SUBJECT: HIPAA GENERAL POLICY PRIVACY & SECUTRITY OF PROTECTED HEALTH INFORMATION
LIFE SCIENCE RDD SERVICES, LLC

REFERENCE: 126
PAGE: 1
OF: 24
EFFECTIVE: 06/15/2017
REVIEWED: 2019, 05/2021, 7/2023

POLICY:
The Life Sciences RDD Services LLC, employees and non-employee members of its workforce who have access to, use, create or disclose health information have a legal and ethical obligation to respect the privacy of patients and fellow employees by maintaining protected health information, "PHI," in strict confidence.

STATEMENT OF PURPOSE:
To describe the Surgery Center's overall policy for maintaining privacy and confidentiality of protected health information as required by the Health Insurance Portability and Accountability Act of 1996 and any applicable state law.

DEFINITIONS:
- Health information means any information, whether oral or recorded in any form or medium (e.g., computer record) that:
    - Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
    - Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.
- Protected health information, otherwise known as "individually identifiable health information," that includes any and all health information records that:
    - Identifies the patient; or
    - There is a reasonable basis to believe the information can be used to identify the patient.
- Electronic protected health information (or "EPHI") is PHI that is created, received, maintained, or transmitted in electronic form.
- Authorization permits a covered entity to use and disclose only specific protected health information to specified individuals for specified purposes that are almost always for purposes other than treatment, payment or healthcare operations. An authorization has an expiration date.
- Business Associate is a person or entity who is not a member of the covered entity's workforce who performs a function for or on behalf of a covered entity that involves the use or disclosure of PHI.
- Designated Record Set is a group of records or any item, collection, or grouping of information that is maintained, collected, used or disseminated by or for the covered entity.
- Disclosure means the release, transfer, provision of access to, or divulging in any other manner, of information outside the entity holding the information.
- Covered entity means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form.
- Indirect treatment relationship means a relationship between an individual and a health care provider in which:
    - The health care provider delivers health care to the individual based on the orders of another health care provider; and

  - The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care services to another health care provider, who then provides the services or products, or reports the diagnosis or results to the individual. Providers with an indirect treatment relationship are not required to obtain a patient authorization; e.g., a radiologist that only reads and interprets an x-ray does not need to obtain patient authorization to use or disclose PHI for that purpose.
- Health care operations include, but are not limited to, any of the following activities of the covered entity:
  - Conducting quality assessment or improvement activities;
  - Reviewing the competence, qualifications or performance of health care practitioners, evaluating health plan performance, conducting training programs in which students, trainees or practitioners of health care learn under supervision to practice or improve their skills, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
  - Underwriting, premium rating, and other activities relating to health insurance or health benefits;
  - Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
  - Business planning and development, and;
  - Business management and general administrative activities of the entity; i.e., resolution of internal grievances, customer satisfaction surveys, due diligence in connection with the sale or transfer of assets to a covered entity, etc.
- Minimum necessary is defined as the least amount of PHI required to accomplish the purpose of the use or disclosure. For example, records compiled in response to a PHI request for a specific date of service should not include treatment records for other dates of service. However, the minimum necessary limitation does not apply when a disclosure is made for treatment purposes.

CONTENTS:

POLICIES:

1. HIPAA Compliance Officer and Committee [45 CFR § 164.530 (a)]

The HIPAA Compliance Officer for this covered entity shall be an assistant to the Medical Director. The responsibilities of the HIPAA Compliance Officer include general oversight of HIPAA compliance including Privacy and Security, keeping the center current on policies and procedures regarding HIPAA, receiving and responding to complaints about the Privacy and Security procedures of this facility and responding to requests from the individual wishing to exercise their rights under HIPAA Law. Documentation and logs will be kept in compliance with HIPAA laws. The center's HIPAA Committee will consist of the Compliance Officer, Executive Director, Pre and Post Op manager, and Surgery Manager.

2. Employee Responsibilities

Employees will not use or disclose any patient or employee PHI unless specifically authorized to do so under existing state or federal law, by the patient or his/her authorized representative, or by order of a court.

An employee will, upon the request of, or upon termination of his/her relationship with, The Life Sciences RDD Services LLC, return any PHI obtained from or through the centers resources or which were made available to the employee pursuant to the performance of his/her duties for the Surgery Center.

Any requests for copies of PHI should be scrutinized carefully to ensure that the requestor is properly authorized; e.g., legal representative/guardian, or the request is accompanied by a valid written authorization signed by the patient.

All employees are responsible for safeguarding Protected Health Information from any intentional or unintentional use or disclosure that is a violation of the HIPAA Privacy and Security Rule.

Violations of the HIPAA Privacy or Security policies and procedures will be grounds for disciplinary action, up to and including immediate termination.

2.2 Non-Retaliation

This facility recognizes and supports the responsibility and right of every individual to address potential HIPAA concerns and to request guidance without fear of punishment or harassment from others, including co-workers, supervisors and leadership. Therefore retribution, retaliation or harassment of any kind against any person who requests guidance or brings a violation, real or perceived, to the attention of leadership, is forbidden.

3. Training [45 CFR §164.53O (b)

Employees are expected to understand their responsibilities under the Federal Privacy Rules and corresponding state laws and regulations that deal with the use and disclosure of PHI. As such, all employees are required to

A. Complete their initial HIPAA Privacy training upon hire
B. Complete their initial HIPAA Security training upon hire
C. Document evidence of such training completion to the Life Sciences RDD Services LLC's Director
D. Training will include:
a. Patient Confidentiality
b. Appropriate Safeguards and breaches
c. Email and Internet Usage
d. Usage and Disclosure of PHI
e. Notice of Privacy Practices (including Individual Rights)
f. Annual training regarding updates to HIPAA Privacy and Security
g. Validation that the training is effective

4. Disciplinary Policy [45 CFR §164.530(e)]

Any member of this facility's workforce who fails to comply with this facility's policies and procedures or the requirements of the HIPAA privacy or security rule shall be subject to sanctions imposed through this facility's discipline and discharge policies.

Examples of the sanctions that may be applied for certain actions are:

1. Failure to promptly report any violation of this facility's policy or procedure or requirement of the HIPAA privacy or security rule to the Privacy Officer.
    a. First Incident - Written Reprimand
    b. Second and Third incidents — employee counseling and re-education.
    c. Fourth incident — possible termination.
2. Inadvertent violation of any of this facility's policies or requirement of the HIPAA privacy or security rule.
    a. First Incident - Written Reprimand
    b. Second and Third incidents— employee counseling and re-education.
    c. Fourth incident — possible termination.
3. Knowingly violating of any of this facility's policies or requirements of the HIPAA privacy or security rule.
    a. First Incident - Written Reprimand
    b. Second incident —possible termination.
4. Knowingly and improperly obtaining or disclosing electronic protected health information - Termination of Employment.
5. Obtaining protected health information under false pretenses - Termination of Employment.
6. Obtaining or disclosing protected health information with intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm - Termination of Employment.

The Privacy Officer/Medical Director and/or Human Resources Director shall cause written documentation of the sanctions that are applied, if any, to be kept in written or electronic form for six (6) years after the date of its creation or the date when it is last in effect, whichever is later.

In addition, violations may subject the offender(s) to civil or criminal fines and penalties.

A. Civil penalties maybe assessed in the amount of $100 per incident, up to $25,000 per person, per year, for violations of a similar nature.
B. Federal criminal penalties may apply to individuals that knowingly and improperly disclose PHI or obtain PHI under false pretenses. Penalties would be higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing PHI; up to $100,000 and up to five years in prison for obtaining PHI under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

5. Complaint Process [45 CFR §164.530(d)]

Individuals who desire to make a complaint against this facility concerning the privacy and security policies and procedures, compliance with these policies and procedures or the requirements of the HIPAA privacy and security rules may do so by filing a written complaint to the Privacy Officer.

The Privacy Officer will investigate the complaint and respond to the individual in writing concerning their findings, and what action, if any, the facility will take in response to the complaint.

Written documentation of any complaints and the associated response to the complaint shall be kept for six years.

6. Documentation Requirements [45 CFR §164.530]

This facility will adhere to the HIPAA documentation standards and will maintain the HIPAA policies and procedures in written or electronic form for six years from the date of its creation or the date when it last was in effect, whichever is later. Additionally, complaints, any requests from individual's regarding their rights under HIPAA law, and any responses to those requests or complaints will be maintained for six years.

7. Permitted Uses and Disclosures [45 CFR §164.506]

Employees will not use or disclose any patient or employee PHI unless specifically authorized to do so under existing state or federal law, by the patient or his/her authorized representative, or by order of a court.

If a patient desires a copy of all or any part of his/her record, the release for this information (see attached) will be provided to the patient as soon as possible and the record will be provided to them in person or by mail within 30 days of the request.

Employees shall not:

1. Transmit PHI through any communication system (i.e., e-mail, fax, etc.) that does not have appropriate safeguards. The existence of appropriate safeguards should not be assumed unless authorized Network personnel have provided such assurances to users of these systems.
2. Discuss or otherwise disclose PHI to any individual or entity unless such communication / disclosure
    a. is necessary for treatment, payment or health care operations (as defined above),
    b. is subject to disclosure that does not require authorization as described in the center's Notices of Privacy Practices
    c. is to the individual
    d. has been authorized by the individual
    e. a use or disclosure requiring an opportunity to agree or object
    f. is required to the Secretary of DHHS for enforcement of the HIPAA Privacy Rule

3. Disclose PHI to anyone unless reasonable steps have been taken to confirm and verify the receiving party's identity and authorization to have access to such information.

8. Minimum Necessary [45 CFR §164.502(b)]

Unless the request is made for treatment purposes, to the individual, with a valid authorization, required by law or to Department of Health and Human Services (DHHS) for Privacy Rule enforcement purposes only the "minimum necessary" information that will satisfy the request shall be disclosed (see the "minimum necessary" definition above). Access authorization will be on a need to know basis only.

9. Appropriate Safeguards [45 CFR §]64.530('c,)J

All employees are responsible for safeguarding Protected Health Information from any intentional or unintentional use or disclosure that is a violation of the HIPAA Privacy and Security Rule. The administrative, technical and physical safeguards this facility has in place to safeguard the privacy and security of protected health information and to limit incidental uses or disclosures included, but is not limited to:

- Disposing of all paper material containing PHI in appropriate bins or receptacles designated for destruction of confidential information
- Disposing of used of unused specimen cups, tubing, vials and other materials that may be labeled with PHI in appropriate waste receptacles
- Securing medical record storage
- Adhering to the facility Medical Record Destruction/Retention Policy.
- Escorting visitors and vendors in areas where PHI may be visible
- Avoid leaving patient records unattended in areas where they may be viewed or accessed by unauthorized persons
- Keeping voices low when discussing patient information
- Refraining from discussing patients in public areas outside of the facility
- Following Fax Transmittal Procedures
- Requests for PHI made via telephone — place a call back to the requesting facility to verify origination of call or confirm origination of call on caller ID.
- Turn computer screens away from visitors or any other unauthorized persons when feasible
- Use automatic log-offs that time out the session after a designated period of inactivity Password sharing is prohibited

10. Opportunity to Agree or Object [45 CFR § 164.510]

In the following situations, PHI may be released if the individual is informed in advance and given the opportunity to object or prohibit or restrict such disclosures:

- Facility Directory — name, location, general condition and religious affiliation may be put in the patient directory for use by callers or visitors who ask for the patient by name and by clergy
- To family, friends or others involved in the individual's care or payment for care

"No Information" Patient
A patient has the right to request that no information about his/her admission be given to anyone who calls to inquire or who comes to visit. When a request for patient information comes from "the outside," if the patient is a no information, state "I'm sorry, we have no information about a patient by that name."

Information regarding "Release of General Patient Information" is available for patient education on "No Information." It is included in this section, and will be given to any patient requesting "No Information." A "No Information" request form will be signed by the patient and placed in the front of the medical record.

The person obtaining the "No Information request will be responsible for obtaining the consent form and notifying Registration, Patient Rooms, and OR to place a "No Information" next to the patient's name on the schedule.

11. Authorizations [45 CFR §164.508J

The Medical Records Staff maintains the paper hardcopy of patient records for 3 months for physician and nurse review. They are then scanned into the computer and placed into the appropriate locked confidential container to be professionally shredded within 1 month. The medical records staff is responsible for monitoring, controlling and releasing any paper records.

12. No Authorization Necessary [45 CR §164.512]

There are certain circumstances in which the facility is not required to obtain a HIPAA compliant authorization prior to using or disclosing the patient's PHI. The disclosures listed below must be tracked so that they can be retrieved and listed in an accounting of disclosures.

The following are situations when PHI can be disclosed without the patient's written consent or authorization:
12.1 When required by law: This facility may disclose PHI when a law requires that it report information about suspected abuse, neglect or domestic violence, or related to suspected criminal activity, for FDA-regulated products or activities, or in response to a court order. PHI may also be disclosed to authorities that monitor compliance with these activities.

Michigan reporting requirements:
- Abortion procedure report to Michigan Department of Public Health (MDPH)
- Abuse/neglect/exploitation of Adult to Michigan Department of Social Services (MDSS) or Law Enforcement (see DUTY TO WARN/REPORT below)
- Abuse/neglect/exploitation of nursing home patient to MDSS or Law Enforcement (see DUTY TO WARN/REPORT below)
- AIDS/HIV report to Local Health Department
- AID S/HIV or other infectious agents, if present at death, to funeral director
- Asphyxiation or death by drowning, to local Law Enforcement
- Births to local registrar (city for cities greater than 40,000 population; otherwise county)
- Birth defects, to MDPH
- Cancer Registry cases to MDPH

- Child Abuse / neglect to the Michigan Family Independence Agency (MFIA) or Law Enforcement (see DUTY TO WARN/REPORT below)
- Designated Conditions (specified communicable diseases, infections and non- communicable diseases, per Michigan Admin. Code.R325.171 et.seq.) to County/Local Health Department
- Death of infant under two years of age, cause unknown, to County Medical Examiner.
- Death to County Medical Examiner, if death occurs more than 10 days after the deceased was last seen by a physician, if the cause of death appears to be other than the illness or condition for which the deceased was being treated, or if the attending physician cannot accurately determine the cause of death,
- Fetal death (a fetus which has completed at least 20 weeks of gestation or weighs at least 400 grams), to MDPH
- Lead poisoning or Reyes syndrome, to MDPH
- Misadministration of radioactive materials to Nuclear Regulatory Commission
- Occupational diseases aggravated by workplace exposure, to MDPH
- Spinal cord and traumatic brain injury, to MDPH
- Deadly weapon (knife, gun, etc.) to local Law Enforcement

Duty to Warn/Report for Victims of Suspected Abuse, Neglect, Violence:

While patient's confidentiality is a protected right, the law provides exceptions to that right in certain circumstances. Two major exceptions are duties to warn, and to report circumstances to third parties when necessary to protect the patient or others. Many reporting activities are required for statistical purposes and are done by Administration. In two instances, however, most licensed caregivers, including a physician, physician's assistant, nurse, person licensed to provide emergency medical care, psychologist, or social worker) is called upon to report or warn third parties based upon information learned in the treatment of the patient. These are:

1. duty to report abused children, and
2. duty to report when impaired adults appear to have been abused.

Suspected Child Abuse:
Caregivers must report child abuse arises when the caregiver has reasonable cause to suspect that a minor (person under 18 years of age) has been physically, sexually or mentally abused or neglected. The caregiver has a legal duty to immediately make an oral report to the county Family Independence Agency or law enforcement agency. A written report must follow within seventy-two (72) hours of the oral report. (If several employees have knowledge of abuse, only one report need be made).

Suspected Adult Abuse:
Caregivers must report (and all other employees may report) suspected adult abuse arises when there is reasonable cause to suspect that an adult is a vulnerable person being abused, neglected or exploited. A vulnerable adult is an individual who is at least 18 years old; and is unable to protect himself or herself from abuse, neglect, or exploitation because of a mental or physical impairment or because of advanced age.

Note that not every case where one adult has harmed another is reportable. The victim must fall within the definition of a vulnerable person. If the victim is an adult who has is not impaired, such as a battered but competent woman, the confidentiality should not be breached.

12.2 Public Health Activities [45 CR §164.512(b)]

This facility may disclose PHI when required by law to collect information about disease or injury, or to report vital statistics to the public health authority.

12.3 Health Oversight Activities [45 CR §164.512(d)]

PHI may be disclosed to officials of a health oversight agency without the express written consent of authorization of the individual. A health oversight agency is a public agency that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights or laws for which health care is relevant. In Michigan, most of these functions are carried out by the MDPH.

12.4 Related to Decedents [45 CR §164.512(g)]

PHI may be released or disclosed to coroners, medical examiners or funeral directors without the patient's or personal representative's express written consent or authorization, as necessary to carry out their duties with respect to the patient who has died. PHI may be released for the purpose of identifying the deceased person, determining a cause of death, or other duties permitted by law.

12.5 To Avert threat to Health or Safety [45 CR §164.5129(j)]

PHI may be disclosed, consistent with applicable law and professional ethical standards, if the Privacy Contact, in good faith, believes that the use or disclosure is needed to prevent or lessen a serious or imminent threat to the health and safety of a person or the public, and the disclosure is made to a person or persons who can reasonably lessen the threat, including the target of the threat.

12.6 Law Enforcement [45 CR §164.512(e) & (f)]

PHI may be disclosed to a law enforcement official without the express written consent or authorization of the individual for law enforcement purposes in circumstances such as:

- Response to a court order
- To identify a suspect, witness or missing person
- About crime victims
- About a death that may be a result of criminal conduct
- Related to criminal conduct at the facility

12.7 For Specific Government Functions [45 CR §164.5129(k)]

PHI may be disclosed without the express written consent or authorization of the individual in certain circumstances such as:

- Releasing PHI of domestic or foreign military personnel to a designated military authority
- To correctional institutions, in certain circumstances
- For National Security and Intelligence Reasons (such as protecting the President)

12.8 Worker's Compensation [45 CR §164.512 (l)]

PHI related to Worker's Compensation issues may be disclosed without the express written consent or authorization of the individual as authorized by and to the extent permitted by State Worker's Compensation law.

12.9 Disaster Relief Purposes [45 CFR §164.510(b) (4)]

PHI may be disclosed, without the express written consent or authorization of the individual, to a public or private organization authorized by law or by its charter to assist in disaster relief efforts, for the purposes of coordinating uses or disclosures relating to notification of a family member, a personal representative or another person responsible for the care of the patient of the patient's location, general condition or death. Examples of these organizations include FEMA (Federal Environmental Management Agency), SEMA (State Environmental Management Agency), Red Cross, Salvation Army.

13. Deceased Individuals [45 CR §l64.502 (f)]

The same standards regarding release or disclosure of PHI will apply to deceased individuals. Privacy protection does not end with an individual's death.

14. De-Identification/Re-identification/Limited Data Set [45 CR §164.514(a), (b), (c)&(e)]

Information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual can be used and disclosed without the individual's written authorization.

Information can be rendered de-identifiable if the 18 identifying elements listed below are removed and if the remaining information could not be used alone or in combination with other information to identify an individual who is the subject of the information.

Eighteen (18) identifying elements:

1. Name
2. Street address, city, county, zip codes
3. Day and month for any date directly related to the individual including birth date, admission date, discharge date, date of death, individuals aged 90 or older
4. Telephone number
5. Fax number
6. Email address
7. Social security number
8. Medical record number
9. Health plan number
10. Account number
11. certificate/license number
12. Vehicle identifier and license plated
13. Device identifier and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers including finger and voice prints

17. Full face photographs
18. Any other unique identifying number, characteristic or code

A code or other type of identifier maybe assigned to allow information de-identified to be re-identified provided the identifier assigned is not derived from or related to information about the individual or could be used to translate the identity of the individual. Additionally, the identifier shall not be used or disclosed for any other purpose and the mechanism for re-identification shall not be disclosed.

A limited data set may be used or disclosed only for the purposes of research, public health, or health care operations and only if this facility enters into a "data use agreement" with the limited data set recipient.

The limited data set excludes the following direct identifiers

1. Name
2. Postal address information, other than town or city, state or zip codes
3. Telephone number
4. Fax number
5. Email address
6. Social security number
7. Medical record number
8. Health plan number
9. Account number
10. certificate/license number
11. Vehicle identifier and license plated
12. Device identifier and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) addresses
15. Biometric identifiers including finger and voice prints
16. Full face photographs
17. Any other unique identifying number, characteristic or code

<u>15. Personal Representatives [45 CR §164.502(g)]</u>

Personal Representatives of an individual will be given the same rights as the individual with respect to the HIPAA Privacy Rule. Exceptions to this rule are: (i) when the release of PHI to the personal representative could endanger the individual (e.g. suspected abuse, neglect or violence); and (ii) PHI relating to health care provided to an un-emancipated minor which the minor lawfully obtained without the consent or notification of the parent or guardian.

Personal Representative means either of the following:

i. a parent or guardian of an un-emancipated minor;
ii. a person empowered by the patient by explicit written authorization to act on the patient's behalf to access, disclose, or consent to the disclosure of PHI;

iii. a guardian appointed under Michigan law (see §MCL 700.5306), to the extent that the scope of the guardianship includes the authority to act on the individual's behalf with regard to his or her health care; or
iv. if the patient is deceased, his or her personal representative or his or her heirs at law or the beneficiary of the patient's life insurance policy, solely for purpose of proving a claim for benefits;

16. Verification of Identity [45 CR §164.514(h)]

Unless the person and their authority are known to the facility, verification of the identity of the individual requesting PHI (whether oral or written) will be obtained by way of a government issued document with a picture identification (e.g. driver's license, passport, military ID).

See Policy: Verification of Identity of Person Requesting Protected Health Information

17. Notice of Privacy Practices [45 CR §164.520]****Existing Policy

All patients must be given a Privacy Notice, which will provide information on:
• The ways in which the ASC will use and disclose the patient's personal health information
• The patient's rights under HIPAA
• The ASC's duties under HIPAA

17.1 Provision of Privacy Notice

The Privacy Notice must be provided on or before the first encounter with the patient (e.g., the day of the procedure). If the patient returns to the ASC 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 may be delivered electronically (e.g., by e-mail) but the patient must first agree to receive the Privacy Notice in this manner. If the ASC receives information that the electronic Privacy Notice was not deliverable, a paper copy must be provided.

17.2 Posting of Privacy Notice

The Privacy Notice must be posted in a clear and prominent location in the ASC (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.

If the ASC has a web site, a copy of the Privacy Notice must be displayed on the web site. If the Privacy Notice is revised, the web site must also be updated with the revised version.

17.3 Acknowledgment of Privacy Notice

At the time the patient is provided with the Privacy Notice, the ASC must make a good faith effort to obtain a signed or initialed acknowledgment from the patient or the patient's personal representative. The acknowledgment is a statement that the patient has received the Privacy Notice. If a signed or initialed acknowledgment cannot be obtained, the ASC 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 ASC must make good faith efforts to obtain the signed or initialed acknowledgment as soon as practical after the emergency situation has ended.

17.4 Revisions to Privacy Notice

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

- The ASC's uses and disclosures of the patient's information
- The individual's rights
- The ASC's duties
- Any other change to the ASC'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 web site to replace the existing Privacy Notice.

It is the policy of this ASC that the Medical Director/Privacy Officer will assure that revised versions of the Privacy Notice are promptly displayed and distributed.

17.5 Retention of Privacy Notice

The Medical Director/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.

17.6 Procedure for providing Notice of Privacy Practices to individuals:

1. The Executive Director/Privacy Officer will be responsible for posting the Privacy Notice in the waiting area, or other location where patients will see it, as well as on the ASC's web site, if applicable.
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. Employees will place a copy of the signed or initialed acknowledgment in the front of the patient's chart.
4. If an employee is unable to get a signed or initialed acknowledgment, he or she is responsible for completing a "Good Faith Effort" Form and placing a copy in the front of the patient's chart.

5. 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.
6. If the Privacy Notice is revised because of a material change in the ASC's privacy practices, the Medical Director will coordinate the distribution of the revised Privacy Notice and will replace the existing Privacy Notice form posted in the ASC and on the web site.
7. The Medical Director/ Privacy Officer is responsible for retaining copies of the Privacy Notice and all revisions in a file for at least six years.
8. The Medical Director/ Privacy Officer is responsible for ensuring that the ASC retains a copy of the acknowledgment or "Good Faith Effort" forms for at least six years not consistent with the MR retention policy

18. Individual/Patient Rights under HIPAA

Individuals/Patients have the following rights in relation to how their PHI is used or disclosed. Individuals will be informed of these rights in the facility Notice of Privacy Practices.

18.1 Right to Request Restriction on Uses and Disclosures [45 CR §164.502(c)]

Patients have the right to request that we limit how this facility uses or discloses their PHI. This request must be made in writing to the Privacy Officer/ Medical Director. The Privacy Officer/ Medical Director will consider the request, but the facility is not legally bound to agree to the restriction. To the extent that the facility does agree to any restrictions on the use/disclosure of the patient's PHI, the facility will put the agreement in writing and abide by it except in emergency situations. This does not apply to disclosures of PHI already made. The facility will not limit uses/disclosures that are required by law.

The agreement to restrict uses/disclosures can be terminated by either the facility or the patient. If the patient terminates or agrees to terminate the restriction, PHI may be used or disclosed as permitted by these HIPAA policies. If the facility terminates the restriction without the patient's agreement, the facility may only use/disclose information created after notification of the termination has been given to the patient.

18.2 Right to Request Confidential Communications [45 CR §164.502(h)]

Patients have the right to request communication via alternative means or location, such as only contacting the patient at work. This request must be made in writing to the Privacy Officer/ Medical Director. The facility must agree to the request if the request is reasonably easy to implement.

Once a request has been made, the facility must implement a procedure to indicate in the patient record that the request has been granted.

18.3 Right to Access [45 CFR §164.524]

Patients have the right to access, inspect and copy his or her own PHI contained in the medical record. Exceptions to this right of access are:

a. psychotherapy notes
b. information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
c. PHI subject to Clinical Improvements Amendments of 1988 (CLIA) 42 U.S.C. 263 a, to the extent the provision of access to the individual would be prohibited by law.

This request must be made in writing to the Privacy Officer/Medical Director. The Privacy Contact or delegated staff member shall act on a request for access no later than thirty (30) calendar days after this facility's receipt of the request. However, if the request for access is for PHI that is not maintained or accessible to this facility on-site, the request for access be acted on no later than sixty (60) calendar days after this facility's receipt of the request. If this facility is unable to take an action on the request within the applicable time required by the preceding paragraph, the facility may extend the time for the action by no more than thirty (30) calendar days, provided:

1. Within the applicable time required by the preceding paragraph, the facility shall provide the individual with a written statement of the reason(s) for the delay and the date by which this facility will complete its action on the request; and,
2. Only one such extension shall be permitted on a request for access.

If the request is granted, in whole or in part, the Privacy Officer or delegated staff member shall inform the individual of the acceptance of the request and provide the access requested.

Access may be denied without providing the individual an opportunity for review of the denial in the following circumstances:

- Information consists of psychotherapy notes, information compiled in anticipation of litigation, or maintained by a CLIA lab
- When this facility is acting under the direction of a correctional institution, this facility may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or for the transporting of the inmate.
- The information is created or obtained during the course of research and the individual has agreed to temporary denial of access while the research is in progress
- The information was obtained from someone other than the health care provider from whom the individual is requesting access, under the promise of confidentiality and the access request would be reasonably likely to reveal the source of the information

Access may be denied if the individual is informed in writing of the denial and of their right to request a review of the denial under the following circumstances:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

- The PHI refers to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person;
- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

If the denial is made based on one of the three situations above, the individual has the right to have the denial reviewed by a licensed health care professional that the facility designates as a reviewing official and who did not participate in the original decision to deny the request for access. The reviewing official will determine whether or not the requested access should be granted or denied. The facility will abide by the decision of the reviewing official.

The covered entity will, to the extent possible, give the individual access to any other PHI requested after excluding the PHI for which the access was denied.

If the request is denied, in whole or in part, the Privacy Officer or delegated staff member shall provide the individual with a written denial explaining:

1. The basis for the denial;
2. If applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights;
3. A description of how the individual may complain pursuant to this facility's complaint procedures;
4. If this facility does not maintain the PHI that is the subject of the individual's request for access and this facility knows where the requested information is maintained, a statement informing the individual where to direct the request for access.

18.4 Right to Request Amendment [45 CFR §164.526]

Patients have the right to request an amendment to PHI held by this facility. The request for amendment must be submitted in writing to the Privacy Contact and must state the reason to support the requested amendment. The Privacy Officer or delegated staff member must act on the request for amendment within 60 days of the receipt of the request. If the request is not able to be acted on within 60 days, the individual will be notified in writing of a 30-day extension and of the reasons for the delay and the date by which the request will be responded to.

If the request for amendment is accepted, the individual shall be informed of the acceptance of the request and the amendment will be made. The Privacy Officer or designee will obtain the individual's identification of relevant persons with whom the amendment needs to be shared and obtain the individual's agreement to allow the facility to notify such persons. Reasonable efforts will be made by the facility to timely inform and provide amendment to persons identified by the individual, including business associates who this facility knows has the PHI which has been amended, and have or may have relied upon the incorrect information to the detriment of the individual.

The request for amendment may be denied if it is determined that the PHI that is the subject of the request:

a. was not created by this facility
b. is not part of the designated record set
c. is not be available to the individual under the right to access rules
d. is accurate and complete

If the request is denied, in whole or in part, the Privacy Officer or delegated staff member shall provide the individual with a written denial explaining:

1. The basis for the denial;
2. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a complaint
3. A statement that if the individual does not submit a statement of disagreement to the denial, the individual may request that the facility provide his or her amendment request and denial with any further disclosures of PHI that is the subject of the amendment request
4. A description of how the individual may complain pursuant to this facility's complaint procedures

If this facility is informed by another covered entity of an amendment to an individual's PHI, the Privacy Officer or designee will amend the PHI contained in the medical record.

18.5 Right to an Accounting of Disclosures [45 CR §1 64.528]

Patients have the right to receive an accounting of disclosures of PHI that have been made in the six years before the request was made including disclosures made by business associates.

The individual must request the accounting of disclosures in writing to the Privacy Contact. The request will be responded to within 60 days of receiving the request, or the individual will be notified of the reason why the request cannot be met in 60 days and indicate when the response will occur. The extension cannot exceed 30 days.

An exception to the individual's right for an Accounting of Disclosures:

A health oversight agency or law enforcement official may request that an individual's right to an accounting of disclosures made to the agency or official be temporarily suspended for up to 30 days. The agency or official must make the request to suspend the individual's right to an accounting of those disclosures in writing, stating that such an accounting to the individual would be reasonably likely to impeded the activity's activities, and specifying the time for which suspension is required.

Disclosures requiring tracking and reporting upon the request of the individual are:

1. Disclosures made accidentally or intentionally, in error, and without the individual's written authorization (e.g. PHI faxed or e-mailed to the wrong number or person, employee inappropriately accesses a co-worker's PHI when access is not authorized);
2. Disclosures required by law;
3. Disclosures for public health activities;
4. Disclosures about victims of abuse, neglect or domestic violence;

5. Disclosures for health oversight activities;
6. Disclosures pursuant to subpoena or judicial or administrative proceeding;
7. Disclosures for law enforcement purposes, such as identifying crime victims or witnesses;
8. Disclosures about decedents to coroners, medical examiners, funeral homes or for cadaver organ or tissue donation;
9. Disclosures for research purposes;
10. Disclosures to avert a serious threat to health or safety of an individual or the public;
11. Disclosures for specialized government functions other than national security purposes; and
12. Disclosures for workers' compensation purposes.

The accounting will be in writing and include the disclosures of PHI that occurred after April 14, 2003 and in the six years prior to the date of the request (or a shorter time period if specified by the individual) including disclosures to or by any facility business associate. A "business associate" is defined as a person or entity that performs a function for or on behalf of the facility, and that function requires the use or disclosure of PHI. If business associate reports to this facility a disclosure listed above, the facility will record this disclosure according to the Accounting of Disclosures procedure.

The accounting will include for each disclosure:

1. The date of the disclosure;
2. The name and address of the entity or person who received the PHI;
3. A brief description of the PHI disclosed; and
4. A brief statement of the purpose of the disclosure.

Reporting of honest and unintentional mistakes will not result in retaliation; however, repeated inappropriate or any intentional unauthorized disclosures of an individual's PHI may result in disciplinary action.

<u>Procedure for tracking/recording accounting of disclosures:</u>

1. For all disclosures listed under "disclosures requiring tracking" above, the employee making the disclosure will follow department procedures for reporting the disclosure.
2. Additional recording and tracking of those disclosures, including inappropriate accidental or intentional disclosures without an individual's authorization, must be done by the employee, as follows:
    a. Collect the following information:
        1) The date of the disclosure;
        2) The name and address of the entity or person who received the PHI;
        3) A brief description of the PHI disclosed; and
        4) A brief statement of the purpose of the disclosure.
3. Record the information on the Surgery Center form. (should be same form as CI-{I/ISC)

Business Associates [45 CFR §164504]

A business associate (BA) is a person, company or entity that performs a function or service for or on behalf of this facility, and creates uses or discloses PHI to carry out that function. A Business Associate is not a member of the facility's workforce.

If the person, company or entity is a Healthcare Provider and the disclosure is for treatment purposes, then the relationship qualifies as an exemption and no written agreement is required.

If an entity meets the definition of Business Associate, this facility may only disclose PHI to that Business Associate if the Business Associate has assured us, through a written contract, which it will comply with all applicable sections of the HIPAA Privacy Rule.

This facility will ensure it enters into a Business Associate Agreement (BAA) with any person, company or entity performing a function or service on behalf of this facility in which PHI is created, used or disclosed to carry out that function. The BAA will become effective on the date of the execution of the Services Agreement and will terminate at the time of the termination or expiration of the Service Agreement. Appropriate use, return, or destruction of all ePHI will be determined in the contract with each BA.

20. Marketing [45 CFR §164.508(a) (3)]

Marketing is defined by the Privacy rule as follows:
"To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."
Before giving or sending a patient marketing material, a HIPAA compliant authorization must be obtained from the patient.

Face-to-face encounters with patients may occur without an authorization to discuss services and products, provide samples, recommend brand name prescriptions, or distribute calendars, pens or gifts of nominal value.

The definition of marketing excludes:

- Communications to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits;
- For treatment of the individual; or
- For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

All other marketing communications require a HIPAA compliant authorization to be signed by the patient prior to sending such communications.

21. Security

21.1 The Security Standard (164.306)

The HIPAA Security Standard aims to ensure the confidentiality, integrity and availability of all Electronic Protected Health Information (EPHI) that is created, received, maintained or transmitted by the Covered Entity.

The standard aims to protect against any reasonably anticipated threats or hazards to the security and integrity of EPHI, and to protect against any reasonably anticipated uses or disclosures of such information.

21.2 Security Policies and Procedures (164.3 16 (a))

Upon hire, new employees receive a copy of the Life Sciences RDD Services LLC's Employee Handbook, and agree to the confidentiality statement that revealing any information about patients or employees to any unauthorized person is not permitted. Their HIPAA training goes into more detail of their access and authorization.

This facility has entered into a BAA with the Miller Media Inc. for all information technology services related to electronic communications and the maintenance of any electronic PHI. Assessments are conducted as necessary to maintain compliance with technical operations and user activity regarding ePHI.

This facility operates under the Security Policies and Procedures of the Miller Media Inc. Information Security Department.

21.3 Policies and Procedures for Access Authorization

All employees must maintain his/her own passwords to access information on specific workstations that allow them to perform their needed functions. These passwords are selected by the employee but designated by Miller Media Inc. to be limited to only the ePHI that their employees' job/duties require.

Non-members are categorized as follows with regards to access authorization:

A. Patients and their families/visitors do not have authorization to use any computer system in the facility in any manner. In the event that an employee and/or their family member is a patient here, it is against the policy of this entity for that employee/family member to access their own ePHI through any of our systems.
B. Vendors, students, and others in the facility with specific duties may observe information that is accessed by the employee/physician for learning or other business purposes pertaining to their need. No password will be provided to these people for their own use of WSC computers.
C. Upon termination of employment, passwords will be deleted to prevent the terminated employee from having access to any of WSC information.
D. All BAAs will have authorization to access the information required by their functions in the BAA agreement.

E. All other non-members of the WSC will not have access to our systems.

21.4 Contingency Plan

The Contingency Plan will determine how ePHI is backed up and recovered in the event of a disaster that prevents the center from accessibility to the ePHI. It will include the emergency mode of operations in case of this type of disaster.

21.5 Security Risk Analysis

A risk analysis will be reviewed annually to protect the center's ePHI.

AUTHORIZATION TO RELEASE PATIENT INFORMATION

Patient Name: _____ Patient Phone No.: _____
Date of Birth: _____

1. I authorize the use or disclosure of the above-named individual's health information as described below:

2. The following individual or organization is authorized to make the disclosure:
   _____
   _____
   _____
   Address:_____
   _____

3. The type and amount of information to be used or disclosed is as follows: (include dates where appropriate)

☐ Most recent discharge summary ☐ Laboratory results from (date) _____to (date)_____
☐ History and physical ☐Entire record from (date) _____to (date)_____
☐ Consultation reports from (doctors' names)_____
☐ Other
_____

4. I understand that the information in my health record may include information relating to: sexually transmitted diseases, acquired immunodeficiency syndrome (AIDS), human immunodeficiency virus (HIV), behavioral or mental health services, treatment for alcohol and drug abuse, and genetic testing; and I consent to the release of that information.

5. This information may be disclosed to and used by the following individual or organization:
   _____
   Address: _____
   For the purpose of:_____

6. I understand I have the right to revoke this authorization at any time. I understand if I revoke this authorization I must do so in writing and present my written revocation to The Life Sciences RDD Services LLC Director. I understand the revocation will not apply to information that has already been released in response to this authorization. I understand the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy. Unless otherwise revoked, this authorization will expire on the following date, event or condition: _____. If I fail to specify an expiration date, event or condition, this authorization will expire in six months.

7. I understand that authorizing the disclosure of this health information to the individual or organization named above is voluntary. I can refuse to sign this authorization. I need not sign this form in order to assure treatment. I understand I may inspect or copy the information to be used or disclosed, as provided in CFR 164.524. I understand any disclosure of information carries with it the potential for an unauthorized re-disclosure and the information may not be protected by federal or state confidentiality rules. If I have questions about disclosure of my health information, I can contact the Patient Relations Representative at 248-731-4514.

I HAVE READ AND UNDERSTAND THIS FORM. I AM SIGNING IT VOLUNTARILY. I AUTHORIZE THE DISCLOSURE OF MY HEALTH INFORMATION AS DESCRIBED IN THIS FORM.

_____ _____

Patient or Personal Representative Signature Date

If you are signing as a personal representative of the patient, describe your relationship to the patient and the source of your authority to sign this form:

Relationship to Patient: _____
Print Name:_____

Source of Authority (attach relevant documents as applicable)
_____