SOUTHWEST IDAHO ENT
Ear Nose and Throat, P.A.

SOUTHWEST IDAHO SURGERY CENTER

HIPAA PRIVACY NOTICE

Revised: 7/2017, 8/2019, 12/2020, 10/2022

POLICY:

Privacy Notice Requirement:

All patients must be offered a Privacy Notice, which will provide information on:

- The ways in which the Center will use and disclose the patient's personal health information
- The patient's rights under HIPAA
- The Center's duties under HIPAA

Provision of Privacy Notice:

The Privacy Notice must be offered on or before the first encounter with the patient (e.g., the day of the procedure). If the patient returns to the Center for another procedure, the Privacy Notice does not have to be provided again unless the Privacy Notice has been revised since the patient's last visit. Copies must always be available and provided to patients upon request.

The Privacy Notice is offered to the patient on the day of surgery.

Posting of Privacy Notice:

The Privacy Notice must be posted in a clear and prominent location in the Center (in such a place where the patient would reasonably be expected to look, e.g., the waiting area). If the Privacy Notice is revised, the posted version must promptly be replaced with the new version.

Acknowledgment of Privacy Notice:

In the patient's chart, the Facility Consent contains the acknowledgment form, which is signed by the patient on the date of service.

The acknowledgment is a statement that the patient has received the Privacy Notice. If a signed or initialed acknowledgment cannot be obtained, the Center must document the good faith efforts that were made to obtain the acknowledgment and the reason why the acknowledgment could not be obtained. If the acknowledgment cannot be obtained because of an emergency, the Center must make good faith efforts to obtain the signed or initialed acknowledgment as soon as practical after the emergency has ended.

Revisions to Privacy Notice:

The Privacy Notice must be revised if there are material changes affecting any of the following:

- The Center's use and disclosures of the patient's information
- The individual's rights
- The Center's duties
- Any other change to the Center's privacy practices

If revisions are made to the Privacy Notice because of a material change discussed above, the revised Privacy Notice must be redistributed to patients who return for another surgery or procedure. The revised Privacy Notice must also be made available and provided to patients or other persons. The revised Privacy Notice must also be posted in the waiting area and, if applicable, on the www.swient.com to replace the existing Privacy Notice.

It is the Policy of this Center that the Privacy Officer will ensure that revised versions of the Privacy Notice are promptly displayed and distributed.

Retention of Privacy Notice:

The Privacy Officer must keep copies of all versions of the Privacy Notice for at least six years. Signed acknowledgments and Good Faith Effort forms must also be kept for at least six years.

PROCEDURE:

The Director of Nursing will be responsible for posting the Privacy Notice in the waiting area or other location where patients will see it.

The Privacy Notice may be included in the package of information that is provided to all physician offices for distribution to patients prior to their date of service.

1. When a patient signs in for a procedure, the front desk staff is responsible for determining whether the patient has visited the Center in the past and checking to see if the patient has a signed or initialed acknowledgment on file.
2. If the patient does not have a signed or initialed acknowledgment on file, employees are responsible for giving the patient a copy of the current Privacy Notice and obtaining a signed or initialed acknowledgment.
3. If the acknowledgment cannot be obtained because of an emergency, employees will obtain the signed acknowledgment as soon as practical after the emergency situation has ended. If the acknowledgment cannot be obtained on that date of service, a Good Faith Effort form will be completed, and an attempt will be made to get the acknowledgment signed on the next date of service.
4. If the Privacy Notice is revised because of a material change in the Center's privacy practices, the Privacy Officer will coordinate the distribution of the revised Privacy Notice to all patients, in all preassembled packets of information, to all physician offices and will replace the existing Privacy Notice form posted in the Center, on the website and in any other location.
5. The Privacy Officer is responsible for retaining copies of the Privacy Notice and all revisions in a file for at least six years.
6. The Privacy Officer is responsible for ensuring that the Center retains a copy of the acknowledgment or Good Faith Effort forms for at least six years.

Incident Response Plan:

The purpose of this Incident Response Plan (IRP) is to provide guidance on the appropriate steps to be taken and documented in the event of a possible security incident or data breach, from the time of the suspected breach to post-incident response closure, so that all incidents are handled in a consistent manner and the exposure to the potentially breached party is limited. It also provides a methodology for collecting evidence in the event of criminal activity. Documentation of responsive actions taken in connection with any security incident or data breach, as well as documentation of the post-incident events and actions taken, is critical in making appropriate changes to business practices to improve the safeguarding and handling of Company Sensitive Information and PHI.

APPLICABILITY:

This IRP process applies to all employees, administrative consultants, contractors and anyone who may experience or witness a security incident or possible data breach. After discovery, this process provides Information Technology with a checklist or outline for responding so that steps or information related to the incident are not missed. We are committed to protecting our information and responding appropriately to a security incident or data breach.

SCOPE:

Protection of our information and data is paramount. This IRP will provide a checklist for responding to a security incident or potential data breach. An incident can be intentional or unintentional, and this IRP could be implemented in response to many events having an adverse effect on the SWISC network.

GUIDELINES:

This IRP describes our safeguards to protect sensitive information, including PHI. These safeguards are provided to:

- Protect the confidentiality, integrity and availability of data and the SWISC network.

- Protect against a data breach that could result in harm or inconvenience to a client or user and meet any notification requirements.
- Protect against anticipated threats or hazards to the security or integrity of sensitive information, including PHI.
- Identify and assess the risks that may threaten PHI.
- Conduct a reasonable investigation to determine the likelihood of information that has been or will be misused.
- Conduct a post-incident investigation, after-action report and plan of correction.
- Develop written policies and procedures to manage and control these identified risks or vulnerabilities.
- Adjust the Information Security Program to reflect changes in technology, the sensitivity of data stored and internal or external threats to information security.

PROCESS:

This section establishes suggested steps for responding to an incident and initiating the IRP.

I. Incident Response Process—Initial Discovery

1. Anyone suspecting or noting a security incident, data breach, potential system compromise or malicious activity contacts the Network Administrator.
2. The Network Administrator determines if there has been a security incident and the nature and seriousness of the incident by considering the following questions and documents the initial triage.
    - Does the system contain Company Sensitive Information or PHI?
    - Is there a chance that outside law enforcement may need to get involved?
    - Is there a requirement or desire to perform a forensics analysis of the system compromised?
    - If the answer is “yes” to any of these questions, immediately coordinate actions to be taken and apply the guidelines below as appropriate.
    - If the answer is “no” to all the questions, apply the guidelines below as appropriate.
    - Do a preliminary analysis—isolate the compromised system by disconnecting the network cable. If this is not feasible or desirable, block access to the compromised system via the network.
3. Determine the security incident type—try to determine the cause of the malicious activity and the level of system privilege attained by the intruder, and implement appropriate remedial measures.
4. If a system is compromised:
    - Disable any compromised accounts and terminate all processes owned by them.
    - Compile a list of IP addresses involved in the incident, including log entries if possible.
    - Determine the users who need to change their passwords due to the compromise, as well as whether or not they have accounts on other systems using the same credentials.
    - Notify the owners of the compromised accounts and reissue credentials. Consider the likelihood of the intruder having access to the compromised account email and utilize other contact methods.
    - Require all affected users to update their passwords.
    - Rebuild the system, and verify that its network access should be reestablished.
    - Perform a network vulnerability scan of the system after it is unblocked to identify any unresolved security issues that might be used in future attacks against the system.

II. After-Action Reporting

1. Communicate with all affected parties within 48 hours of the completion of the response.
2. Review the chronology of the event.
3. Identify what went wrong and what went right. For instance, “Encryption was used on the file server containing Company Confidential Information and PHI.”
4. Identify the threat or vulnerabilities that were exploited and determine whether they can be alleviated.
5. Review if all intrusion detection or prevention was in place, active and up to date.
6. Document lessons learned and assign appropriate updates to IRP.

III. Incident Response—Breach Notification

1. If a security incident is suspected to be a data privacy breach, immediately notify the Network Administrator.
2. Determine what information was suspected to be breached (i.e., specific individuals' first and last names with a type of PHI).
3. When appropriate, bring in an incident response expert or law enforcement to conduct an investigation. Identify the scope, time frame and source(s) of the breach, the type of breach, whether data encryption was used and for what and possible suspects (internal or external, authorized or unauthorized, employee or nonemployee user).
4. Review for other compromised systems.
5. Monitor all systems for potential intrusions.
6. Determine the notification requirements (statutory or contractual) and address within the required timeframe.

WORKFORCE TRAINING:

It is Southwest Idaho Surgery Center's Policy to train all members of its workforce who have access to PHI on its privacy policies and procedures.

All staff members receive HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Company's privacy policies and procedures.

SAFEGUARDS:

Southwest Idaho Surgery Center has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements.

Southwest Idaho Surgery Center implements Business Associate Agreements with all contracted services in an effort to protect our health information.

Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets and periodically changing door access codes. Additionally, all staff members can only access PHI by using their own login information. Firewalls ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions and that they will not further use or disclose PHI in violation of HIPAA's privacy rules. Currently, all data in the local data center is backed up using industry standards with off-site storage of media. Axis currently utilizes technology that allows the IT team to quickly remove, disable and start staff member access to PHI.

SANCTIONS:

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Plan will be imposed in accordance up to and including termination.

MITIGATION:

Southwest Idaho Surgery Center shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of a participant's PHI in violation of the policies and procedures set forth. As a result, if an employee becomes aware of a disclosure of protected health information, either by a staff member of the Company or an outside consultant/contractor that is not in compliance with this Policy, they should immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

RETALIATORY ACTS:

No employee may intimidate, threaten, coerce, discriminate against or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation or opposing any improper practice under HIPAA. No individual shall be required to waive their privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

POLICY:

The Policy includes provisions to describe the permitted and required uses and disclosures of PHI by Southwest Idaho Surgery Center.

Specifically, the Policy document requires Southwest Idaho Surgery Center to:

- Not use or further disclose PHI other than as permitted by the Policy or as required by law.
- Ensure that any agents or subcontractors to whom it provides PHI received from the Company agree to the same restrictions and conditions that apply.
- Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures.
- Make PHI available to participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures.
- Make the Company's internal practices and records relating to the use and disclosure of PHI received by the Company available to the Department of Health and Human Services (DHHS) upon request.

DOCUMENTATION:

The Company's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented. If a change in law impacts the Privacy Notice, the Privacy Policy must promptly be revised and made available. This change is effective only with respect to PHI created or received after the effective date of the notice. Southwest Idaho Surgery Center shall document certain events and actions (including authorizations, requests for information, sanctions and complaints) relating to an individual's privacy rights. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

INCIDENT REPORTS:

The Company has developed an Incident Report form. This form is used to document reports of privacy breaches that have been referred to the Privacy Officer from staff members who have reviewed or received the suspected incident. After receiving the Incident Report form from staff members, the Privacy Officer classifies the incident and its severity and analyzes the situation. Documentation shall be retained by the Company for a minimum of six years from the date of the reported incident. If the Privacy Officer is able to resolve the incident, the Privacy Officer shall also document the actions taken to resolve the issue in the Incident Report form.

COMPLIANCE:

Violations of this Policy may lead to the suspension or revocation of system privileges and/or disciplinary action. SWISC reserves the right to advise appropriate authorities of any violation of law.

ACCOUNTABILITY AND EXCEPTIONS:

All users are accountable for reporting any suspected data breach of the SWISC network to the Network Administrator. Internal Audit is responsible for ensuring compliance with the HIPAA Security Regulations-Compliance Policy and the controls created to safeguard the network.

Information Technology responds to the incident, analyzes and collects the audit records and any logs, redeploys new credentials to affected users after identification and is responsible for maintaining updates to the Information Security Program annually.

Any exceptions must be approved by the Medical Director and Network Administrator. This plan has been approved by the Governing Board.

TERMINATING USER ACCESS:

Procedures to terminate access to PHI will also include termination of physical access to the Surgery Center. The Center will change door codes periodically and ensure keys, identification badges and timeclock cards are all returned. The IT security officer is notified of the employee's departure and deactivates their accounts.

ACCESS AUTHORIZATION:

Southwest Idaho Surgery Center will grant access to PHI based on an individual's job functions and responsibilities. The Privacy Officer, in collaboration with IT and senior management, is responsible for determining which individuals require access to PHI and what level of access they require through discussions with the individual's manager and/or department head. The IT department will keep a record of authorized users and the rights that they have been granted with respect to PHI. IT keeps a comprehensive matrix of how and to whom rights are granted.

PHI INVENTORY:

PHI	Type & Location	Used By	Disclosed By	Purpose of Use
Paper Medical Record	Nurses station, front desk cabinetry, billing office	Reception staff, nursing staff, physicians, billing staff	Billing staff	Registration, patient care, billing
Electronic Schedule	All computers	Reception staff, nursing staff, billing staff	NA	Registration, patient care, billing
Paper Schedules	Nurses station, operating rooms, sterile processing	Physicians, nursing staff, operating room staff, sterile processing staff	NA	Patient care
Incident Reports	Manager's office	Manager	NA	Incident tracking and quality analysis
Claims	Billing office	Billing staff	Insurance companies	Billing

USE AND DISCLOSURE:

The Company will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- **Use**: The sharing, employment, application, utilization, examination or analysis of individually identifiable health information by any person working for or within the Company or by a Business Associate of the Company.
- **Disclosure:** For information that is protected health information, disclosure means any release, transfer, provision of access to or divulging in any other manner of individually identifiable health information to persons not employed by or working within Southwest Idaho Surgery Center with a business need to know PHI.

ACCESS TO PHI:

All staff who perform participant functions directly on behalf of the Company or on behalf of group health plans will have access to PHI as determined by their department and job description, and as granted by IT. These employees with access may use and disclose PHI as required under HIPAA, but the PHI disclosed must be limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Policy and the use and disclosure procedures of HIPAA. Staff members may not access either through our information systems or the participant's medical record the medical and/or demographic information for themselves, family members, friends, staff members or other individuals for personal or other non-work-related purposes, even if written or oral participant authorization has been given.

MINIMUM NECESSARY:

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual
- Uses or disclosures made pursuant to a valid authorization
- Disclosures made to the Department of Labor
- Uses or disclosures required by law
- Uses or disclosures required to comply with HIPAA

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any business associate or providers or for internal/external auditing purposes, only the minimum necessary amount of information will be disclosed. All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

For making requests for disclosure of PHI from business associates, providers or participants for purposes of claims payment/adjudication or internal/external auditing purposes, only the minimum necessary amount of information will be requested. All other requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Authorities:

45 CFR §164.520 (Privacy Notice)

45 CFR §164.530 (Documentation and retention)

45 CFR Parts 160 and 164, RIN 0945-AA03 Modification to the HIPAA and HITECH Rule, Effective 9.23.13