name”).
An employee accesses E-PHI when not authorized to do so while working off-site.	Develop and implement proper clearance procedures, and verify the training of workforce members before granting remote access. Establish remote access roles specific to applications and business requirements. Different remote users may require varying levels of access based on their job functions. Ensure that the issue of unauthorized access to E-PHI is appropriately addressed in the required sanction policy.

Home or other offsite workstations left unattended, risking improper access to E-PHI.	Establish appropriate procedures for session termination (time-out) on inactive portable or remote devices. Inspirit Therapy Associates should hire a vendor to deliver systems or applications with default settings that are appropriate for its needs.
System(s) contaminated by a virus introduced from an infected external device.	Install Facility_Name}} approved firewall software on all laptops that store or access E-PHI or connect to networks on which E-PHI is accessible. Install, use, and regularly update virus-protection software on all portable or remote devices that access E-PHI.
Lost or stolen laptop or other portable device that houses E-PHI or is accessible through the device.	Maintain an inventory log that includes all types of hardware and electronic media (that could be traceable), such as hard drives, magnetic tapes or disks, optical disks, digital memory cards, and security equipment. Implement processes for maintaining a record of the movements of any person(s) responsible for or permitted to use hardware and electronic media containing E-PHI. Require the use of a lockdown or other locking mechanisms for unattended laptops. A password protects all portable or remote devices that store E-PHI. All portable or remote devices that store E-PHI are required to employ encryption technologies of the appropriate strength.
Lost or stolen laptop or other portable device that houses E-PHI or is accessible through the device.	Develop processes to ensure appropriate security updates are deployed to portable devices such as smartphones and PDAs. Consider the use of biometrics, such as fingerprint readers, on portable devices.

Lost critical operational E-PHI on the remote device.	Develop processes to ensure backup of all E-PHI entered into remote systems. Deploy a policy to encrypt backup and archival media. Ensure the use of encryption technologies of the appropriate strength.
Loss or theft of E-PHI left on the device after inappropriate disposal by the facility.	Establish E-PHI deletion policies and procedures for media disposal. At a minimum, this involves complete deletion, via specialized deletion tools, of all disks and backup media prior to disposal. Physical destruction may be an appropriate option for systems nearing the end of their operational life cycle.
Data is left on an external device (accidentally or intentionally), such as in a library or a hotel business center.	Prohibit or prevent the downloading of E-PHI onto remote systems or devices without an operational justification. Ensure the workforce is appropriately trained on policies that require users to search for and delete any files intentionally or unintentionally saved to an external device. Minimize the use of browser-cached data in web-based applications that manage E-PHI, particularly those accessed remotely.
Contamination of systems by a virus introduced by a portable storage device.	Install virus-protection software on all portable or remote devices that store E-PHI.
Data intercepted or modified during transmission.	Prohibit transmission of E-PHI via open networks, such as the Internet. Prohibit the use of offsite devices or wireless access points (e.g., hotel workstations) for non-secure access to email.

	Use more secure connections for email via SSL and utilize message-level standards, such as S/MIME, SET, PEM, and PGP. Implement and mandate appropriately strong encryption solutions for the transmission of E-PHI (e.g., SSL, HTTPS, etc.).
Contamination of systems by a virus introduced from an external device used to transmit E-PHI.	Install virus-protection software on portable devices that can be used to transmit E-PHI.

1.011: Contingency & Disaster Recovery Planning

Effective/Revision Date: {{Policy_DATE1011}}

Policy Classification(s): HIPAA

POLICY:

Inspirit Therapy Associates acknowledges that contingency planning and disaster recovery planning are distinct plans with two very different levels of criticality. However, these two plans are being combined under a single policy for fluid personnel education and effective process management. Unique differences and alternative actions or priorities will be specifically noted.

Criticality Analysis

Highest Priority:	Clinical Documentation (Active Patient Data)
High Priority:	AR Summary Reports (All Available Records)
	Clinical Documentation (Inactive Patient Data)
	Billing & Reimbursement Information (Active Claims Data)
Moderate Priority:	Billing & Reimbursement Information (Inactive Patient Accounts)
Low Priority:	General Business Resources (Policies, Procedures & Business Operations/Correspondence, etc.)

Backup & Data Retention

Backup and data retention procedures are detailed in the Record, Electronic Media & Device Retention &/or Disposal Guidelines, HIPAA Policy 1.005, under Information Access & Management, and will be carried out as stipulated in that policy. If, however, an emergency circumvents a full system backup, then we will defer to the criticality analysis chart, which serves as a guideline for prioritizing data backups. Note: Active patient clinical records supersede all other scheduled data backups, whether it is anticipated as a short-term situation or an actual disaster.

This facility uses

{{Policy_R001011_01}}

{{Policy_R001011_02}}

An inventory list of all hardware, applications, and operating system programs is maintained. The system and software are on:

{{Policy_R001011_01}}

{{Policy_R001011_02}}.

Should hardware be destroyed, stolen, or compromised in any way, it will be replaced within five (5) working days, and installation will be scheduled upon its receipt and/or download.

Installation/Recovery/Restoration Priorities

Installation, restoration, and recovery order in the event of system or physical plant/hardware compromise

1. Obtain hardware, as applicable.

2. Install, recover, or restore all operating systems and applications for the Server, workstations, and laptops (s), as applicable. Installation priorities include, but are not limited to, the following:

    a. Operating systems;
    b. Cybersecurity systems (malware, antivirus, etc.);
    c. Network systems and connections;
    d. Practice software (patient records, billing, claims, etc.);
    e. Other associated software or applications.

NOTE: The term 'laptop' is a generic term for all portable devices approved for use in clinical documentation and/or billing activities**,** including tablets, iPads, Chromebooks, etc.

Manual Procedures—Hardware and/or Software

Inspirit Therapy Associates will revert to manual procedures for capturing data, accessing data, and updating patient clinical or account records in the event the system and/or application is unavailable for more than twenty-four (24) hours. If the operating system or an application operationally fails and cannot be restored within three (3) working days, the Business Office Manager or their designee will obtain a replacement disk from the applicable vendor, utilizing

overnight mail, or download the required software and proceed to install/restore/recover according to the vendor's recommendations. This condition is considered an ‘emergency’ but not a disaster. Routine clinical and billing forms will be accessed if manual procedures are implemented.

The owner or designee of Inspirit Therapy Associates, in collaboration with the HIPAA Officer, IT Consultant/Administrator, and Compliance Officer, considers a ‘disaster’ a period exceeding five (5) working days during which the computer hardware, software, and/or the physical plant are not accessible or usable under normal circumstances. Under these circumstances, the owner or designee will declare the condition a disaster and implement relocation and/or disaster management directives.

Relocation

If relocation is necessary but hardware and software are still usable, the appropriate individuals, including but not limited to employees, patients, payers, licensing/registration boards, and vendors, will be notified of the temporary operating addresses once determined or acquired. Hardware and software will be assessed for functionality, and installation and recovery or restoration of operating and application software will be performed in the ‘installation’ and ‘criticality’ order noted above.

Hardware and/or Software Compromise

When the physical plant is accessible and usable, the Installation/Recovery/ Restoration and Manual Procedures will be implemented as noted above.

Contingency or Disaster Chain of Command & Deployment of Personnel & Vendors

The owner will determine whether a security emergency or disaster condition exists. If the owner is inaccessible, the HIPAA Officer will determine, in collaboration with the IT Administrator/consultant and the Compliance Officer, whether to proceed.

If the physical plant is rendered unusable because of an actual or impending environmental or natural disaster, all available personnel, without compromising safety, will be deployed to assist in:

1. Making data entries and transmitting or printing reports and/or claims.

2. Verification of e-PHI backup and accessibility.

3. Securing and/or relocating all PHI.

4. Securing and/or relocating system hardware.

5. Securing and/or relocating clinical equipment.

6. Securing and/or relocating furniture, accessories & supplies.

If the physical plant is usable and accessible, but the facility suffers a system crash, networking obstacle or compromise, or application failure, the owner or designee will engage the following individuals/entities in this order:

{{Policy_R001011_03}}

The Contingency and Disaster Plans will be reviewed annually, or more frequently if systems, applications, policies, and/or responsible parties/vendors undergo changes.

Actual system and/or application failures or compromises will constitute a “Response Emergency and/or Disaster Drill.” In addition to the “Response Drills,” Inspirit Therapy Associates will conduct a “paper drill” on an annual or biannual basis to validate that procedures are understood and that access to vendors and resources is adequate to ensure effective and efficient recovery.

A constant state of readiness for an emergency or disaster is facilitated by:

1. Maintaining a (current) copy of the system’s technical configuration schematic, both onsite and offsite. The onsite copy will be maintained with the System Inventory List to facilitate a quick response to emergency and/or disaster situations.

2. Maintaining and updating, as necessary, the procedural or electronic operations manual for the restoration of:

    a. Hardware;

    b. Software;

    c. Data files;

    d. Network.

3. Maintaining current copies of software applications, operating systems, and other software-related resources for each of our critical systems, as noted in the Criticality and Installations sections of this policy.

4. The Business Office Manager, HIPAA Officer, or their designee will monitor the functionality of the backup systems in the cloud and external drives, as well as operating and application software, at least every six months, or more frequently if necessary.

1.013: System Maintenance & Control Logs

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

POLICY:

Inspirit Therapy Associates will not only make every effort to maintain a secure environment, but it will also take proactive steps to ensure optimal functioning of its server and/or network software applications and operating systems. The owner or his/her designee, who is ultimately responsible for security, has appointed the following individuals to manage the day-to-day maintenance and controls that ensure optimal functionality.

PROCEDURE:

The Business Office Manager or his/her designee is responsible for:

1. Staying apprised of product changes, new releases, and/or versions for Inspirit Therapy Associates hardware and software.

2. Evaluating the applicability and necessity of updating software applications with new versions.

3. Interfacing with the owner or designee, IT Consultant/Administrator, the computer equipment vendor, and the application software vendors for proper use, repair, replacement, and general maintenance of system assets and resources.

4. Maintaining and updating the system and associated Inventory Logs.

5. Maintaining a System Maintenance Log detailing routine maintenance, updates, and hardware/software additions, eliminations, modifications, and relocations.

The Consultant/Administrator is responsible for:

1. Providing a current schematic of the system's technical configuration.

2. Providing a restoration procedural or operational manual for critical operations and applications.

3. Maintaining appropriate security controls by performing a baseline security audit and associated corrective action.

4. Configuring backup systems in the cloud-based or via physical hardware and software.

5. Developing and maintaining procedures and/or systems for 'access controls' for personnel, vendors, and business associates.

6. Carrying out patch management.

7. Installing and maintaining effective firewalls, viruses, spyware, and other malware programs.

8. Facilitating virus or malware destruction and/or quarantining and/or correcting associated malfunctions, if not carried out by the Business Office Manager or the user.

9. Participate in the development, review, and modification of security policies and procedures as needed.

1.015: Security Incident Management

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

DEFINITION:

HIPAA security standards define a security incident as an attempted or successful access, use, disclosure, modification, or destruction of information on a system without appropriate

authorization. The incident need not involve “protected health information” to qualify as a security incident, as many security incidents occur because they compromise the system's security and attempt to bypass security controls.

Some examples of security incidents that would be germane and/or of potential risk to Inspirit Therapy Associates are:

1. Shared passwords.

2. Unlocked screens and/or extended log-off times.

3. Worm, virus, and/or malware infections.

4. Access and/or attempts to access applications or the internet without authorization.

5. Social browsing (employees/students without E-PHI access rights).

6. Unauthorized software downloads (screensavers, etc.).

7. Saving data to the local drive versus in the cloud.

8. Unprotected laptops are used in or in transit to remote sites.

POLICY:

Inspirit Therapy Associates will orient and provide ongoing education to its personnel and business associates, as appropriate, regarding privacy and security and, specifically for this policy, what constitutes security incidents, how they occur, what course of action is expected, and what sanctions could be anticipated for failure to act appropriately. Inspirit Therapy Associates will employ the three implementation specifications for the security incident standard:

1. Identification and response to the security incident—Employees, agents, and business associates will be expected to be vigilant regarding the need to recognize a security incident and/or attempt. They will be held responsible for taking appropriate action, whether it involves intercepting, terminating, or merely reporting it. If there is a suspected or known incident, the proper course of action is to notify and engage the HIPAA Officer.

2. Mitigation of harmful effects of the security incident—Employees should only carry out interventional procedures if they are sure they will halt or minimize the effects of the incident. An example would be if the virus software notified a user of a potentially harmful virus, he/she should immediately quarantine it and report it to the HIPAA Officer; however, if application behavior is questionable and a security attack could be underway, the user should merely cease using the application (do not terminate) and immediately inform the HIPAA Officer so corrective action can be assured.

3. Document security incidents—Employees should make definitive, dated notations of suspected or known security incidents and provide the documentation to the HIPAA Officer. The HIPAA Officer will log the incident and complete any necessary additional documentation. The Officer will also take and document the corrective action and its outcome.

These reports will be incorporated into the ongoing risk assessment to help improve security controls, improve personnel education, and mitigate future security incidents.

As part of Security Incident Management, Inspirit Therapy Associates will conduct access and security audits, as well as physical plant inspections, to enhance its efforts to maintain a secure environment. The audits will be focused on random and will include, but not be limited to:

1. Areas of known breaches;
2. Access level compliance (application and read, read/write & read/write/delete);
3. Access site and purpose (application and email/internet sites);
4. See PHI-EPHI & Proprietary Data: Confidentiality, Use, Disclosure & Access, HIPAA Policy 1.007 (2e) for additional details.

1.017: Remote Use of/Access to E-PHI

Effective/Revision Date: {{Policy_DATE1017}}

Policy Classification(s): HIPAA

The roles and authority of the IT Consultant/Administrator & the HIPAA Compliance Officer can be interchanged.

Introduction:

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access facility data from a mobile device connected to an unmanaged network outside of Inspirit Therapy Associates's direct control. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

1. Laptop/notebook/tablet computers.
2. Mobile/cellular phones.
3. Smartphones.
4. Personal Digital Assistant (PDA).
5. Home or personal computers accessing corporate resources.
6. Any mobile device capable of storing company data and connecting to an unmanaged network.

The policy applies to any hardware and related software that could be used to access company resources, even if the equipment is not sanctioned, owned, or supplied by the Inspirit Therapy Associates.

The overriding goal of this policy is to protect the integrity of the private and confidential patient and business data that resides within Inspirit Therapy Associates's technology infrastructure. This policy aims to prevent this data from being stored insecurely on a mobile device or transmitted over an insecure network, where unsanctioned resources can potentially access it. A breach of this type could result in loss of information, exposure of PHI, damage to critical applications, loss of revenue, and damage to the Inspirit Therapy Associates's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Inspirit Therapy Associates's direct control to backup, store, and otherwise access company data of any type must adhere to company-defined processes for doing so.

Applicability

This policy applies to all Inspirit Therapy Associates's employees, including full and part-time staff, independent contractors, and other agents who utilize either company-owned or personally-owned mobile devices to access, store, back up, relocate, or access any of this facility's or patient-specific data. Such access to this confidential data is a privilege, not a right. It forms the basis of the trust our company has built with its patients, referrers, and the community. Consequently, employment at Inspirit Therapy Associates does not automatically guarantee the initial or ongoing ability to use these devices to access corporate networks and information.

It addresses a range of threats to or related to the use of enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive protected health information is deliberately stolen and sold by an employee.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware, and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial, personal, and/or confidential data could expose the enterprise to the risk of non-compliance with various HIPAA regulations, identity theft, and other privacy laws.

The addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of the Inspirit Therapy Associates's IT

consultant/administrator. The non-sanctioned use of mobile devices to back up, store, or access any company-related data is strictly prohibited.

This policy complements any previously implemented policies that specifically address the data access, storage, movement, and connectivity of mobile devices within the enterprise network.

Responsibilities

The HIPAA Compliance Officer is responsible for ensuring the confidentiality, integrity, and availability of corporate data. The HIPAA Compliance Officer has delegated the execution and maintenance of Information Technology and Information Systems to the Inspirit Therapy Associates's IT consultant/administrator. Other staff are responsible for following the procedures and policies within Information Technology and Information Systems.

All of Inspirit Therapy Associates's employees are responsible for acting in accordance with company policies and procedures.

Affected Technology

Connectivity of all mobile devices will be centrally managed by Inspirit Therapy Associates's IT consultant/administrator and will utilize authentication and strong encryption measures. Although IT is not able to directly manage external devices, such as home PCs, which may require connectivity to the company's network, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the Inspirit Therapy Associates's infrastructure.

Policy and Appropriate Use

It is the responsibility of any Inspirit Therapy Associates employee who uses a mobile device to access corporate resources to ensure that all security protocols generally used in managing data on conventional storage infrastructure are also applied here. It is imperative that any mobile device used for company business be utilized appropriately, responsibly, and ethically. Failure to do so will result in the immediate suspension of that user's account. Based on this, the following rules must be observed:

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to the company and company-connected infrastructure. IT will engage in such action if it believes such equipment is being used in a manner that puts the Inspirit Therapy Associates's systems, data, users, and the patient's PHI at risk.

2. Before initial use on the company network or related infrastructure, all mobile devices must be registered with the IT department. The Inspirit Therapy Associates will maintain a list of approved mobile devices, as well as related software applications and utilities. It will be stored remotely on {{Policy_R001011_01}} {{Policy_R001011_02}}

   Devices that are not on this list may not be connected to the company's infrastructure. If a preferred device does not appear on this list, personnel may contact the HIPAA Compliance

Officer for assistance. Although IT currently allows only listed devices to be connected to the company's infrastructure, it reserves the right to update this list as needed in the future.

3. End users who wish to connect such devices to non-corporate network infrastructure to gain access to company data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT consultant/administrator. Company data is not to be accessed on any hardware that fails to meet Inspirit Therapy Associates's established IT security standards.

4. All mobile devices attempting to connect to the company network through an unmanaged network (i.e., the Internet) will be inspected using technology centrally managed by Inspirit Therapy Associates's IT consultant/administrator. Devices not previously approved by IT that are not in compliance with IT's security policies or represent any threat to the company network or data will not be allowed to connect. Laptop computers or personal PCs may only access the company network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required. Smart mobile devices such as smartphones, PDAs, and Ultra-Mobile Portable Computers (UMPCs) will access the company's network and data using Mobile VPN software installed on the device by IT.

Security

1. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. A strong password must protect all mobile devices, and all data stored on the device must be encrypted using strong encryption. See the Inspirit Therapy Associates's guidance for passwords. Employees agree to never disclose their passwords to anyone, particularly family members, when conducting business work from home.

2. All users of mobile devices must employ reasonable physical security measures to protect their devices. End users are expected to secure all such devices used for this activity, whether they are in use or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain sensitive or confidential enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Inspirit Therapy Associates's IT consultant/administrator. Anti-virus signature files on any additional client machines, such as a home PC on which this media will be accessed, must be up to date.

3. Passwords and other confidential data, as defined by Inspirit Therapy Associates's IT consultant/administrator, are not to be stored unencrypted on mobile devices.

4. Any mobile device that is being used to store the Inspirit Therapy Associates's data must adhere to the authentication requirements of the Inspirit Therapy Associates's IT consultant/administrator. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by the Inspirit Therapy Associates's IT consultant/administrator before any enterprise data-carrying device can be connected to it.

5. IT will centrally manage security policies, network, application, and data access using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said

security implementation will be considered an intrusion attempt and will be dealt with in accordance with Inspirit Therapy Associates's overarching security policy.

6. Employees, contractors, and temporary staff will follow all company-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. Refer to Electronic Media & Device Retention &/or Disposal Guidelines, HIPAA Policy 1.005, for detailed data wipe procedures for mobile devices.

7. In the event of a lost or stolen mobile device, it is the user's responsibility to report this to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

8. Location-based services and mobile check-in services, which utilize device GPS capabilities to share a user's real-time location with external parties, are prohibited within the workplace. This applies to both company-owned and personal mobile devices used within the company premises.

Help & Support

1. Inspirit Therapy Associates's IT consultant/administrator will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT consultant/administrator.

2. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Inspirit Therapy Associates's IT consultant/administrator. This includes, but is not limited to, any reconfiguration of the mobile device.

3. IT reserves the right to limit end users' ability to transfer data to and from specific resources on the company network through policy enforcement, and any other means it deems necessary.

Organizational Protocol

1. IT can and will establish audit trails, and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used to investigate possible breaches and/or misuse. The end user agrees to and accepts that his/her access and/or connection to Inspirit Therapy Associates's networks may be monitored to record dates, times, duration of access, and other relevant information in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that external parties may have compromised. In all cases, data protection remains Inspirit Therapy Associates's highest priority.

2. The end user agrees to immediately report to his/her manager and Inspirit Therapy Associates's IT consultant/administrator any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of protected health information, company resources, databases, networks, etc.

3. {{Policy_R001017_01A}}

{{Policy_R001017_02A}}

4. Every mobile device user will be entitled to a training session on this policy. While a mobile device user will not be granted access to the Inspirit Therapy Associates's resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

5. Any questions relating to this policy should be directed to the HIPAA Compliance Officer.

1.019: Business Associates & Business Associate Agreements

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

DEFINITIONS:

Covered Entity: According to HIPAA

1. Health plans
2. Health care clearinghouses
3. Most healthcare providers

BUSINESS ASSOCIATE

A Business Associate person/entity who is not part of the workforce and who, on behalf of a covered entity, performs or assists with:

Functions or activities involving the use or disclosure of individually identifiable health information, including but not limited to claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing of claims; legal consultation; actuarial and/or accounting services; data aggregation, management, and administration; accreditation services and/or financial services to or for such covered entity.

INTRODUCTION

HIPAA only applied to Covered Entities prior to the passage of HITECH (Health Information Technology for Economic and Clinical Health) via the American Recovery & Reinvestment Act of 2009 (ARRA). Most Covered Entities utilize entities not directly covered by HIPAA to carry out activities and functions that involve Protected Health Information. HIPAA requires that Covered Entities have a compliant Business Associate Agreement for each Business Associate to aid in the protection of PHI and E-PHI. Under HIPAA Privacy, a business associate who violated its business associate agreement was liable for breach of contract but was not directly liable for violating HIPAA.

With the passage of HITECH, the obligations of business associates were significantly changed. Section 13401(a) of HITECH -- Application of Security Provisions states explicitly that most of the HIPAA Security Rule, specifically 45 CFR § 164.308 (Administrative Safeguards), 164.310

(Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policy and Procedures and documentation requirements) shall apply to a Business Associate of a Covered Entity in same manner that such sections apply to the Covered Entity. Section 13404(a) further provides that the requirements of HITECH Subtitle D, the Privacy subsection of HITECH (Breach Notification and PHI/E-PHI Disclosure), which apply to Covered Entities, are also applicable to Business Associates.

Both HITECH sections require that the HITECH privacy and security requirements applicable to Business Associates must be incorporated into the Business Associate Agreements/Contracts. These new requirements make a Business Associate directly responsible for provisions previously applied only to the Covered Entity. At the same time, HITECH Section 13404(c) also specifies that the increased civil and criminal penalties also apply to Business Associates.

POLICY:

Inspirit Therapy Associates utilizes a 2014 HITECH-compliant Business Associate Agreement.

Should the business associate have special requests for agreement content, we will consider them, provided they do not increase our risk and/or liability.

The HIPAA Officer maintains a list of business associate agreement terms and dates, which are reviewed annually or more frequently as necessary. See the current ***Business Associate Agreement Form, HIPAA 141.***

1.021: Breach Notification Requirements

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

DEFINITION OF BREACH

A breach is generally an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information and poses a significant risk of financial, reputational, or other harm to the affected individual.

An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.

2. The unauthorized person who used the protected health information or to whom the disclosure was made.

3. Whether the protected health information was actually acquired or viewed.

4. The extent to which the risk to protected health information has been mitigated.

There are three exceptions to the definition of “breach.” They are:

1. The unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.

2. The inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

3. The covered entity or business associate has a good faith belief that the unauthorized individual to whom the impermissible disclosure was made would not have been able to retain the information.

In both numbers 1 and 2, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

POLICY:

It is the policy of Inspirit Therapy Associates to fully comply with the Breach Notification requirements set forth by HITECH in the event of a breach of unsecured protected health information by this facility. For the purposes of this policy, ‘unsecured’ means that the PHI/E-PHI was available to an unauthorized individual without being first rendered unusable, unreadable, or indecipherable through the use of encryption or destruction technologies and methodologies by either this facility/or one of its business associates.

PROCEDURE:

Conduct a Risk Assessment

The first step, if you discover or suspect a breach, is to conduct the required risk assessment. A comparison to the most recent risk assessment performed would be prudent to determine if any new vulnerabilities or changes could have contributed to the breach. The risk assessment is required even if the breach of PHI was secured through encryption; it must address the following four items to determine if the PHI was compromised:

1. The nature and extent of PHI involved.

2. To whom the PHI may have been disclosed.

3. Whether the PHI was actually acquired or viewed.

4. The extent to which the risk to the PHI has been mitigated.

A breach notification is required if the risk assessment fails to demonstrate that there is a low probability that the PHI has been compromised if the PHI was unsecured. It is essential to note that HHS encompasses not only unauthorized access to PHI by thieves and external hackers, but also impermissible uses by knowledgeable insiders.

Regardless of whether you determine that notice is required, you should document your risk assessment for all potential breaches. We also recommend that you reassess your practice's privacy and security practices after any breach to prevent the same lapse from recurring.

Determine if a Breach Notice Must be Sent to an Affected Individual

If notice is required, you must notify any patient affected by a breach without unreasonable delay, meaning within sixty (60) days of the discovery or the timeframe specified by the state for the response (refer to ***HIPAA 140 Exhibit A*** or consult state law for deadlines) of discovery. A breach is "discovered" on the first day that you know (or reasonably should have known) of the breach. You are also required to report the breach on the first day that any employee, officer, or other agent of your practice (other than the person who committed the breach) knows about the breach.

The notice must be in plain language that a patient can understand and should provide the following information:

1. Brief description of the breach, including dates.

2. Description of types of unsecured PHI involved.

3. Steps individuals should take to protect themselves against potential harm.

4. Brief description of steps you have taken to investigate the incident, mitigate harm, and protect against further breaches.

5. Your contact information.

If you do not have all of the above information when you first need to send the notice, you can provide a series of notices that fill in the information as you obtain it.

Determine the Method of Notification to Affected Individuals

You must provide written notice to the patient at the patient's last known address by first-class mail. Alternatively, you can contact your patient by email if they have indicated that this is the preferred manner of contact. It is advisable to discuss with patients the physical or email address where they would prefer to be contacted in the unlikely event that a breach notice needs to be sent.

Notify the Secretary of Health & Human Services (HHS)/Office of Civil Rights via Its Website

Contents of the Notification of a Breach for Individuals

The notification will include, to the extent possible:

1. A description of the breach.

2. A description of the types of information that were involved in the breach.

3. The steps that the affected individual(s) should take to protect themselves from potential harm.

4. A brief description of what the covered entity is doing to:

    a. Investigate the breach;

    b. Mitigate the harm;

    c. Prevent further breaches;

    d. Provide contact information at no cost to the individual.

Breach Notification Requirements

Inspirit Therapy Associates will make the following notifications in the following manner, as outlined below, based on the number of breaches listed.

Breaches of Less than Five Hundred (<500) Individuals, We Will:

1. Provide the affected individual with a notice in written form by first-class mail or send an email notice if the affected individual has agreed to receive such notices electronically. The notice will be provided without unreasonable delay, and in no case, later than sixty (60) days following the discovery of the breach or the timeframe specified by the state for the response (refer to ***HIPAA 140 Exhibit A*** or consult state law for deadlines). If there is insufficient or out-of-date contact information, our facility will do the following if the breach involves:

    a. For two (2) to nine (9) individuals with out-of-date or insufficient contact information, our facility will utilize an alternative form of the written notice, e.g., telephone, website posting, or other HHS-approved means;

    b. Ten (10) or more individuals with out-of-date or insufficient contact information our facility will provide the notice on the home page of our website or provide the notice in major print or broadcast media where the affected individuals most likely reside (this type of notification will include a toll-free number or collect call option for individuals to contact our facility to determine if their protected health information was involved in the breach.

2. Provide Health & Human Services, Secretary of State, with an electronic notice of the breaches within sixty (60) days of the end of the calendar year in which the breaches occurred. A separate form will be completed for every breach that occurred during the calendar year. The electronic form, Office of Management and Budget (OMB) No. 0990-0346, will be completed as posted on the Health & Human Services website. *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html*

Breaches of Five Hundred (500) or More Residents within Our State or Jurisdiction, We Will:

1. Provide a notice to prominent media outlets by press release serving our State or jurisdiction. It will be provided without unreasonable delay, and in no case later than sixty (60) days after the discovery of the breach. It will include the same information required for the individual notice.

2. Provide Health & Human Services, Secretary of State, with an electronic notice of the breaches within sixty (60) days of the end of the calendar year in which the breaches occurred. A separate form will be completed for every breach that occurred during the

calendar year. The electronic form OMB No. 0990-0346 will be completed as posted on the Health & Human Services website.
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Business Associate Caused Breaches

If a business associate causes a breach of unsecured protected health information, the business associate must notify Inspirit Therapy Associates following the discovery of the breach. The business associate must provide notice to our facility without unreasonable delay and no later than sixty (60) days from the discovery of the breach. To the extent possible, our business associate is expected to provide our facility with the identification of each individual affected by the breach, as well as any information required to be provided by our facility in our notification to the affected individuals.

Burden of Proof

We recognize that our facility and our business associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. We further acknowledge that we will comply with the Privacy Rule relating to breach notification. For example, we maintain current policies and procedures regarding breach notification and, at least annually, review their content, including, but not limited to, disciplinary measures for workforce members who do not comply with them.

1.024: Electronic Signature Authentication

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

Inspirit Therapy Associates has adopted this Electronic Signature Authentication Policy to comply with its duties under HIPAA and HITECH as well as to comply with its obligation to protect the confidentiality and integrity of electronic protected health information (EPHI) as prescribed by the Inspirit Therapy Associates's Code of Conduct, professional ethics and standards.

Policy Statement

This Electronic Signature Authentication Policy is based on the following:

1. The owner or designee of Inspirit Therapy Associates has approved the use of electronic signatures to authenticate the entries in patients' clinical records.

2. Electronic signatures are in accordance with federal and state law.

3. Verifiable misuse of the authentication process, such as sharing passwords and/or signature keys, will result in disciplinary measures being taken.

4. This policy applies to all members of the workforce who have been authorized to use an electronic signature for electronic health information.

Definitions:

1. **Attestation** is the process of verifying that something is accurate or true. In the context of electronic signatures, it refers to the act of applying an e-signature to content, thereby demonstrating authorship and legal responsibility for a particular unit of information.

2. **Authentication** is the security process of verifying a user's identity that authorizes the individual to access the system (e.g., the sign-on process). Authentication is necessary because it assigns responsibility to the user for entries he or she creates, modifies, or views.

3. **An electronic signature** is a generic, technology-neutral term for the various ways an electronic record can be signed (or attested). It can include a digitized image of a signature, a biometric identifier, a secret code or PIN, or a digital signature. According to the U.S Electronic Signatures in Global and National Commerce Act, an e-signature is an "electronic sound, symbol, or process attached to, or associated with, a contract or other record and adopted by a person with the intent to sign a record." The most frequently used types of signatures for EPHI are:

    a. A biometric signature can be generally classified as either a physiological recognition method (fingerprint, iris, retinal, voice, facial, and hand geometry recognition) or a behavioral recognition method (characteristics include the changes in the timing, pressure, and speed during the course of signing), i.e., the dynamics of a person's handwritten signature which is recorded as an algorithm that can be compared to future signatures;

    b. A digital signature encrypts data (represented by a series of numbers), identifies who did the encryption, and then validates and detects whether changes have been made. A digital signature is tightly bound to the document using a unique number or electronic "fingerprint. This cryptographic signature (a digital key) authenticates the user, provides nonrepudiation, and ensures message integrity. The signature applied is considered the authentication of the specific entry, whether that electronic signature image is reviewed on a desktop or mobile device screen directly within the computerized clinical record system, or whether the signature image has been printed on a paper version of the clinical record;

    c. A digitized signature is an electronic representation (applied image) of a handwritten signature. This image is usually created by scanning a wet signature using digital photography. The signature may be captured in real-time (at the time the user applies the signature), or a previously saved image may be applied.

4. **Non-repudiation** "assures the origin or delivery of data" so that the sender cannot deny sending a message, and the receiver cannot deny receiving it.

5. **A Paper Signature (Wet) is a handwritten signature on paper.** This type of signature illustrates consent and identifies the signer. The ink permanently binds the signature to the paper, making it virtually impossible to remove.

Policy

All persons authorized to authenticate patient records (clinical and/or billing) attest that they will comply with this policy. Inspirit Therapy Associates permits practitioners and specific other designated individuals to authenticate entries by executing their signature. Inspirit Therapy Associates utilizes the following types/methods:

1. Electronic Documentation:

   {{Policy_R001024_01A}}

   {{Policy_R001024_01B}}

   {{Policy_R001024_01C}}

2. Practice Management (billing):

   {{Policy_R001024_01A}

   {{Policy_R001024_01B}}

   {{Policy_R001024_01C}}

3. Paper: Wet Signature

Clinicians and/or other authorized individuals applying an electronic signature must attest to having reviewed the contents of the entry and also that they have determined that the entry contains what they intended. Only unsigned documents can be altered once the individual has authenticated the entry, and those changes require justification. Inspirit Therapy Associates's system generates a change log that documents who made a change, the date of the change, and the reason for the alteration. The change log is audited according to the HIPAA calendar or more frequently, as necessary.

Procedure

Electronic Access Provisions

1. To gain entry into Inspirit Therapy Associates software on a computer, the individual must authenticate himself or herself on two levels:

   a. Initially, when turning on the computer, a unique login and password specific to the individual must be entered to gain access to the operating system on the computer;

   b. Subsequently, to access Inspirit Therapy Associates proprietary software, a second unique login and password specific to the individual must be utilized.

2. The computer will reject a user and deny entry into the Inspirit Therapy Associates system after five attempts at entering the unique login and password information incorrectly. An IT Consultant/Administrator level intervention is required for the individual to gain subsequent access to the system. System administration-level access is granted only to the IT Consultant/Administrator and specific designees who have been educated and have demonstrated competency in system and/or software utilization.

Safeguards

1. Passwords must meet the requirements noted in PHI-EPHI & Proprietary Data: Confidentiality, Use, Disclosure & Access, HIPAA Policy 1.007, and must be unique to each individual and may not be shared for any reason except in emergencies established by the Owner and/or HIPAA officer. Login information must be treated as strictly confidential.

2. The following rules apply to clinicians and other designees to mitigate unauthorized access to the system and forgery of electronic signatures:

    a. Each individual typically uses one specific computer with a unique number assigned to that individual;

    b. Clinicians and designees may, under authorized situations, use another individual's computer if they use their login and passwords to access E-PHI to which they have authorized access. The system will deny access if they attempt to access unauthorized information;

    c. The IT Consultant/Administrator is responsible for assigning computers, logins, passwords, and computer numbers. Only explicitly designated staff may assist in that maintenance as approved by the HIPAA officer;

    d. Entries on the computer that the clinician has electronically signed are locked. The clinician or other staff members cannot alter them;

    e. Clinical record entries that are locked can be unlocked only by the IT Consultant/Administrator or management-level staff, and only in specific circumstances, i.e., for entries unrelated to the clinical record content. Such unlockings of the clinical record are recorded in the audit log. Only the clinician who signed the chart can unsign it, and this is only possible with the authorization of the HIPAA officer;

    f. The system maintains an audit trail providing details of the names of individuals accessing clinical records and/or attempts to unlock a clinical or billing document.

3. A cloud-based vendor maintains the server for Inspirit Therapy Associates, and backups are continuous; the vendor protects the system with current and effective virus and anti-malware software, as well as firewall encryption.

4. Inspirit Therapy Associates educates its staff in the proper use of the electronic signature, mandating verifiable HIPAA privacy and security education followed by an attestation stating that, "I am responsible and accountable for the use of my e-signature I will be the only one who has access to use my specific signature code."

5. Inspirit Therapy Associates orients its staff to its progressive disciplinary measures as noted in HIPAA Performance Feedback, HIPAA Policy 1.0027, and HIPAA Positive Corrective Action & Sanctions HIPAA Policy 1.0029. This orientation includes the disciplinary consequences for failure to adhere to and/or report known or suspected violations of HIPAA privacy and security requirements and processes

6. Any attempt by any staff member or onsite partner to alter an access or signature protocol will result in disciplinary action.

7. The IT Consultant/Administrator will periodically and/or routinely monitor and report any new or heightened risks related to access and/or electronic signatures.

Enforcement

All officers and employees at Inspirit Therapy Associates are required to adhere to this policy, and all supervisors are responsible for ensuring its enforcement. Inspirit Therapy Associates works diligently to mitigate the potential for a HIPAA violation; if, however, an infraction should occur, it will be immediately investigated and corrective action will be implemented as necessary. Corrective action could include physical, administrative, and/or technical modifications to mitigate the risks, implementation of stricter educational requirements, and/or a series of disciplinary measures up to and including termination of employment as well as criminal or professional sanctioning in accordance with Inspirit Therapy Associates disciplinary policy and HIPAA regulations.

1.025: Identity Theft Detection, Prevention & Mitigation Program (Red Flag Rule)

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

Inspirit Therapy Associates will comply with the Red Flag Regulations established by the Federal Trade Commission and any applicable state regulations governing identity theft. The actions required to ensure compliance are:

1. Designate a Red Flag Security Official.
2. Perform a Risk Assessment of internal and external risks.
3. Develop the Red Flag Regulation Policy & Procedure.
4. Educate its employees and agents.
5. Review and/or modify the plan based on ongoing monitoring results.
6. Create a mitigation plan.

Procedure:

1. The owner or their designee has appointed the Business Office Manager as the Red Flag Security Official. He/she is responsible for:
    a. Managing the day-to-day program in coordination with the Compliance Officer;
    b. Organizing the Risk Assessment Team, which includes business office personnel, the Compliance Officer, the HIPAA Officer, and her/himself;
    c. Reporting any findings related to the program and/or action taken or needed to the owner or designee and the Compliance Officer.
2. Steps 2 & 4 are documented in the Annual Compliance Tracking Manual.
3. Step 3 is the development and ongoing monitoring of this policy.

4. Step 5 requires the Red Flag Security Officer and the Compliance Officer to review the status of identity theft prevention on a regular basis. Any security breaches or attempted breaches must be documented and addressed immediately. The Compliance Officer will report to the owner or their designee, at least annually, on the effectiveness of the program.

5. Mitigation activities will have the ‘priority’ status and will include:

    a. Notification (immediate) of the event (breach or attempted breach) to the Security Official;

    b. Identification of the event, the person(s) involved, and any intervention;

    c. Documentation of the event on the External Incident Report Form by the discovering party;

    d. Assessment of the event by the HIPAA/Compliance Officers(s) and the owner or designee;

    e. Implementation of corrective action, as necessary;

    f. Communication with state and/or federal authorities.

1.027: HIPAA Performance Feedback

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

HIPAA regulations require an annual performance review related to HIPAA compliance

POLICY:

It is the policy of Inspirit Therapy Associates to give timely, objective feedback to all individuals working for or on its behalf. Formal performance review sessions are conducted at, but not limited to, the ninety (90) day introductory period and no less than annually thereafter. All employees are expected to participate in the formal feedback sessions by completing and submitting a self-assessment and by offering comments and/or additional information to the reviewer. Informal feedback sessions should, when appropriate, augment the required formal reviews.

The outcome of the performance feedback session should:

1. Provide both the employee and the reviewer with a quantifiable assessment of performance.

2. Assure the employee that a uniform instrument is used for all reviews examining the same traits, characteristics, and functions for similar positions.

3. Provide the reviewer with a system that correlates quantifiable performance measures with job classification, position status, and compensation adjustments.

PROCEDURE:

{{Policy_R001027_02}} This facility utilizes a standardized performance tool for job-specific performance, but also addresses HIPAA compliance conduct, as required by federal law.

{{Policy_R001027_03}} This facility utilizes a customized performance tool for all employees. It includes job-specific performance as well as HIPAA compliance conduct as required by federal law.

On or near the review date, the two individuals meet and review both written performance reviews. Comments, recommendations, and assessment similarities and variances are documented, as are objectives, goals, and action plans.

1. Complete the performance feedback session utilizing both the employee's and the employer's documented scoring and comments.

2. Dated signatures should be entered on the reviewer's Performance Review. Both original documents, if applicable, should be filed in the employee's personnel file, with the employee receiving a duplicate copy of each document.

1.029: HIPAA Positive Corrective Action & Sanctions

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

This policy is risk management-based; it is not required by law. If you include it, you must be consistent in application and never terminate "at will" unless per this policy's procedure.

POLICY:

It is the policy of Inspirit Therapy Associates to relate and enforce its policies, procedures, standards of performance and conduct, and all regulatory mandates governing Inspirit Therapy Associates. Common sense, good judgment, and professionalism are the best guides for proper workplace conduct by employees and agents. In cases where these obligations and responsibilities are breached, Inspirit Therapy Associates may take positive corrective action up to and including discharge.

When the Positive Corrective Action System is engaged, the employee/agent is entitled to impartial and swift intervention. Additionally, he/she is entitled to guidance via a written corrective action plan. He/she may exercise his/her right to the Employee/Agent Grievance Resolution System if he/she feels that the action taken is disproportionate to the offense or not optimally executed.

PROCEDURE:

Any management-level employee may activate the Positive Corrective Action System; however, consultation with the owner or their designee is recommended prior to action at Step II and is required at Steps III and IV, unless immediate action is essential.

{{Policy_R001029_01}}

All employees/agents involved in the Positive Corrective Action System:

1. Will be afforded the opportunity to provide a written explanation of his/her conduct.

2. Will be subject to performance/conduct monitoring for correction or improvement as recommended in the corrective action plan.

3. Could be subject to work suspension while the allegation is being researched (this would be in extreme situations where immediate action is warranted; suspension would be with pay unless there is evidence of gross negligence or misconduct)

4. A written report will be provided, detailing the infraction and outlining a corrective action plan, if applicable, at Step I, II, or III.

5. Will be given a written report noting the status of improvement within

Feb 16 2026

Below is a list of HIPAA-related infractions and corresponding corrective actions, organized by frequency of occurrence. This list is not exhaustive and is intended solely as an example. The disciplinary action taken may be mitigated or accelerated based on the level of harm, including, but not limited to, the volume, financial impact, cooperation with the investigation, and self-reporting.

Sample HIPAA Infractions & Sanctions	**Occurrences**		
	1st	**2nd**	**3rd**
Failure to comply with established Privacy & Security policies, procedures, and guidelines	VC	WW/P	T
Overt or covert mismanagement of a patient’s PHI	T		
Falsification of or mismanagement of personnel or clinical records, PHI/E-PHI, or other compliance plan violations	P/T		
Unauthorized or illicit use of Inspirit Therapy Associates property on paid time, including, but not limited to, personal internet and e-mail use	VC	WW/P	T
Retaliation against a HIPAA violation by a realtor	P/T		
Malicious HIPAA violations via use and/or disclosure with the intent to harm or commit an illegal act	T		

1.030: HIPAA Complaint Process

Effective/Revision Date: {{Policy_DATE6029}}

Policy Classification(s): HIPAA

It is the policy of Inspirit Therapy Associates to afford any patient, visitor, or employee/ agent the opportunity to raise a concern or voice a complaint related to HIPAA regulations. Consistency in managing this process is of foremost importance to this facility, and the HIPAA Office will be fully engaged in any complaints raised or voiced.

1. The HIPAA Officer is the primary point of contact for any HIPAA/HITECH complaints. These complaints may include, but are not limited to, breaches or compromises of Protected Health Information (in any medium, including paper and electronic), any HIPAA-required Patient Rights, or any other related HIPAA/HITECH requirements.

2. Patients, their representative, or staff member may file a HIPAA/HITECH-related complaint by submitting it in one of the following ways:

    a. In-person (preferred method).

    b. By mail either on Inspirit Therapy Associates's Complaint Form or by letter. Correspondence should be addressed to:

    Inspirit Therapy Associates
    Attention HIPAA Officer: {{Name_of_Owner_or_Designated_HIPAA_Officer}}
    3852 Creamery Rd
    De Pere, WI 54115

    i. By *TELEPHONE*: #(920) 338-9670

    ii. By *FACSIMILE* #: {{Fax-Number}}

    iii. By email: feelbetter@inspiritpt.com Confidential to HIPAA Officer

    Documented confirmation that the patient understands the security requirements for exchanging patient information over the Internet and his/her liability for use and disclosure when communicating via email should be obtained.

3. The complaint should include as much detail as possible, but minimally:

    a. The date of the alleged infraction;

    b. The specific infraction and privacy concern;

    c. The name of the individual engaged in the infraction, if known or applicable;

    d. A contact address, phone number, e-mail address, or fax number for responding to the complaint if not resolved at the time of the complaint issuance.

4. The HIPAA Officer will meet or respond to the complainant personally within two (2) working days or sooner of the complaint submission. If the HIPAA Officer contacts the complainant

by phone, every measure is taken to ensure the confidentiality of the complainant's identity prior to discussing the complaint. Additionally, any correspondence, facsimile, or electronically transmitted communication will be double-checked and directed only to the number provided by the complainant.

5. The HIPAA Officer will record the complaint and attempt to verify its validity.

6. If the complaint appears to be a misunderstanding of HIPAA requirements or Inspirit Therapy Associates's policies, the HIPAA Officer should attempt to explain the requirements. If the discussion results in a retraction of the complaint, the HIPAA Officer should document the complaint form to reflect "no further action required based on clarification." However, the HIPAA Officer should facilitate the complaint process if the complainant wants to proceed with the complaint. At no time should a complainant feel pressured or coerced to drop a complaint, even if a misunderstanding is evident.

7. Once the complaint is validated, if not dismissed, the HIPAA Officer will log the complaint and file the HIPAA Complaint Form in the Complaint File.

8. If the complaint requires investigation time, the complainant will be advised and given a follow-up date.

9. The HIPAA Officer will investigate by reviewing the alleged infraction circumstances with the relevant staff and by examining any relevant audit, monitoring logs, and/or forms associated with the complaint.

10. The HIPAA Officer will complete the investigation portion of the HIPAA Complaint Form and note whether the investigation findings yielded a valid or invalid complaint. The results should be handled as follows:

    a. Valid Complaint—The HIPAA Officer, in conjunction with the owner, will implement the Corrective Action Policy to the fullest extent if the complaint involves personnel. The complainant will be notified, via a letter, of the investigation's results and the course of action taken. The ***HIPAA Complaint Form***, along with the letter, will be filed in the Complaint File with a cross-reference placed in the complainant's chart (clinical or personnel). Legal counsel and/or compliance consultant will review all correspondence relating to complaints for tone, rationale, and applicability prior to distribution.

    b. Invalid Complaint—The HIPAA Officer, in conjunction with the owner or designee, will draft a letter to the complainant stating the reasons the complaint was found to be invalid. The ***HIPAA Complaint Form***, along with the letter, will be filed in the Complaint File with a cross-reference placed in the complainant's chart (clinical or personnel). Legal counsel and/or the compliance consultant will review all correspondence relating to complaints for tone, rationale, and applicability prior to distribution.

    c. Undetermined Complaint—The HIPAA Officer will engage either and/or both legal counsel and the compliance consultant to give professional opinions on the complaint status. Once the determination is made, the complaint will be handled as noted in (a) or (b) above.

11. Nothing in the complaint procedures should limit the complainant's ability to contact the Office of Civil Rights for intervention.

1.031: Court-Ordered Subpoena & Legal Counsel Request for Records

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

POLICY:

It is the policy of Inspirit Therapy Associates to comply with all applicable state and federal requirements regarding access to and/or the release of protected Health information, regardless of whether it is in paper or electronic form. This facility will follow the procedures outlined below as they relate to subpoenaed records.

Court-Ordered Subpoenas:

It is not necessary for Inspirit Therapy Associates to obtain a HIPAA-compliant authorization form from a patient for court-ordered subpoenas in accordance with HIPAA Privacy Rule 45 CFR § 164.512(e), which states that a Covered Entity may disclose PHI without patient authorization in response to a court order for judicial or administrative proceedings. The order must be a valid legal directive issued by a court with appropriate authority. Those authorized to sign the legal directive are:

1. Judge: A court order signed by a judge is universally recognized as valid under HIPAA for disclosing PHI without patient authorization.
2. Court Magistrate: In many jurisdictions, a magistrate (or magistrate judge) has the authority to issue court orders, including those related to the release of records, and such orders are also valid under HIPAA. Magistrates are judicial officers who can issue orders in certain proceedings, depending on the court's structure and jurisdiction.
3. Court Clerk or Other Officials: In some cases, a court clerk or other court official may issue orders under specific circumstances (e.g., administrative orders or discovery orders), but these must still be issued under the authority of the court. A clerk-issued document without judicial oversight (e.g., a judge or magistrate's approval) may not qualify as a "court order" under HIPAA unless it meets the regulatory requirements.
4. The authority to issue a court order may vary by jurisdiction (e.g., federal vs. state courts, or specific state laws). Some jurisdictions allow magistrates or other judicial officers to issue orders for records, while others may require a judge's signature. The Covered Entity must verify that the order is valid and issued by an authorized court official.

Attorney-Signed Subpoenas:

An attorney-signed subpoena (without judicial approval) does not qualify as a court order under HIPAA. For a subpoena to permit disclosure without patient authorization, it must either be accompanied by a court order (signed by a judge or magistrate) or meet the "satisfactory assurances" requirements (e.g., proof of patient notification or a protective order, per 45 CFR § 164.512(e)).

Satisfactory Assurances: For a subpoena not accompanied by a court order, the Covered Entity must receive the following from the requesting attorney:

1. The attorney must provide "satisfactory assurances" that reasonable efforts have been made to notify the patient; that is, the attorney must demonstrate that the individual whose PHI is requested has been notified of the request. Notification can be done by providing:
   a. A written statement and supporting documentation showing that the individual was notified (e.g., via written notice sent to the individual's last known address) and allowed to object to the disclosure;
   b. The notice must include sufficient information about the legal proceeding to allow the individual to raise objections in court.
2. Secure a Qualified Protective Order: The attorney must show that they have sought a qualified protective order that:
   a. Prohibits the use or disclosure of PHI for purposes other than the litigation or proceeding;
   b. Requires the return or destruction of the PHI (including copies) at the end of the litigation or proceeding.
3. Documentation: The attorney must provide a written statement and accompanying documentation (e.g., copies of the notice or proposed protective order) to demonstrate compliance with these requirements.

Disclosures for Law Enforcement Purposes

If the attorney is acting on behalf of a law enforcement agency or in a law enforcement context (e.g., representing a government entity), they may request PHI without authorization under specific conditions. Satisfactory assurances in this context depend on the type of law enforcement request:

1. <u>Administrative request (e.g., Subpoena, Summons, or Investigative Demand)</u>

   a. The attorney must provide a written administrative request, such as a subpoena, summons, or other lawful process issued by a law enforcement authority.
   b. The request must include a statement that:

      i. The PHI sought is relevant and material to a legitimate law enforcement inquiry.

      ii. The request is specific and limited in scope to the purpose of the inquiry.

      iii. De-identified information could not reasonably be used instead of PHI.

2. Other Law Enforcement Contexts

   For specific law enforcement purposes (e.g., identifying a suspect or reporting certain types of injuries), the covered entity may require assurances that the request is legitimate and authorized by law. The identification process might involve verifying the attorney's credentials or the authority of the requesting agency.

3. No Authorization Required: The above provisions apply only when the attorney is not acting on behalf of the patient (e.g., when a signed authorization is not present). If the attorney has patient authorization, these assurances are not needed.

4. Exceptions and Notes

    a. No Disclosure may be made if an objection has been raised: If the individual objects to the disclosure in a judicial proceeding (after notification), the covered entity may not disclose PHI unless a court resolves the objection or a qualified protective order is in place.
    b. Minimum Necessary Standard: Even with satisfactory assurances, the covered entity must limit disclosures to the minimum necessary PHI to achieve the purpose of the request.
    c. Business Associate: If the attorney is acting as a business associate of the covered entity (e.g., providing legal services), a business associate agreement (BAA) may be required instead, ensuring the attorney safeguards PHI (45 CFR § 164.504(e).

1.033: Regulatory Inspections & Surveys Relating to HIPAA

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

POLICY:

The Inspirit Therapy Associates acknowledges that inspections and surveys are integral to the business process in the healthcare sector. Some of these are scheduled events, and others are unannounced visits. Regardless of the situation, Inspirit Therapy Associates will make every effort to be prepared at all times and to be cordially receptive to any surveyor, inspector, or federal or state agent presenting himself/herself.

PROCEDURE:

Guidelines for Preparation and Reception of the Reviewer and Response

Inspirit Therapy Associates's Employee Responsibilities:

1. Comply with all policies, procedures, standards of practice, and other regulatory mandates as reflected and/or referenced in Inspirit Therapy Associates's policy and operations manuals.

2. Request valid identification and authorization of any/all reviewers and verify the provided credentials.

3. Contact the owner or designee and alert him/her immediately to the surveyor's presence or contact; subsequently, alert the HIPAA Officer to the same. Advise the surveyor that the HIPAA Officer is the appropriate individual to respond to a HIPAA matter and/or surveys. If the HIPAA Officer, owner, or designee is unavailable, request a reschedule of the survey. If the request is denied, contact the next most senior manager so they can meet with and accompany the reviewer(s). Continue efforts to contact the HIPAA Officer and the owner or designee during or following the survey.

Survey Managing an Individual's Responsibilities:

Unannounced Site Audits

1. Request an opening discussion, in private, for the opportunity to discuss the purpose and scope of the review

Scheduled or Unannounced Site Audits

1. Advise the surveyor of the clinic's HIPAA policies regarding:
    a. "Minimal Necessary" use and disclosure;
    b. Establish those parameters specific to patient physical privacy and record access;
    c. Obtain a copy of the surveyor's Business Associate agreement with the payer if he/she is contracted by a payer to perform audits.
2. Review allowable and restricted activities specific to this surveyor.
3. Inquire whether the surveyor will be photographing, video/audio taping discussions, and/or specific situations or items.
4. Establish the surveyor's timeframe to be in the clinic, as well as the subject matter of the audit:
    a. HIPAA compliance
    b. HIPAA Breaches
    c. Other incidents or issues
5. Document each step of the review and all questions asked, videotape or audiotape the review process, and duplicate the photographed and videotaped items.
6. Designate a document controller (preferably a Management Team member to track all the documents reviewed, requested, and/or copied.
7. Offer to correct, on the spot, any violations that could be immediately handled; confirm that the surveyor notes any corrections agreed to and subsequently made.
8. Request a closing conference, videotape/audiotape the proceedings, or minimally document each comment carefully.
9. Determine if a follow-up visit will occur, if and when a report will be received, and what timeline will be required for a response and/or corrective action.

Post-site Visit Audit

1. Organize the documents, notes, pictures, etc., that were made or taken by Inspirit Therapy Associates's designee and review them thoroughly.
2. Assess the event, including but not limited to any known aberrant findings presented by the surveyor or personally discovered, and perform a risk assessment based on those findings.

3. Prepare a verbal summary of the event for Inspirit Therapy Associates's workforce based on general information or assumptions that would be applicable to the audience.

4. Conduct a "key managers' meeting" to discuss the survey, its perceived or known outcome, and any directives communicated by the surveyor.

5. Develop a plan of action as needed.

6. Engage a consultant and/or legal counsel to begin a defense and/or appeal if findings or citations are unfounded

1.035: Consent for the Use and Disclosure of Images, Videos, Voice and/or Written Testimonials

Effective/Revision Date: Feb 16 2026

Policy Classification(s): HIPAA

POLICY:

It is the policy of Inspirit Therapy Associates to comply with HIPAA's Use and Disclosure regulations globally, particularly in this matter, which includes obtaining HIPAA authorization releases and consents for the use and disclosure of images, videos, voice recordings, and written testimonials. Inspirit Therapy Associates respects each patient's right to confidentiality and adheres strictly to that right.

Testimonials:

On occasion, patients provide testimonials about our services and/or personnel, and, if permitted by the author of the testimonial, Facility_Name}} may wish to post the comments in the clinic and/or on our website. We will always request that the patient sign the Inspirit Therapy Associates's ***Authorization for Release of PHI Form, HIPAA 143*** as well as the ***Consent to Use & Disclosure of Images, Videos & Testimonials Form, HIPAA 208*** prior to taking any such use or disclosure action.

Images and Videos:

On occasion, a patient's condition, a unique injury, or a specialized rehabilitation technique is photographed and/or videotaped. If we believe that sharing this photograph and/or videotape could enhance the patient's condition or rehabilitation, or that of subsequent patients, we will request permission to share the image or video with professional colleagues or other specified individuals. If the patient agrees to allow sharing, the process will proceed by completing both forms noted above. This process is not necessary if the image or video does not, in any way, identify the patient.

PROCEDURE:

The attending therapist desiring to share and/or post testimonials, images, videos, etc., must explain the purpose of using and/or disclosing the patient's PHI as well as describe the venue in which it will be viewed or heard if the patient agrees to the request the attending therapist will provide him/her with the proper forms for completion. Once the patient has completed and

signed the authorization and consent forms, the therapist will review them for accuracy, make a copy for the patient, and give the originals to the business office designee for filing or scanning. If the document is scanned, the original hard copy will be shredded and disposed of in a compliant manner. Special attention will be given to reviewing the background that is visible in videos or photographs to ensure that other patients are not inadvertently exposed. If this occurs, permission must also be obtained from the individuals involved.

At no time will any retaliatory action be taken against a patient if he/she declines the therapist's request for use and/or disclosure. Additionally, the patient can, at any time, revoke his/her authorization and consent, and Inspirit Therapy Associates will immediately take action to eliminate the use or disclosure, subject to the approval and consent.

NOTE: When using photos or videos, even with permission, be sure to review the visible background for PHI/ePHI, as well as other patients for whom permission has not been obtained. All patients in the photo/video must permit their use prior to publishing.

1.037: Use or Disclosure of Reproductive Healthcare Privacy Protected Health Information - Overturned/Vacated

Note: The Reproductive Healthcare Rule per Purl v HHS declared major portions of the 2024 RHC Rule to be unlawful, and it vacated those provisions. Under the Administrative Procedure Act (5 U.S.C. § 706(2)), when a court "sets aside" an unlawful agency action, the regulation ceases to exist, with OCR treating the RHC Rule and attestation requirements as void.

Unless a state passes legislation that is more stringent than HIPAA's Use and Disclosure provisions, providers are not required to comply with the 2024 RHC Rule unless it is reinstated on appeal or through new rulemaking. Providers should apply HIPAA Privacy Rule standards for Use and Disclosure as stipulated in the preceding policies.

1.038 Substance Use Disorder or Treatment Records

Effective/Revision Date: Feb 16 2026
Policy Classification(s): HIPAA

POLICY:

The Substance Use Disorder policy establishes standards and procedures for the protection, use, and disclosure of Substance Use Disorder (SUD) records in compliance with 42 CFR Part 2, as amended, and the Health Insurance Portability and Accountability Act (HIPAA), with an effective date of February 16, 2026. This policy ensures that patients receiving services at Inspirit Therapy Associates are afforded enhanced confidentiality protections when SUD-related information is present in the clinical record. SUD records may not be used or disclosed to initiate or substantiate criminal charges, civil actions, or administrative or legislative proceedings against a patient without a valid Part 2 Court Order.

This policy applies to all workforce members, including employees, contractors, students, and volunteers, regardless of record format (paper, electronic, or verbal). Workforce members will

be oriented to SUD requirements; violations of this policy may result in disciplinary action up to and including termination. Questions regarding SUD disclosures must be directed to the practice's HIPAA Officer before releasing information.

All SUD records require additional safeguards beyond standard HIPAA protections and apply to all SUD information, regardless of payer type or clinical setting.

DEFINITIONS/TERMS:

1. Substance Use Disorder (SUD) Record is any information, whether recorded or not, that:
    a. Identifies an individual as having or having had a substance use disorder, and
    b. Is created, received, or maintained by a Part 2 program or a provider who has received such information from a Part 2 program.

2. Part 2 Program is an individual or entity that holds itself out as providing, and does provide, substance use disorder diagnosis, treatment, or referral for treatment. Note: Outpatient therapy providers are generally not Part 2 programs; however, Part 2 obligations apply when SUD records are contained in any records received and or maintained.

PROCEDURE:

SUD records may not be used or disclosed unless the patient provides a written authorization that meets Part 2 requirements, with limited exceptions permitted by law. The SUD authorization exceeds the general HIPAA Authorization requirements. See: SUD Consent Form HIPAA 277.

The SUD authorization must:

1. Be in writing.
2. Identify the patient.
3. Identify the specific recipient(s).
4. Specify the purpose of the disclosure.
5. Describe the information to be disclosed.
6. Include an expiration date or event.
7. Be signed and dated by the patient (or authorized representative).

Legal Authorization Exceptions:

Our practice may disclose records without a patient's authorization:
1. In a medical emergency where patient consent cannot be obtained.
2. When authorized entities conduct audit and evaluation activities.
3. For research, in accordance with applicable safeguards.
4. For court orders that specifically authorize disclosure under Part 2. Note: Subpoenas, warrants, or general court orders do not override Part 2 protections unless they meet Part 2 requirements.

Segregation of Records:

This facility will segregate SUD records from its general clinical records, limit access to only workforce members with legitimate treatment or operational needs, and disclose only the minimum necessary. Additional access controls will be applied to all electronic medical records.

All patients have the right to:

1. Receive a clear explanation of how their SUD records are protected.
2. Revoke their consent at any time (except to the extent action has already been taken).
3. Request an accounting of disclosures, where applicable.
4. File a complaint without retaliation.