Policy

Title:	HIPAA Policy
Effective Date:	January 15, 2020
Approved By:	President's Council
Responsible Party:	Vice President for Clinical Operations
History:	2/14;10/26/15
Related Documents: University Compliance Plan	

SALUS UNIVERSITY[1]

HIPAA POLICY MANUAL

[1] This policy refers to all clinical operations of Salus University, including but not limited to The Eye Institute and The Pennsylvania Ear Institute, and The Speech-Language Institute, hereinafter referred to collectively as "Salus."

TABLE OF CONTENTS

SALUS UNIVERSITY

HIPAA TRAINING AND POLICIES

HIPAA

Health Insurance Portability and Accountability Act of 1996

Who does HIPAA affect?

HIPAA is a federal statute that affects the entire health care system from patients to employers, health plans, physician offices, hospitals, optometric office, dental offices, billing companies, and other entities providing or dealing with the healthcare of individuals.

What is the scope of HIPAA?

HIPAA affects the privacy and security of Protected Health Information (PHI).

What is the HITECH Act?

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was a federal law that legislation created to stimulate the adoption of electronic health records (EHR) and supporting technology in the United States.

Why do you need to know about HIPAA?

HIPAA is a federal law. It requires all health care personnel to be educated about HIPAA policies and procedures. It includes anyone who does or might have access to any patient information. ALL schools of Optometry, faculty, staff and students must comply with the regulations and be trained on HIPAA regulations.

The Transaction Standard

The transaction standard applies to the electronic transmission of transactions outside of an organization or practice. All organizations or practices were to submit claims electronically to Medicare after October 2003, unless they had fewer than 10 employees.

The Security Standard

The security standard applies to the security of an organization's computer system and any information collected, obtained, transmitted, or stored electronically.

The Privacy Rule

The privacy rule became effective April 14, 2003, and is intended to protect or safeguard the privacy of protected health information. Protected health information is information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; --OR— the past, PRESENT, or future payment for the provision of health care to an individual.

Protected Health Information (PHI)

Protected health information means information that identifies an individual patient (alone or in combination with other publicly available information) and that is:

- Generated or received by a health care provider who engages in the electronic transmissions of individually identifiable health information as part of one of the transactions identified in the HIPAA regulations, a health plan, or a health care clearinghouse.
- Relates to the past, present, or future physical or mental health or condition of the individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual.
- PHI includes demographic information collected from the individual.

PHI can take any form:

- Hard copy
- Electronic
- Oral
- Photographs, video, audio recordings.

Identifiers include, but are not limited to:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo codes,
- Birth date, admission date, discharge date, date of death;
- Telephone numbers.
- Fax numbers.
- Electronic mail addresses.
- Social security numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.

- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images.
- Any other unique identifying number, characteristic, or code.

For a detailed description of the information that must be removed to render PHI “de-identified”, see the policy entitled “DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION,” later in this manual.

Confidentiality of health information

Salus University believes that all patients and employees have the right to have their medical, financial, personal information, records, data, etc. protected from unauthorized viewing, discussion, or disclosure. In order to safeguard this right, employees may only look at, use, discuss, or disclose company, patient, or employee information for reasons which are necessary to the performance of their assigned duties.

A breach of university, patient, or employee confidentiality—whether intentional or unintentional--may result in the immediate termination of employment.

Do's and Don’ts's

- Protected health information can be shared with other outside providers and members of their staff on a "need-to-know" basis. See “MINIMUM NECESSARY STANDARD”
- Verbal communication of confidential information is never to be discussed in open, public areas.
- Disclose information only with the authorization of the adult patient or parent/legal guardian of a child under the age of 18, except for “emancipated minors.” See policy entitled “MINORS”.
- Protected health information should only be given out via the telephone in limited circumstances. Verification of the requester and the necessity for that person to have the information must be obtained.

- Leaving a message confirming scheduled appointments if patient or parent of a minor is not available can be done as long as there is no specific information regarding the nature of the appointment unless the patient or parent has directed you not to leave such messages

- Do not leave specific test results or the details of the test given on an answering machine. Leave only a message to call a specific staff member's name and the appropriate phone number unless the patient or parent has directed you not to leave such messages.

Challenging individuals

Each employee is responsible for challenging an individual who accesses areas that contain protected health information. Employees should question and verify the need of that individual accessing the area.

Ways to maintain confidentiality

- Discuss patient information privately--never in elevators, lobbies, or corridors.

- Charts, forms, and information containing patient information should be face down and if in a mailbox or wall box should face the wall or door.

- Do not leave patient records or information where unauthorized individuals can read them.

- Dispose of unnecessary patient information in proper receptacles for shredding--not ordinary trash.

Faxing protected health information

- All appropriate measures should be taken to protect confidentiality of patient information whenever fax machines are used as a mechanism for transmission.

- A cover sheet containing a standard confidentiality statement must be used with each transmission of protected health information.

- All pre-programmed fax numbers must be verified for accuracy on an annual basis. Create a checklist of pre-programmed fax numbers to be verified annually.

- All fax machines and printers that are used for transmitting or printing protected health information must be placed in secure areas. A secure area is one that is not accessible to the general public or is easily accessed by patients or other individuals.

Accessing protected health information

Direct access to patient medical records for routine business functions shall not be permitted except to treating providers, students and Salus University employees who:

- Display the proper identification
- Have a "need to know" to perform their job duties
- Have been instructed on policies of confidentiality including penalties arising from violation

How can you protect yourself?

Limit the amount of patient information you access to the minimum necessary to do your job. Take special care to respect the privacy of co-workers and colleagues who are patients. Do NOT discuss the health care services of your co-workers with anyone who is not directly involved in their care. Do not ask coworkers why they are patients or reasons for accessing health services.

Privacy of protected health information

Salus (and all health care providers) must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information. "Reasonable safeguards" mean that we must make reasonable efforts to prevent uses and disclosures not permitted by the rule.

The Privacy Rule does NOT require structural or systems changes such as:

- Private rooms
- Soundproofing of rooms
- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners
- Encryption of telephone systems

Notice of privacy practices

- Right to receive a "Notice of Privacy Practices"
- Right to authorize any use or disclosure of protected health information
- Right to restrict use or disclosure of protected health information
- Right to an accounting disclosure of protected health information

- Right to inspect, copy, and request amendments to protected health information

HIPAA requires us to inform all patients of our Notice of Privacy Practices. Each patient will receive a copy one time. New patients will acknowledge receipt with their signature on the demographic intake form.

Patients may request another copy of the Notice of Privacy Practices at any time. A copy is also available on the applicable clinical website and in the lobby of each clinic.

There is a formal process for patients to:

- Request copies of their medical record
- Obtain a list of who has accessed their information
- Make amendments to their medical records
- Complain to the Salus Compliance Officer or the Department of Health and Human Services about our privacy practices

What is a Business Associate Agreement and why is it needed?

PHI may only be shared with Business Associates with whom Salus has entered into an approved Business Associate Agreement (BAA). Salus will take remedial action against any Business Associate who fails to comply with an approved BAA and/or the HIPAA privacy and security regulations.

ACTIVITIES THAT INVOLVE USE OF PROTECTED HEALTH INFORMATION

- Making appointments for patients.
- Sending reminders of existing appointments.
- Reviewing patient database to find patients that need to make an appointment (recalls).
- Intake when the patient comes to the appointment.
- Sign in sheets.
- Waiting room procedures.
- Checking insurance coverage.
- Validating demographic information.
- Retrieving old clinical charts.
- Work up of patient before attending examination.
- Attending examination.
- Writing or phoning medication prescriptions, including responding to validation calls from the pharmacy.
- Validating prescriptions for glasses or contact lenses.
- Assisting patients with prescriptive devices.
- Writing and filling orders for glasses or contact lenses.
- Communicating with outside laboratories. Communicating with device manufacturers.
- Responding to validation calls from outside vendors of contact lenses.
- Referring patients and on-going communication with other professionals involved in the patient's care.
- Preparing and submitting bills to third party payers, or to the patient, and collections.
- Marketing or advertising products and services.
- Providing relevant information to patient caregivers.

- Returning patient phone calls.
- Training providing faculty, residents, professional students, graduate students and staff.
- Reporting adverse events or contagious diseases to the FDA or other public health authorities.
- Sending clinical files or portions of them to providers or others that the patient directs.
- Sending clinical files to attorneys involved in litigation.
- Communicating with school nurses regarding children's exams.
- Participating in managed care organization credentialing.
- Conducting clinical research.
- Writing articles for professional journals.
- Business planning and administrative management.

Who has access to information?

Patients have the right to access and obtain a copy of their medical or billing information. (Patients at our facilities have always had this right—unless prohibited by law.)

We must act upon a request within 30 days. As always has been the case in maintaining good patient relations, we expect to act on such requests as soon as possible.

Valid authorization for release of information must be in writing and contain the following items: (See policy entitled "DISCLOSURE OF PROTECTED HEALTH INFORMATION"*

- name and address of the patient
- name of the person or facility requesting the release of the patient's record
- name of the person or provider to whom the patient's health record is to be released
- purpose of the release
- specific and meaningful description of the information to be released from the health record
- signature of the patient or the signature of the patient's legal representative

- date on which the consent was signed
- statement of the individual's right to revoke the authorization
- date, event, or condition on which the consent will expire if not previously revoked

Authorization is NOT required for the following:

For payment reasons, including but not limited to:

- To the patient's health insurance in pursuit of payment
- To Billing/Auditing personnel with a need to know

For treatment reasons, including but not limited to:

- Emergency release via telephone for patient care
- Release to health care providers who are involved in the treatment of the patient and have a demonstrated need
- Direct patient transfer to other health care facilities
- Referrals within Salus for further evaluation or treatment
- Facilitate conversation for patients with limited English proficiency
- To spouses, friends, and family members if the provider can reasonably infer that the patient does not object and it is in the patient's best interest. (See policy entitled “PROVIDING INFORMATION TO FAMILY AND FRIENDS OF PATIENTS INVOLVED IN CARE.”

For operational reasons, including but not limited to:

- Research/audits by governmental agencies
- Peer review/OA review
- Accreditation Council on Optometric Education (ACOE) accreditation visits
- Risk Management

Authorization IS required to release information to the following:

- Attorneys not directly employed by Salus University (requests for records after accidents, etc.)

- Insurance companies (that are not part of the patient's bill at Salus)
- Life insurance
- Employers/employment agencies
- Armed forces
- Health care facilities—if not involved in the care of the patient
- Prisoners—cannot be released directly to a prisoner. Information may be released to the Medical Director or to the superintendent of the facility where the prisoner resides. The medical director or the superintendent may sign authorization.
- Residents of boy's/girl's school (same as for prisoner applies)
- Schools (authorization is accepted from program representative of school system in lieu of patient/parent/guardian)
- Physicians or Consultants not engaged or employed by Salus University staff unless we are referring the patient for care
- Social agencies
- Disability determination
- Workers' Compensation

The following disclosures ARE REQUIRED by law:

- Follow-up by child protective services/prosecutor's office when Salus has filed a request
- To avert a serious threat to health or safety
- To facilitate organ or tissue donation

Public health risks

- To prevent or control disease, injury, or disability
- To report any abuse or neglect of a patient
- To report reactions to medications or problems with products (FDA, etc.)
- To notify patients of a recall of a medication or product they may be using

- To notify a person who may have been exposed to a disease or at risk for contracting or spreading a disease or condition
- Health oversight activities (qualified state and federal surveyors with proper identification)
- National security and intelligence activities
- Law enforcement
- In response to a court order, subpoena, warrant, summons, or similar process
- To identify or locate a suspect, fugitive, material witness, or missing person
- About the victim of a crime if, under certain limited circumstances, we are unable to obtain the victim's agreement
- About criminal conduct at Salus
- In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description, or location of the person who committed the crime
- Medical information about foreign military personnel to the appropriate foreign military authority

Request for amendment to the record (by the patient)

An individual has the right to request an amendment to his/her designated record set (medical or billing records) for as long as Salus maintains the information. All requests for amendments must be made in writing and the school has 60 days to act (with possible 30-day extension).

Salus must:

- Notify the individual that the amendment was accepted
- Inform relevant persons identified by the individual

We can never delete the original information.

The amendment allows for the patient to supply a written supplement to his/her protected health information.

Denying a request for amendment

We may deny the patient's request for amendment if the information:

- Was not created by us (unless originator is no longer available). For example, if it is a medical report from another practitioner and the patient disagrees with that practitioner's information, we cannot change the medical record.

- Is not part of the patient's medical or billing records (information that is not relevant).

- If the record is not available for inspection. For example, if records are not kept beyond 7 years.

- Is accurate and complete. For example, if we have made a notation in the record that it is correct but the patient still wants it removed.

What steps do we take when we deny the request for amendment?

- We must provide timely, written notice of the denial to the individual.

The notice must explain the following:

- Reason for denial

- Right to submit written statement of disagreement or have request and denial included with future disclosures

- Individual's right to complain to us or directly to the government

- We may prepare a rebuttal statement to the individual's statement of disagreement; a copy of the rebuttal statement must be given to individual.

- We must include request and denial with future disclosures

Accounting of disclosures

Individuals have the right to request an "accounting of disclosures." The request must be made in writing.

The following disclosures of health information do not require tracking:

- Disclosures for treatment, payment and healthcare operations

- Disclosures made to the individual or authorized by the individual

- Disclosures made to persons involved in the individual's care

- Disclosures for national security or intelligence purposes

- Disclosures to correctional institutions or law enforcement

- Disclosures made prior to the date of compliance of the privacy standard

Right to request restrictions

An individual has the right to request restrictions to the use and disclosure of his/her protected health information. We are not required to allow the restrictions, but are required to permit the request. If Salus agrees to the restrictions, we may not make uses or disclosures that are inconsistent with the restrictions, unless the uses or disclosures are mandated by law.

The request for restrictions must be made in writing. Salus will document and retain the restriction for a period of at least 6 years from the date of its creation or the date it last was in effect, whichever is later.

Business associates

A "business associate" is a person or entity who is not a member of the Salus University workforce and who provides certain functions, activities, or services for us involving the use and/or disclosure of protected health information.

The business associate requirements do not apply to entities who disclose protected health information (PHI) to providers (such as physicians, pharmacists, and laboratories) for treatment purposes.

In order to comply with the Health Insurance Portability and Accountability Act (HIPAA), Salus University will maintain a copy of all non-employment contracts and business associate agreements.

Complaints

Patients have always had the right to complain to Salus University or any of our state, federal, or accrediting bodies, Under HIPAA, we have to tell patients that they can complain to us, Risk Management, or the Department of Health and Human Services Office of Civil Rights.

The following requirements must be met in order to file a complaint:

- A complaint must be filed in writing.
- The person must name the facility where the violation occurred and describe what happened.
- The complaint must be filed within 180 days of occurrence.

What is ePHI?

ePHI = Electronic Protected Health Information

- Patient demographic data (e.g., address, date of birth, date of death, sex, e-mail/Web address)
- Medical record number, account number, or SSN
- Dates of service (e.g., date of admission, discharge)
- Medical records, reports, test results, appointment dates

ePHI or electronic Protected Health Information is patient health information which is computer based (e.g., created, received, stored or maintained, processed and/or transmitted in electronic media). Electronic media includes computers, laptops, disks, memory sticks, PDAs, servers, networks, dial-modems, e-Mail, Websites, etc.

What are the information security standards for protection of ePHI?

- "Information Security" means to ensure the confidentiality, integrity, and availability of information through safeguards.
- "Confidentiality"--that information will not be disclosed to unauthorized individuals or processes.
- "Integrity"—the condition of data or information that has not been altered or destroyed in an unauthorized manner. Data from one system is consistently and accurately transferred to other systems.
- "Availability"—the property that data or information is accessible and useable upon demand by an authorized person.

What are the Federal Security Rule General Requirements? [45 CFR §164.308-a]

- Ensure the CIA (confidentiality, integrity and availability) of all electronic protected health information (ePHI) that the Salus creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI (e.g., hackers, virus, data back-ups).
- Protect against unauthorized disclosures.
- Train workforce members ("awareness of good computing practices").
- What are the consequences for security violations?
- Risk to integrity of confidential information (e.g., data corruption, destruction, unavailability of patient information in an emergency).
- Risk to security of personal information (e.g., identity theft).

- Loss of valuable business information.
- Loss of confidentiality, integrity, and availability of data (and time) due to poor or untested disaster data recovery plan.
- Embarrassment, bad publicity, media coverage, news reports.
- Loss of patients' trust, employee trust, and public trust.
- Costly reporting requirements.
- Internal disciplinary action(s), termination of employment.
- Penalties, prosecution, and potential for sanctions/lawsuits

DISCLOSURE OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, with certain exceptions, it is the policy of Salus to obtain a signed patient authorization before making a use or disclosure of protected health information. Salus requires a signed authorization prior to releasing Protected Health Information (PHI) other than for purposes of treatment, payment or operations, such as quality assurance or utilization review. Salus shall comply with applicable federal and state laws and regulations regarding the release of PHI for the prevention of serious harm to an individual.

1. Any request for the release of PHI must be accompanied by a written authorization signed by the patient before release of the PHI will be permitted, except under circumstances set forth in Salus' policy regarding disclosure of PHI without an authorization.

2. Staff members of Salus are required to obtain a copy of an authorization to release PHI in writing, which must be maintained in the patient's record.

3. Staff members may not rely on assurances from others that a proper authorization exists.

4. Facsimile or photostatic copies of the authorization are acceptable if reasonable attempts are made to certify the identity of the sender.

5. Salus is not required to disclose PHI precisely in accordance with an individual's authorization. In various cases, it may be burdensome to undertake the effort to review the record and select the portions relevant to the request (or to redact portions not relevant). In such circumstances, Salus may provide the entire record to the individual who may then redact and release the PHI as desired to the requester. The entire record may not be sent to anyone other than the individual who is the subject of the PHI.

6. Salus must document and retain all signed authorizations for six years from the date of its creation or the date when it last was in effect, whichever is later.

7. A named insured may sign a valid authorization for an individual if the named insured is a personal representative for the individual under applicable law.

8. To be a valid authorization under this policy, the authorization must be written in plain language, and must contain at least the following elements:

    a) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

    b) The name or other specific identification of the person(s), or class of person(s), authorized to make the requested use or disclosure;

    c) The name or other specific identification of the person(s), or class of persons, to whom the Salus may make the requested use or disclosure;

d) An expiration date or an expiration event that related to the individual or the purpose of the use or disclosure;

e) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

f) A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by law;

g) The signature of the individual and the date; and

h) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

DISCLOSURE OF PROTECTED HEALTH INFORMATION WITHOUT AN AUTHORIZATION

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to obtain a signed patient authorization before making a use or disclosure of protected health information, except in those circumstances in which HIPAA does not require such an authorization. As stated in HIPAA, we will not obtain a signed patient authorization in the following circumstances:

1. Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:

    a) Providing care to patients in our office

    b) Writing/sending, and filling prescriptions for drugs and eyewear, contact lenses or other prescriptive devices

    c) Preparing and submitting claims and bills

    d) Receiving/posting payments, and collection efforts

    e) Managed care credentialing

    f) Professional licensure and specialty board credentialing

    g) Quality assurance

    h) Financial audits/management

    i) Training of professional and non-professional staff, including students

    j) Office management

    k) Fraud and abuse prevention activities

2. Disclosures to business associates that have signed a business associate agreement.

3. Disclosures that are required by our state law, provided that we disclose only the precise protected health information required, and only to the recipient required.

4. Disclosures to applicable state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.

5. Disclosures to applicable local, state, or federal governmental agencies to report suspected child abuse, elder abuse or neglect.

6. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration ("FDA"), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.

7. Disclosures to applicable local, state, or federal governmental agencies in order to report suspected abuse, neglect, or domestic violence regarding adults, provided that we:

    a) Get an informal agreement from the patient unless:

    b) We are required by law to report our suspicions.

    c) We are permitted, but not required by law to disclose the protected health information, and we believe that a report is necessary to prevent harm to our patient or other potential victims.

    d) We tell the patient that we are making this disclosure, unless:

    e) Telling the patient would put the patient at risk for serious harm, or

    f) Someone else is acting on behalf of the patient and we think that this person is the abuser and that telling him or her would not be in the best interest of the patient.

8. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that we only disclose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.

9. Disclosures in response to a court order, provided that we disclose only the precise protected health information ordered, and only to the person ordered.

10. Disclosures to police or other law enforcement officers regarding a crime that we think happened at our office, provided that we reasonably believe that the protected health information is evidence of a crime.

11. Uses of protected health information to market or advertise our own health care products or services, or for any other marketing exception [see MARKETING AND ADVERTISING]

12. Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the protected health information only for purposes preparatory to research or to a researcher only using the protected health information of deceased patients, provided that the researcher gives us the assurances required by HIPAA.

13. If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described in paragraphs 1 through 13, we will obtain a signed patient authorization before making the use or disclosure.

PROVIDING INFORMATION TO FAMILY AND FRIENDS OF PATIENTS INVOLVED IN CARE

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to give patients a chance to agree or object to providing protected health information to close family or friends who are helping with the patient's care.

If we feel that it is necessary or appropriate to inform a close family member or friend who is involved in a patient's care about certain protected health information relevant to their involvement, we will give the patient a chance to agree or object to such disclosure before we make it. If the patient is present or available when this need arises, we will do any of the following:

- Get an oral agreement from the patient that the disclosure is acceptable.
- Give the patient a chance to object to the disclosure.
- Infer from the circumstances that the patient does not object. For example, we can reasonably infer that the patient does not object if the family member or friend is in the examining room with the patient.
- If the patient is not present or available when the need arises, we will use our best judgment about whether it is in the patient's best interest to disclose the information. An example might be when a family member or friend comes to our office to pick up eyewear that the patient previously ordered, as a convenience to the patient.

If we make a disclosure to a close family member or friend under the circumstances described in paragraph 1, we will only disclose information that is relevant to the family member or friend's involvement with the patient's care. Examples:

- If the patient's spouse will pick up ordered eyewear, we will provide the eyewear but not disclose any diagnoses or special features of the eyewear.
- If a son or daughter will assist a patient with eye drops, we will provide information about when and how the drops should be administered, but will not disclose the patient's diagnosis.

If someone claiming to be a family member or friend of the patient initiates contact with us seeking information, we will:

- Verify the identity of the caller and their relationship to the patient.
- Determine if they are involved in the patient's care.

- Determine if the patient is available (by phone, email, or other communications method) to either agree or object to the disclosure. If so, we will give the patient the chance to agree or object. If the patient objects, we will not disclose any information to the caller. If the patient is not available by any reasonable means, we will use our best judgment to determine whether disclosure of information is in the patient's best interest.

An individual has the right to request restrictions to the use and disclosure of his/her protected health information. If Salus agrees to the restrictions, we may not make uses or disclosures that are inconsistent with the restrictions, unless the uses or disclosures are mandated by law.

ELECTRONICALLY TRANSMITTING PROTECTED HEALTH INFORMATION

Sending Protected Health Information (PHI) by email exposes the PHI to two risks:

- The email could be sent to the wrong person, usually because of a typing mistake or selecting the wrong name in an auto-fill list.

- The email could be captured electronically en route.

HIPAA requires that we take reasonable steps to protect against these risks but acknowledges that a balance must be struck between the need to secure PHI and the need to ensure that clinicians can efficiently exchange important patient care information.

YOU MUST NEVER SEND OR RECEIVE EMAIL CONTAINING PHI FROM ANY DEVICE EXCEPT A SALUS-MANAGED COMPUTER OR A SALUS-MANAGED SMARTPHONE.

In addition, you must continue to observe the following rules:

- Limit the information you include in an email to the minimum necessary for your clinical purpose. [see MINIMUM NECESSARY STANDARD]

- Whenever possible, avoid transmitting highly sensitive PHI (for example, mental health, substance abuse, or HIV information) by email.

- Never send PHI by email unless you have verified the recipient's address (for example, from a directory or a previous email) and you have checked and double-checked that you have entered the address correctly.

- Always include a privacy statement notifying the recipient of the insecurity of email and providing a contact to whom a recipient can report a misdirected message.

Recommended Privacy statement: Please be aware that e-mail communication can be intercepted in transmission or misdirected. Please consider communicating any sensitive information by telephone, fax, or mail. The information contained in this message may be privileged and confidential. If you are NOT the intended recipient, please notify the sender immediately with a copy to compliance@salus.edu and destroy this message.

You may continue sending PHI by email from one salus.edu email address to another salus.edu email address so long as you follow the rules above.

You may exchange PHI by email outside the salus.edu network, so long as you follow the rules above AND so long as one of the circumstances below applies:

1. The email is being sent to a non-Salus clinician, research collaborator, or collaborating institution, AND it contains information urgently needed for patient care AND the patient identifiers are limited to name, date of birth, medical record number, or phone number, as needed.

OR

2. The email is being sent to a non-Salus clinician, research collaborator, or collaborating institution, AND it must be transmitted in a timely manner, AND it contains no direct identifiers (name, address, Social Security number, date of birth, phone/fax numbers, or patient email address) and no highly sensitive PHI (for example, mental health, substance abuse, or HIV-related information). Note: Less direct identifiers such as medical record number or initials (for example, "Mr. S") may be included.

OR

3. The patient or research subject has agreed to the use of email by completing a Consent for Email Communication form.

Please note that the circumstances set out above include different time elements. You may send PHI by email to non-Salus clinicians or collaborators (circumstances 1 or 2) only if the information must be communicated in an urgent or timely manner. There is no timeliness requirement attached to circumstances 3 or 4.

REMEMBER:

- These guidelines attempt to minimize the risk of a breach of privacy, but they do not eliminate that risk.
- Some divisions of the University may impose more restrictive limitations on email, and you must be familiar with those restrictions.
- If you discover that an email with PHI has been misdirected, you must immediately report it to the HIPAA Privacy Officer, at 215-276-6070, or the security incident hotline: 844-570-7233 (code – 791755).

MARKETING AND ADVERTISING

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to require a signed patient authorization to use or disclose protected health information for marketing or advertising purposes, unless not required by the HIPAA Privacy Rule.

Marketing means to make a communication that encourages the person receiving the communication to purchase a product or service. Generally, if the communication is "marketing", then the communication can occur only if Salus first obtains the individual's

authorization. Marketing also means "an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service. This part of the definition of marketing has no exceptions. If the marketing involves direct or indirect remuneration, the authorization must state that such remuneration is involved.

Communication is not "marketing" if:

1. It is made 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, Salus making the communication. For example, Salus would use the patient listing to announce the opening of a new Salus clinics and/or acquisition of improved equipment.

2. It is made for treatment of the individual. For example, prescription refills or referral to a specialist.

3. It is made for case management or care coordination for the individual, or direct or recommended alternative treatments, therapies, health care providers, or settings of care to the individual.

The three exceptions above must otherwise be permissible under the Privacy Rule, and a covered entity may us a business associate to make the communication.

The following addresses specific procedures at Salus:

1. If a marketing communication discloses protected health information, Salus always obtains a signed patient authorization. If it is determined that a communication is "marketing," obtain a signed HIPAA-compliant authorization from the individual prior to using or disclosing PHI for marketing purposes. Do not seek or obtain "blanket authorizations" for marketing. These are expressly prohibited under HIPAA.

Salus must obtain a signed authorization from the appropriate individual each time Salus wishes to use his/her PHI for a purpose other than described on a previously signed authorization. Retain signed authorization forms for six (6) years. Direct any questions regarding whether an activity is "marketing" to the Compliance Officer.

2. If we use protected health information in connection with a marketing communication, we will get a signed patient authorization, except for:

a) Marketing communications about our own health care products or services.

b) Communications made in the course of treatment, case management, or care coordination for an individual patient.

c) Communications made during a face-to-face encounter with a patient.

d) Communications consisting of distribution of promotional gifts of nominal value. We consider a gift to be of nominal value if the individual gift is worth less than $10 per item, and if we distribute less than $50 in gifts to any one patient per year.

e) Communications falling into these specified categories do not require a signed patient authorization.

3. When we need an authorization, we will include information about any money or other valuable thing that we get from someone else in connection with the communication. The Compliance Officer is responsible for obtaining signed patient authorizations for marketing, when they are required, and for making sure that the authorization discloses any money or thing of value that we get from someone else in connection with the marketing communication.

SALE OF PROTECTED HEALTH INFORMATION

POLICY:

Salus does not, and contractually requires that its Business Associates do not, directly or indirectly accept any remuneration in exchange for an Individual's PHI without first obtaining a valid HIPAA Authorization which includes a specific statement that remuneration will be received in connection with the use and disclosure of the Individual's PHI (Use Salus' "Authorization to Use and Disclose PHI With Remuneration");

EXCEPT that Salus or its Business Associate may, without having to first obtain a valid HIPAA-Authorization, directly or indirectly receive remuneration in connection with uses and disclosures of PHI for any of the following permitted purposes (for purposes of this HIPAA Privacy Policy, individually, each a "Permitted Purpose" and collectively, the "Permitted Purposes"):

- The purpose of the exchange is for Public Health Activities (45 CFR § 164.512(b));
- The purpose of the exchange is for Research (45 CFR §§ 164.501 and 164.512(i)), and the price charged reflects the costs of preparation and transmittal of the data for such purpose;
- The purpose of the exchange is for the Treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent PHI from inappropriate access, use, or disclosure;
- The purpose of the exchange is a Health Care Operation concerning the Sale, Transfer, Merger, or Consolidation of all or part of Salus with another Covered Entity, or an entity that following such activity will become a Salus, and due diligence related to such activity;
- The purpose of the exchange is for remuneration that is provided by Salus to a Business Associate for activities involving the exchange of PHI that the Business Associate undertakes on behalf of and at the specific request of Salus pursuant to a Business Associate Agreement;
- The purpose of the exchange is to provide an Individual with Access and a copy of the Individual's PHI (45 CFR § 164.524); or
- The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate as the exceptions provided above.

PROCEDURES:

If Salus, or its Business Associate, is to receive any money, either directly or indirectly, in connection with a specific use or disclosure of an Individual's PHI, determine whether such use and/or disclosure is a Permitted Purpose.

If the use or disclosure is a Permitted Purpose, no HIPAA Authorization is required.

If the use or disclosure is not any one of the Permitted Purposes, then obtain the Individual's written authorization for receipt of remuneration by using Salus' Authorization to Use and Disclose PHI With Remuneration form.

If a third party has presented a signed "HIPAA-compliant" Authorization from the Individual, review and confirm the validity of the document, which must include the following elements in accordance with HIPAA and the HITECH Act:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- The name or other specific identification of the person(s) or classes of persons, to whom Salus may make the requested use or disclosure;
- An expiration date or an expiration event that relates to the Individual or the purpose of the use or disclosure;
- A statement of the Individual's right to revoke the Authorization in writing and the exceptions to the right to revoke, together with a description of how the Individual may revoke the Authorization;
- A statement that information used or disclosed pursuant to the Authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule;
- Signature of the Individual and date;
- If the Authorization is signed by a personal representative of the Individual, a description of such representative's authority to act for the Individual;
- A statement that Salus will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the Individual's providing Authorization for the requested use or disclosure;
- A description of the purpose of the requested use or disclosure;
- A statement that the Individual may refuse to sign the Authorization; and

- A statement that the use or disclosure of the requested information will result in direct or indirect remuneration to Salus from a third party.

Provide a copy of the signed Authorization to the Individual.

MAINTAIN A COPY OF THE SIGNED AUTHORIZATION, OR AN ELECTRONIC COPY, FOR A PERIOD OF SIX (6) YEARS FROM THE DATE OF ITS CREATION, OR THE DATE WHEN IT WAS LAST IN EFFECT, WHICHEVER IS LATER IN THE PATIENT'S MEDICAL FILE.

DISCLOSURES FOR RESEARCH

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to obtain a signed patient authorization before using or disclosing protected health information for research purposes, unless the research satisfies one of HIPAA's exceptions to the need for authorization. In accordance with HIPAA's exceptions:

1. We will not obtain a signed patient authorization if a researcher has obtained, and presents to us, a proper waiver of authorization from an Institutional Review Board ("IRB") or Privacy Board. This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information, and the research could not practically be conducted if research participants; authorizations were required.

2. In order to be a proper waiver, the following criteria must be satisfied:

    a) We must have documentation that the IRB has determined that a waiver is appropriate because:

        i. The use or disclosure of protected health information during the research poses no more than minimal risk to the privacy of the research participants;

        ii. The protected health information is necessary for the research;

        iii. As a practical matter, the research could not proceed without a waiver.

    b) We must have documentation from the IRB specifying what protected health information can be used or disclosed as part of the waiver.

    c) We must have documentation that the IRB made all its determinations according to proper procedures.

    d) The documentation must be signed by the chair of the IRB. The documentation must include the name of the IRB and the date of its approval of a waiver.

3. The Compliance Officer is responsible for obtaining proper IRB waivers of authorization for research that we want to conduct without a signed patient authorization. The Compliance Officer will consult with the IRB to determine what information the IRB or Privacy Board wants in order to make its determinations. If an outside researcher wants to use protected health information about our patients, the Compliance Officer is responsible for reviewing all documents that the researcher presents in support of a waiver of authorization, to verify their sufficiency.

4. The Compliance Officer is responsible for any ongoing communication with an IRB that has granted a waiver of authorization, if any is needed.

5. We will rely upon the IRB's statement of the protected health information that is subject to the waiver as being the minimum amount of protected health information that is necessary for the research.

6. We will not obtain a signed patient authorization if a researcher gives us specific assurances that:

    a) The researcher wants to review or disclose protected health information solely to prepare a research protocol or take other steps in preparation for research. These might include checking a database to see if any patients are good candidates for the research.

    b) The researcher will not take any protected health information off-site from where it is held.

    c) The researcher needs the protected health information for research purposes.

7. The Compliance Officer is responsible for reviewing all assurances that an outside researcher may give us in support of a disclosure of protected health information. The Compliance Officer is also responsible for providing specific assurances whenever we want to obtain protected health information from someone else for activities preparatory to research.

8. We will not obtain a signed patient authorization if a researcher wants the protected health information in order to conduct research solely on deceased patients and provides specific assurances that:

    a) The researcher is asking for protected health information strictly to conduct research.

    b) The person identified in the protected health information is dead. The researcher should supply a death certificate.

    c) The researcher needs the PHI in order to perform research.

9. If a data use agreement has been completed with the Principal Investigator, a limited data set can be used and disclosed in connection with research, public health or healthcare operations. Limited data set is addressed under the applicable section.

Authorizations for Research

1. If an authorization is needed, the researcher is responsible for obtaining it to conduct the research. The Compliance Officer is responsible for reviewing all authorizations presented to us by outside researchers. The authorization will describe the information to be used or disclosed, the purpose of the disclosure, and specify the time period in which the authorization is in effect.

An individual may revoke their authorization for research. The researcher can continue to use to disclose PHI that was obtain prior to the time an individual revoked their authorization.

PERSONAL REPRESENTATIVES FOR PATIENTS

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to allow properly authorized personal representatives to stand in the shoes of a patient in order to exercise all the rights that the patient could exercise regarding the use and disclosure of protected health information and to give any required consent for a use or disclosure of protected health information.

Policy:

Salus treats personal representatives who have *legal authority* (hereinafter, a "Personal Representative") to act on behalf of an individual as if such Personal Representative were to have "stepped into the shoes" of the individual for purposes of access to and use of the individual's PHI relevant to such personal representation.

Procedures:

Prior to releasing PHI to a person claiming to be a Personal Representative, verify the person's authority as follows:

1. Request identification from the person to determine whether such person has authority to act as a personal representative on behalf of a Patient in making decisions related to health care (e.g., Court Order appointing Guardian; Power of Attorney etc.).

2. If the documentation is sufficient to ensure that the requesting individual is an authorized Personal Representative of the individual, treat such person as a Personal Representative, with respect to PHI relevant to the personal representation.

3. If the documentation is not sufficient to ensure that the requesting individual is an authorized Personal Representative of the individual, the PHI may not be released to the requesting individual unless a written Authorization from the individual has been obtained, or the disclosure may be permitted under the "Family Member, Relatives and Friends" policy and procedure.

Salus may not treat a person as a Personal Representative of an **unemancipated minor** if the minor has the authority to make decisions with respect to PHI pertaining to a health care service under State law. See policy and procedures governing "**Minors**".

Do **NOT** treat a person as the Personal Representative of the individual if there is reasonable belief that:

the individual has been or may be subjected to violence, abuse or neglect by such person; or

treating such person as the Personal Representative could endanger the individual and in the exercise of professional judgment, it is not in the best interest of the individual to treat the person as the individual's Personal Representative.

Contact and notify the Compliance Officer in the event a negative determination is made regarding the release of PHI, or the authority of the requesting individual to act as the Personal Representative is questionable.

1. Deceased adult patients

The personal representative of the estate of the deceased adult patient may provide consent/authorization regarding use or disclosure of the decedent's protected health information. [see DECEDENTS]

2. Before we work with someone claiming to be a personal representative, we will verify their legal authority to so act. This might include:

    a) checking a photo identification

    b) examining court orders, powers of attorney or other legal documents

If we are unsure of a person's authority to sign consents/authorizations permissions or exercise rights regarding protected health information of a patient, we will not use or disclose that protected health information until any such ambiguity is resolved.

NOTICE OF PRIVACY PRACTICES

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to:

1. Distribute a Notice of Privacy Practices to every patient at their first appointment.

    a) The Notice of Privacy Practices to use is attached to this Policy. Only the Compliance Officer has authority to change this Notice of Privacy Practices.

    b) The Patient Representatives at the Front Desk are responsible to distribute the Notice of Privacy Practices.

    c) The front desk Patient Representatives must ask the patient to sign an acknowledgement of receipt of the Notice of Privacy Practices. The acknowledgement of receipt is attached to this Policy. The signed acknowledgement of receipt is placed in the patient's medical record.

    d) If the patient chooses not to sign the acknowledgement of receipt, the front desk Patient Representatives must make a note of the fact that the patient was asked and that the patient refused. This note will be placed in the patient's medical record.

    e) It is not necessary to give a Notice of Privacy Practices to a patient every time they come in after September 23, 2013 unless we change the Notice of Privacy Practices.

    f) At every patient encounter, the front desk Patient Representatives must review the patient's medical record to determine if the patient has previously signed an acknowledgement of receipt (electronically maintained in the electronic health record).

    g) If yes, it is not necessary to give that patient another Notice of Privacy Practices unless we have changed our Notice of Privacy Practices since the date of the acknowledgement of receipt. Our most current Notice of Privacy Practices will always have an effective date on the front.

    h) If no, then it is necessary to distribute a Notice of Privacy Practices and ask for signature on an acknowledgement of receipt.

2. Copies of the Notice of Privacy Practices will be available at all Salus University clinics so that patients and visitors can take one, if they wish.

3. A Copy of the Notice of Privacy Practices shall also be posted on Salus' website and updated promptly upon any changes to the Notice of Privacy Practices.

4. Our Notice of Privacy Practices will be redistributed as above whenever we change it.

We will use and disclose protected health information in a manner that is consistent with HIPAA and with our Notice of Privacy Practices. If we change our Notice of Privacy Practices, the revised Notice of Privacy Practices will apply to all protected health information that we have, not just protected health information that we generate or obtain after we have changed the Notice of Privacy Practices.

PATIENTS' ACCESS TO THEIR PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to allow patients to inspect and/or obtain a copy of their own protected health information under the conditions stated in this policy. If the patient has a personal representative, the personal representative can inspect or request a copy of the patients protected health information on behalf of the patient.

1. We require that patients send a written request to inspect or obtain a copy of their protected health information. If a patient calls on the telephone asking to inspect or obtain a copy their protected health information, we will inform the patient of the requirement to send the request in writing.

2. Our appropriate clinic Director or Medical Records Manager is responsible for handling patient requests to inspect or request copies of their protected health information.

3. We will respond to a patient's request to inspect or obtain copies of their protected health information within 30 days of receiving the written request, or 60 days if the protected health information is stored off-site. If we need more time, we can have one 30 day extension, but we must notify the patient in writing of the extension before the original time period expires. Use the form letter, attached in Exhibit A.

4. We can deny the patient's request only for one or more of the following reasons:

A patient cannot inspect or obtain a copy of information if it was prepared in connection with a lawsuit.

A patient cannot inspect or obtain a copy of information if it is generated as part of the patient's participation in a clinical trial and the request is made during the clinical trial. We must have informed the patient about this restriction when the patient signed up for the clinical trial. The patient must be allowed to inspect or copy this information when the clinical trial is over.

A patient cannot inspect or obtain a copy of information if we got the information from someone else who is not a health care provider, and we promised that person that his/her identity would remain confidential.

A patient cannot inspect or obtain a copy of information if we, or another health care professional, determine that this would likely endanger the life or physical safety of the patient or someone else.

A patient cannot inspect or obtain a copy of if it references someone else, and we, or another health care professional, determine that access would likely cause substantial harm to such other person.

A patient's personal representative (for example, legal guardian, or parent of a minor) cannot inspect or obtain a copy of information about the patient if we, or another health care professional, determines that this would likely cause substantial harm to the patient or another person.

A patient cannot inspect or obtain a copy of information that is not in a designated record set.

5. We will afford each Patient the right of access to inspect and obtain a copy of his or her PHI, with the exception of the following:

    a) Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and

    b) Information maintained by us that is: (i) subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 262a, to the extent the provision of access would be prohibited by law; or (ii) exempt from the Clinical Laboratory Improvement Amendments of 1988, pursuant to 42 C.F.R. 493(a)(2).

If the appropriate clinic uses an electronic health record (EHRs) to create, maintain and use PHI, then:

    a) We will afford each Patient the right to obtain a copy of his or her PHI in an electronic format; and

    b) If the Patient requests it, we will transmit a copy of his or her PHI in electronic format directly to another entity or to a person designated by the Patient, provided that the Patient's request is clear, conspicuous, and specific.

6. If we deny a patient access to their protected health information, we will notify the patient of our decision.

7. If the denial is based upon reasons 4 d, e, or f, the patient has a right to a review of our decision.

    a) The Compliance Officer or Director of the Facility will handle the review.

    b) The Compliance Officer or Director of the Facility will look at the information that the patient wants to inspect or copy, and decide if we were correct in determining that the patient's circumstances meet the specifications of paragraph 4d, e, or f.

        i. If not, the patient may inspect or copy the information.

        ii. If so, the patient may not inspect or copy the information.

The patient may not further question our decision. Our notice to the patient will include instructions about how the patient may take advantage of this review right. We will use the denial notice letter accompanying this policy.

8. When we permit a patient to inspect or copy the requested information, we will:

a) Provide the information in the form or format that the patient requests, if we can reasonably produce it that way. If we cannot, we will either agree with the patient about another format or give it to the patient in hard copy.

b) Allow the patient to inspect or copy the information at our office during normal business hours. Within these limits, the patient can select the date and time to inspect or copy the records.

9. We will notify the patient that their request to access information is granted. We will use the access notice letter attached to this policy.

PROCEDURES:

If the Patient Appears In Person to Request PHI

1. Require the Patient to submit the request for access in writing, specifying the scope of information to which he/she wishes to have access or copies of (e.g., all information; billing information; information pertaining to a specific date of treatment).

Request at least one form of identification from the Patient, e.g., driver's license, birth certificate or passport.

Verify that all sources that may contain the requested PHI are checked. This includes PHI maintained solely on Salus' computer system and in Salus' business office. Salus shall attempt to provide the Patient with the requested PHI as soon as possible.

In the event Salus determines that it will take longer than 30 days to produce the requested information, the Compliance Officer shall be contacted immediately.

Salus may charge a per page copying fee provided that the fee is a reasonable, cost-based fee and provided that the fee includes only the cost of copying (including the cost of supplies and labor for copying) and postage when the Patient has requested the copy be mailed. Adhere to any additional restrictions under state law on caps for copy charges. Salus may charge an amount not greater than its labor costs in responding to a Patient's request for a copy of PHI (or a summary or explanation of such information) in an electronic format.

2. Patient Requests Information by Telephone or Fax

Requests for PHI from a Patient made by telephone or fax, provided that the request is made on an Authorization to Disclose PHI form, are acceptable.

Have the PHI available for pick-up by the Patient or representative of the Patient, or mail the information to the Patient at the address specified in the Authorization.

Advise the Patient that if someone other than the Patient is going to pick up the PHI from Salus, the person will need to provide proof of identity and authority for pick up.

3. Denial of Patient's Request for PHI

Requests for access may be denied if:

a) if the access requested is likely to endanger the life or physical safety of the individual or another person;

b) the PHI makes reference to another person, and it has been determined that the release of the information could lead to harm to that other person;

c) the request is made by a personal representative of the Patient, and it's been determined that permitting the access could cause harm to the Patient;

In addition, the following information may be excluded:

a) "Psychotherapy Notes";

b) Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and

c) Information maintained by Salus that is: (i) subject to the Clinical

Laboratory Improvements Amendments of 1988, 42 U.S.C. 262a, to the extent the provision of access would be prohibited by law; or (ii) exempt from the Clinical Laboratory Improvement Amendments of 1988, pursuant to 42 C.F.R. 493(a)(2).

If a Patient is denied access to PHI, Salus must:

a) Explain to the Patient why he/she is being denied;

b) Document the denial in the Patient's file; and

c) Allow the Patient the right to have the denial reviewed by a health care professional who is designated by Salus to act as the reviewing official and who did not participate in the original decision to deny the request.

AMENDMENT OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to permit patients to request us to amend their protected health information under the conditions stated in this policy. If the patient has a personal representative, the personal representative may exercise this right on behalf of the patient.

1. We require that all requests to amend protected health information be in writing. If a patient calls on the telephone to request an amendment, we will inform the patient of the requirement to submit this request in writing.

2. Our Compliance Officer is responsible for handling patient requests to amend their protected health information.

3. We will respond to requests for amendment within 60 days after we receive the written request. We can have one 30 day extension if we notify the patient that we need this additional time before the original time period expires. We will use the form letters attached to this policy in Exhibit B.

4. We can deny a requested amendment only for one or more of the following reasons:

   The information is accurate and complete as it is.

   We did not create the information.

   The information is not in a designated record set.

5. If we deny a request, we will notify the patient. We will inform the patient of the right to either submit a statement of disagreement or to have the original amendment request accompany the information. We will use the form denial letter attached to this policy.

6. If we grant the requested amendment, we will notify the patient. We will use the form amendment letter attached its policy. We will:

   Append or link the corrected information to the information that we are holding.

   Send the corrected information to anyone who we know has previously received the incorrect information.

   Send the correct information to anyone that the patient requests.

ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION

It is the policy of Salus to provide our patients, upon request, with an accounting of the disclosures that we have made of their protected health information during the six years preceding their request, subject to the terms and conditions stated in this policy.

1. We will provide an accounting of all of our disclosures of a patient's protected health information, except for the following:

   Disclosures for treatment, payment, or health care operations.

   Disclosures made with a signed patient authorization.

   Disclosures that are incident to other permitted disclosures.

   Disclosures to the patient personally

   Disclosures to family or friends involved in a patient's care.

   Disclosures of a limited data set.

   Disclosures made before April 14, 2003.

2. In order to be able to provide an accounting when a patient requests one, we will keep track of all disclosures that we make of our patient's protected health information, except for those disclosures listed in paragraph 1. Only the Compliance Officer is authorized to make a disclosure of protected health information that is not listed in paragraph 1. The Compliance Officer will document all these disclosures in a separate file. We will keep this documentation for six years. This documentation will include:

   The date of the disclosure

   The name and address (if known) of the person or organization that got the protected health information

   A description of the protected health information that was disclosed

   A statement of the purpose or basis for the disclosure, or a copy of any request for the protected health information that prompted the disclosure.

3. We require that all requests for an accounting be in writing. If a request is made by telephone, we will advise the caller to submit it in writing to the Compliance Officer.

4. We will respond to a request for an accounting within 60 days from our receipt of the written request. If we are unable to provide the accounting within this 60 day period, we may have an additional 30 days, provided that we notify the patient of this delay before the original 60 day period expires. This notice must include the reason for the delay and the date that we will have the accounting ready. We will use the letter accompanying this policy in Exhibit C to

inform patients of a needed delay. The Compliance Officer is responsible for advising patients of delays.

5. Our accounting will list all of the information described in paragraph 2 of this policy. We will use the template accompanying this policy to make our accounting. If we make repeated disclosures of protected health information about a patient to the same person or organization for the same purpose, our accounting will provide all of this information for the first such disclosure, and then indicate the frequency or periodicity of the other disclosures, and the date of the last such disclosure. The Compliance Officer is responsible for generating requested accountings and furnishing them to the patient.

6. We will provide patients with one free accounting, upon request, within any 12 month period. For additional accountings within any 12 month period, we will charge $50.00 for the actual cost of preparing and mailing the accounting. We will require payment of this amount in advance, before we prepare and furnish the accounting.

7. Accounting for Electronic Health Record Disclosures

   Starting on January 1, 2014, Salus shall afford each Individual the right to receive an accounting of disclosures of PHI through an EHR made by Salus, covering a period of three (3) years preceding the request.

RESTRICTIONS ON USE OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to permit patients to request that we restrict the way that we use some protected health information for purposes of treatment, payment, or health care operations.

1. Our Compliance Officer will handle requests from patients for restrictions on the way we use protected health information for treatment, payment, or health care operations.

2. Generally, except as required by law, we will not agree to restrictions requested by patients. In unusual circumstances that the Compliance Officer thinks are meritorious, we may agree to a requested restriction.

3. Salus shall grant requests for restrictions of disclosures to health plans for purposes of carrying out payment or health care operations, and not for purposes of carrying out treatment, when the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

4. If we agree to a requested restriction, the Compliance Officer will document its terms and put this documentation as part of the patient's electronic demographic information. The Compliance Officer will communicate the terms of the restriction to all of our staff that need to know about it. If one or more of our business associates need to know about it as well, the Compliance Officer will inform them.

5. We will honor any restriction that we have agreed to. However, no restriction can prevent us from using any protected health information in an emergency treatment situation.

6. If we have agreed to a restriction but can no longer practically honor it, our Compliance Officer will do either of the following things:

Contact the patient to work out a mutually agreeable termination of the restriction. Our Compliance Officer will document this agreement, and keep it in as part of the patient's electronic demographic information.

Contact the patient and advise that we are no longer able to honor the restriction that we previously agreed to. This notice will only apply to protected health information that we obtain or generate after the notice is given.

CONFIDENTIAL COMMUNICATION METHODS WITH PATIENTS

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to accommodate requests from patients to send protected health information to them in a confidential way, subject to the conditions in this policy.

1. If a patient requests that we use a particular method to communicate with them in order to preserve the confidentiality of their information, we will accommodate that if we reasonably can. We can accommodate the following kinds of confidential communication methods:

   Mail

   Telephone

   Fax

   Email [see ELECTRONICALLY TRANSMITTING PROTECTED HEALTHCARE INFORMATION]

2. We require that such requests be in writing. If a request is received via telephone, the patient is to be directed on how to do the request in writing.

3. We will not ask or require a patient to explain why they want the particular communication method.

4. We will charge the patient the reasonable cost of complying with their request, if any.

5. Our Compliance Officer is responsible for receiving and acting upon patient requests for confidential communication methods

MINIMUM NECESSARY USES AND DISCLOSURES OF PHI

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to only use or disclose the minimum amount of protected health information necessary to accomplish the purpose for the use or disclosure, under the conditions and exceptions described in this policy.

1. People in the following job categories will only have access to the kind or amount of protected health information indicated:

   Attending providers, residents, students, and Opthalmic Technicians — any and all protected health information, including the entire medical record for treatment purposes of patients to whom that are providing treatment.

   Billers — basic demographic information found on office management software demographic screen, financial information and patient medical record only to process unpaid claims. Billers will only review that portion of the record that is necessary to process the unpaid claim.

   Front desk staff basic demographic information found on office management software demographic screen, entire medical record for chart preparation, patient ledger. Front desk staff will only review that portion of the record that is necessary to process the most current patient office visit.

   Dispensary staff — basic demographic information found on office management software demographic screen, patient medical record for information about diagnosis and spectacle prescription. Dispensary staff will only review that portion of the record that is necessary to process spectacle ordering.

   Department Manager — entire contents of patient medical record, including financial data.

   Business and Fiscal Operations Specialist — entire contents of patient medical record, including financial data

   Administrative Assistant — basic demographic information found on office management software demographic screen, patient schedule

   Department Assistant for Finances — basic demographic information found on office management software demographic screen, medical diagnosis and prescription. Department Assistant will only review that portion of the record that is necessary to process this information.

2. We will keep all medical records and billing records secure when they are not in use. Only authorized staff will have access to this secure storage location. We require that all computers be turned off when the user is away from their workstation. All staff are prohibited from browsing at someone else's workstation or using their computer password. Attending providers, students and staff are prohibited from talking about patients in public areas.

3. All attending providers, students and staff will sign a ""Corporate Compliance Program Awareness Certification Form" indicating their commitment to access only the minimum amount of protected health information necessary for them to do their job, and to abide by the restrictions listed above. Violation of this agreement is grounds for employment discipline in accordance with University policies.

4. Whenever we get a request from a third party for protected health information about one of our patients, or whenever we intend to make a unilateral disclosure of protected health information about one of our patients, we will disclose only the minimum necessary amount of protected health information necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:

   The patient has authorized the disclosure.

   The disclosure is for treatment purposes (for example, disclosures to a consultant or follow-up health care provider).

5. We will disclose only the indicated protected health information in response to the following routine kinds of disclosures that we make:

   billing

   further treatment, diagnosis and evaluation

6. We will rely upon the representations of the following third parties that they have requested only the minimum amount of protected health information necessary for their purposes:

   Another health care provider or health plan.

   A public official, like a law enforcement officer.

   Professionals providing services to us (such as attorneys or accountants).

   Researchers supplying documentation of IRB waivers.

7. The Compliance Officer is responsible for determining what the minimum amount of protected health information is necessary for us to disclose in situations that are not routine. The Compliance Officer will consider the reason for the disclosure, whether it falls into any of the circumstances described in paragraph 4 of this policy, and the protected health information that we have, in making this determination.

8. Whenever we request protected health information about one of our patients from someone else, we will ask for only the minimum necessary amount of protected health information necessary for us to accomplish the purpose that prompted us to ask for the information.

PROCEDURE:

To the extent practicable, with respect to the use, disclosure, or request of PHI, Salus shall limit the PHI used, disclosed or released to either:

the Limited Data Set for such PHI, which shall exclude the following direct identifying information of the Individual or of relatives, employers, or household members of the Individual:

1. Names;
2. Postal address information;
3. Telephone numbers;
4. Fax numbers;
5. Electronic e-mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images;

OR

the Minimum Necessary amount of PHI to accomplish the intended purpose of the use, disclosure, or request. Salus or, where applicable, the Business Associate of Salus, shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

If any request for, or use of PHI by, another person appears to be not warranted or is excessive, the concerned employee may consult with the requester or the Individual to determine whether the scope of the request is accurate.

In the event Salus cannot resolve the issue informally, the requested information will not be disclosed until the Compliance Officer is consulted for further direction.

VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to verify the authority and identity of people or organizations that request us to disclose protected health information about our patients, subject to the conditions of this policy statement.

1. If a patient has a personal representative who seeks to sign an authorization to disclose the patient's protected health information to a third party, or to exercise any of the rights that patients have regarding their protected health information, we will take the following steps before we accept their signature or allow them to exercise those rights:

   Ask for copies of any documents that are relevant to their status as personal representative. For example, we will ask for a copy of the court papers appointing a legal guardian, or a power of attorney designating someone to make health related decisions for an incapacitated adult.

   We will ask for a picture identification of the person serving as personal representative.

2. We will review all documents that we receive and make sure that they in fact authorize the personal representative to control the patient's protected health information, and that there are no limits or expiration dates that affect this authority. The Facility Director is responsible for reviewing documents. If there are questions about the documents, the Director will work with the Compliance Officer to resolve them. We will not disclose any protected health information until all questions are answered and we have proper evidence of the authority of the person acting as personal representative.

3. If we receive a request from a third party to see or have a copy of protected health information that we have about our patients without a signed patient authorization, we will take the following steps before we allow such access:

   Ask the requestor for evidence that they are affiliated with an organization or government agency that is authorized to have access to protected health information without an authorization. Evidence can include an official badge or identification card, an assignment on official letterhead, or similar items.

   Ask the requestor for picture identification.

   Ask the requestor to specify the legal authority that the requestor believes allows access to protected health information.

   For example, if we are asked by a representative of a drug or medical device manufacturer to supply protected health information relating to our use of a particular drug or device, we will make sure that the representative is truly affiliated with the drug or device manufacturer; that the drug or medical device manufacturer is under the jurisdiction of the U.S. Food and Drug Administration; and that the drug or device manufacturer is seeking the information because of a quality or safety concern about a product that they manufacture as provided in 45 CFR 164.512.

4. We will review all evidence supplied by the requestor to make sure that the requestor has proper authority to access protected health information, and that there are no limits or expiration dates that affect this authority. The Compliance Officer is responsible for this review. We will not disclose any protected health information about our patients until all questions have been resolved and we are sure that the requestor has proper authority to access the protected health information.

MITIGATION OF KNOWN HARM FROM AN IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to mitigate known harm from an improper disclosure of protected health information, when it is practicable to do so.

1. Whenever we learn of harm caused by an improper disclosure of our protected health information, we will take reasonable steps to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our business associates.

2. Our Compliance Officer will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm. Examples of some mitigation steps

   Getting back protected health information that was improperly disclosed.

   Preventing further disclosure through agreements with the recipient.

3. We do not consider money reparations to be appropriate mitigation.

4. If a business associate has made the improper disclosure, we will require the business associate to cure the problem to our satisfaction, or terminate the relationship with the business associate.

PROCEDURE

If an improper use/disclosure of PHI in violation of HIPAA and/or Salus' Privacy Policies & Procedures is discovered; or Salus is advised of a violation of HIPAA or its Privacy Policies & Procedures by either Salus or a Business Associate:

1. Take reasonable efforts to halt the improper use and/or disclosure, mitigate any harmful effects of the use and/or disclosure; and

2. Contact the Compliance Officer immediately to determine appropriate steps.

   In the event the improper use/disclosure or violation is isolated, the Compliance Officer shall monitor remediation and refer any individual involved for re-training on the specific issue leading to the improper disclosure.

   In the event the improper use/disclosure or violations appears to be widespread, the Compliance Officer shall document the event, re-evaluate safeguards for gaps and make changes, with the approval of the Board, as needed, and monitor remediation activities.

HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS

In order to comply with HIPAA's Privacy Rule, it is the policy of Salus to accept complaints from patients, who believe that we have not properly respected their privacy, and to thoroughly investigate and resolve them.

1. Our Compliance Officer is responsible for accepting all patient complaints about alleged privacy violations. We require all complaints to be in writing. If a complaint comes over the telephone, the Compliance Officer will inform the patient to send it in writing. This can be hard copy or electronic, as the patient wishes. If a patient wishes to remain anonymous, we will accommodate that to the extent practical.

2. The Compliance Officer will keep all patient complaints for at least six years. These will be stored, along with information about the investigation and resolution of the complaint, in a log kept in the Compliance Officer’s office.

3. Upon receiving a patient complaint about privacy, the Compliance Officer will investigate it. The Compliance Officer has discretion to conduct the investigation in the manner considered reasonable and logical in light of the nature of the complaint. Generally, the Compliance Officer will do at least the following in order to investigate a complaint:

   Talk to the person in the office whom the patient thinks violated the patient's privacy.

   Review the patient's clinical chart.

   Talk to other office staff about the patient's concern.

   Talk to the patient.

   Review any information or evidence that the patient presents in support of the claim of a violation of privacy.

4. Based upon the results of the investigation, the Compliance Officer will determine if the patient's complaint is substantiated or not. If the complaint is not substantiated, the Compliance Officer will notify the patient in writing. If it is substantiated, the Compliance Officer will determine what steps are necessary to resolve the issue so that it does not recur.

5. In determining what steps are necessary to resolve a substantiated complaint of a violation of privacy, the Compliance Officer will consider at least the following points:

   What caused the privacy violation?

   If the violation was caused by a failure to comply with existing policy, the Compliance Officer will report the issue for action as a human resources disciplinary matter.

   If the problem was caused by a lack of an appropriate policy, or an inadequate policy, the Compliance Officer will determine how the policy should be changed, or if a policy needs to

be developed. If policy revisions or new policies are needed, the Compliance Officer will work with the Facility Director(s) to accomplish that.

If a business associate was involved in the violation, what must the business associate do to prevent the violation from recurring? If the business associate cannot cure the breach, the business associate contract must be terminated. The Compliance Officer will obtain approval from management before any business associate contracts are terminated.

If the privacy violation caused harm, what steps are necessary to mitigate that harm? The Compliance Officer will consult with counsel to accomplish the steps.

6. Once a resolution of a complaint is determined, the Compliance Officer will work to take the steps identified as necessary for the resolution.

7. If new policies or procedures are put into place as part of the resolution, the Compliance Officer will conduct mandatory training for our workforce regarding them.

8. The Compliance Officer will develop a way to monitor whether the resolution is working to improve our privacy protections. The Compliance Officer will report to the Board on the results of the monitoring. If the Compliance Officer discovers continued problems through monitoring, the Compliance Officer will work to fix the problems.

Privacy Investigation and Log.

The Compliance Officer shall document, adequately investigate (or oversee the investigation of), and, in accordance with the direction of the Board, appropriately respond to, each in-person complaint, telephone call or voice message, and written correspondence, report form, or e-mail message concerning privacy matters. The Compliance Officer shall maintain a Log book which documents the following items in connection with Privacy matter inquiry:

1. Sequential file identification number;

2. Date of report of potential non-compliance or wrongdoing is received;

3. Whether the reporter has identified himself or herself and has been advised of the file identification number;

4. Whether the reporter has brought the matter to the attention of his or her immediate supervisor (and if not, why not);

5. Description of the incident;

6. Identification of person designated as being primarily responsible for investigating the incident, and identification of any outside counsel or external consultants retained to assist in evaluation and investigation of the incident;

7. Current status of the investigation, as periodically updated; and

8. Date matter is resolved and type of resolution, including corrective action taken, where appropriate.

A copy of the form that will be used by the Compliance Officer to document the reports is attached. Document the complaint and resolution and maintain in a secure location for a period of at least six (6) years.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

It is the policy of Salus to use de-identified information instead of protected health information whenever this is feasible. None of HIPAA's Privacy Rules restrictions on the use and disclosure of protected health information apply to de-identified information, which can be used or disclosed freely.

1. The Compliance Officer is responsible for determining the feasibility of de-identifying any protected health information that we have about our patients, and for performing such de-identification if it is feasible.

2. If we de-identify protected health information, we will use HIPAA's "safe harbor" method of eliminating all specified identifiers. We will remove all the identifiers with respect to our patient, the patient's relatives, the patient's household members, and the patient's employer. The identifiers that we will remove are the following:

   Names

   All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

   Telephone numbers

   Fax numbers

   Electronic mail addresses

   Social security numbers

   Medical record numbers

   Health plan beneficiary numbers

   Account numbers

   Certificate/license numbers

   Vehicle identifiers and serial numbers, including license plate numbers

   Device identifiers and serial numbers

   Web Universal Resource Locators (URLs)

   Internet Protocol (IP) address numbers

   Biometric identifiers, including finger and voice prints

Full face photographic images and any comparable images

Any other unique identifying number, characteristic, or code.

3. Even after we have removed all the identifiers listed in paragraph 2, we will not consider information to be de-identified unless we have no actual knowledge that the remaining information can be used, either alone or in combination with other reasonably available information, to identify a patient.

4. If we disclose de-identified information, we will not disclose any key that we have to re-identify the information.

LIMITED DATA SETS

It is the policy of Salus to use a limited data set for certain disclosures of protected health information, whenever this is appropriate and feasible.

1. We will only use a limited data set for disclosures that are for research, public health purposes, or health care operations.

2. A limited data set is protected health information from which all of the following identifiers have been removed:

   Names

   Postal address information, other than town or city, State, and zip code

   Telephone numbers

   Fax numbers

   Electronic mail addresses

   Social security numbers

   Medical record numbers

   Health plan beneficiary numbers

   Account numbers

   Certificate/license numbers

   Vehicle identifiers and serial numbers, including license plate numbers

   Device identifiers and serial numbers

   Web Universal Resource Locators (URLs)

   Internet Protocol (IP) address numbers

   Biometric identifiers, including finger and voice prints

   Full face photographic images and any comparable images.

   In order to consider protected health information to be a limited data set, we will remove all of these identifiers about our patient, the patient's relatives, members of the patient's household, and the patient's employer.

3. The Compliance Officer is responsible for determining whether it is feasible and practical for us to disclose a limited data set, and if so, to create it.

4. Whenever we disclose a limited data set, we will require the recipient to enter into a data use agreement with us. The data use agreement restricts the ways in which the recipient can use the limited data set. We will use a master data use agreement.

MINORS

Policy:

It is Salus' policy to treat a parent, guardian, or other person in "loco parentis" (in the position or place of a parent) with authority under local law to make health care decisions about an unemancipated minor as a minor's personal representative, ***except*** **Salus shall treat the unemancipated minor as the Individual in the following circumstances:**

When a **parent consents** to such independence,

When applicable **Pennsylvania Law permits** the minor to **exercise independent consent**, or

When **Pennsylvania Law permits** a **third party**, such as a court, **to grant consent** on the minor's behalf and does so.

In these cases, Salus shall treat the minor, and not the personal representative, as the Individual who may exercise his or her rights under Salus' HIPAA Procedures.

PROCEDURE:

In cases where the patient is a minor, Salus must first determine whether the minor, parent, or other personal representative must be treated as the Individual for the purpose of each of Salus' HIPAA Procedures.

In Pennsylvania, a minor is an individual under the age of 21. An unemancipated minor is a minor who has not exercised his or her right to independence from parental authority.

Salus shall treat the minor as the Individual if: (1) the parent has consented to a minor's independence, or (2) any other third party permitted under Pennsylvania law to grant consent on the minor's behalf has done so. A court of law is one type of "third party" that may grant a minor the right to independence from parental authority.

Salus must also treat the minor as the Individual if the minor is receiving services relating to:

1. **Prenatal Care**. 35 Pa. Stat. §§ 10102 and 10103.

2. **A Sexually Transmitted Disease**, including HIV/AIDS. 25 Pa. Stat. § 521.14a; Pa. Code § 27.97.

3. **Alcohol or Drug Abuse Treatment**. 71 Pa. Stat. § 1690.112. (Note: *that a physician is statutorily provided with the discretionary authority to notify parents of such treatment*.)

4. **Mental Health Treatment**, if the minor is 14 years or older. 50 Pa. Stat. § 7201. (Note: *that a physician is statutorily required to notify parents that a minor is receiving such services if minor is under* 18. 50 Pa. Stat. § 7204.)

5. **General Medical Health Services**, if the minor (1) is over 18, (2) has graduated from high school, (3) has married or (4) has been pregnant. 35 Pa. Stat. § 10101.

6. **Emergency Situations**. 25 Pa. Stat. § 10104.

In all other cases, Salus will treat the minor's parent or personal representative as the Individual with respect to Salus' HIPAA Policies and Procedures.

Salus must document all requests for Individual Information under this Procedure, the actions taken to determine whether the disclosure could be made, Salus' decision regarding the request and, if a disclosure was made, a description in the log in accordance with Salus' Accounting of Disclosures.

SECURITY BREACH NOTIFICATION

Topic: ***Compliance with Security Breach Notification Laws***

POLICY:

Salus strives to comply with both federal and state law regarding security breach notification requirements applicable to a "Security Breach" of "Protected Health Information" (PHI) or "Personal Information" (PI), as such terms are defined under the applicable laws. Specifically, in the event of a Security Breach of PHI and/or PI, Salus follows the applicable standards of:

1. The HITECH Act, and specifically §13402 (the "Breach Statute");

2. HHS Final Rule for Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164) (the "Breach Notification Rule");

(collectively, the "**Security Breach Notification Laws**").

Salus will develop, implement, maintain and update, as necessary, security breach notification procedures in accordance with the Security Breach Notification Laws to:

(a) ***Detect*** potential and actual Security Breaches;

Investigate and ***Evaluate*** potential and actual Security Breaches;

Respond to a Security Breach by furnishing the required notices; and

Correct and Prevent subsequent similar or dissimilar incidents.

Unless otherwise specified, definitions assigned to terms in the Security Breach Notification Laws shall also be ascribed to such terms as they may be used for purposes of these Security Breach Notification policies and procedures.

SECURITY BREACH NOTIFICATION

Topic: ***Security Awareness & Training***

1. POLICY

Salus provides periodic and annual security awareness & training to its workforce members. Salus shall ensure all workforce members are appropriately trained in their responsibilities under the HIPAA Security Policies as well as Privacy Policies with respect to electronic PHI.

2. PROCEDURES

The Compliance Officer shall be responsible for developing, implementing and updating as necessary training resources and materials to educate workforce members on the requirements of the HIPAA Security Rule and the HIPAA Policies and Procedures.

Security awareness and training shall include at a minimum;

i. *Security Reminders.* The Compliance Officer shall ensure that periodic security reminders are provided to all workforce members as reasonable and appropriate to correct ongoing security concerns, threats, vulnerabilities or violations concerning the confidentiality, integrity and availability of PHI.

ii. *Password Management.* The Compliance Officer shall ensure that workforce members are educated on appropriate password creation, maintenance and confidentiality, including selecting "strong passwords", not sharing passwords with any workforce member or other individual, and not writing down passwords.

iii. *Protection from Malicious Software.* The Compliance Officer shall ensure that workforce members are educated in applications and mechanisms for safeguarding Information Systems and PHI from malicious software including but not limited running periodic security scans and not downloading files from untrustworthy sources.

iv. *Log-in Monitoring.* The Compliance Officer shall ensure that workforce members are educated on Salus' processes for monitoring all log-ins and log-in attempts, procedures for temporary suspending access after failed log-in attempts, and procedures required to re-activate access after failed log-in attempts. The Compliance Officer shall ensure that log-in monitoring processes are appropriate to monitor log-ins to all Information Systtems with PHI.

v. *Mobile Devices*. The Compliance Officer shall ensure that workforce members are appropriately educated on the privacy and security risks associated with mobile devices and other portable media through which PHI may be created, maintained, accessed or transmitted. **Salus shall consult guidance made available by the Office for Civil Rights in creating training and educational materials for workforce members.**

http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

SECURITY BREACH NOTIFICATION

Topic: ***Security Incident Procedures***

1. POLICY

Salus treats HIPAA Security Incidents with the highest concern and regard and shall take action to identify and address any potential or actual security incidents as soon as reasonably possible. Salus shall develop, implement, maintain and update these Security Incident procedures as may be reasonably necessary in order for Salus to identify and respond appropriately to Security Incidents. Salus takes such steps as reasonable and necessary to:

Detect and Identify potential and actual Security Incidents;

Investigate and *Evaluate* potential and actual Security Incidents;

Respond to the Security Incidents as reasonable and appropriate;

Mitigate any harmful effects from the Security Incidents, to the extent reasonably practicable; and

Correct and Prevent subsequent similar or dissimilar Security Incidents.

2. PROCEDURES

Detection and Identification.

i. All employees, agents or vendors of Salus must report any potential/suspected or actual/known Security Incident to the Compliance Officer as soon as possible and without delay. A Security Incident may include *attempts or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in Salus' information systems*.

ii. Business Associates (BAs) shall be required to **report** discovery of any suspected or actual Security Incidents as soon as reasonably practicable. Security Incidents that are Security Breaches, and potential Security Breaches must be responded to Salus as soon as reasonably practicable, but in any case within **fourteen (14) business days** following the BA's becoming aware of, or the actual or constructive delivery of notice of, the Security Incident by the Business Associate or its employees, agents, or other workforce members.

iii. Salus shall periodically audit all systems containing electronic PHI for evidence of unauthorized accesses, uses and other Security Incidents. Monitor all locations from which electronic PHI may be accessed (e.g., computer workstations).

iv. Salus shall periodically evaluate all systems, policies and procedures to identify any security gaps or improper practices and procedures and take such reasonable steps as may be necessary to improve, modify or

otherwise respond to such identified security gaps or practices and prevent the occurrence or re-occurrence of Security Incidents.

Investigation and Evaluation.

i. Salus shall investigate all reported potential and actual Security Incidents. The Compliance Officer shall investigate, gather and document all information relating to the facts and circumstances of a Security Incident.

ii. Salus shall document all pertinent information gathered during any Security Incident investigation, including but not limited to any determinations that a Breach did not occur or that there was no reasonable possibility of misuse.

iii. Salus shall promptly evaluate all reported incidents to determine whether a given Security Incident rises to the level of a Security Breach. *(Conduct **Breach Risk Assessment** to determine whether a Security Incident rises to the level of a Security Breach requiring the provision of notice to affected individuals and entities.)*

iv. Salus shall document and retain all of the information obtained through investigation and evaluation concerning a Security Incident or Breach for a period of six (6) years.

Response.

i. Salus shall respond to any Security Incidents as identified by investigation and evaluation as reasonably appropriate and necessary, including but not limited to corrective and mitigating action as necessary and implementing sanctions against violating employees.

ii. Salus shall respond to any Security Incidents that are reasonably believed to be a Security Breach in accordance with Salus' Security Breach Notification & Mitigation Of Improper Disclosures Policy and Procedures, including but not limited to providing notice of the Security Breach to affected individuals and entities.

iii. Correction, Mitigation and Prevention. Salus shall take reasonably necessary steps to mitigate the harmful effects, as far as reasonably practicable of any Security Incident and/or Breach, including evaluative, disciplinary, and other corrective action as may be appropriate to decrease the risk of harm and/or prevent re-occurrence of the Security Incident and/or Breach, and implementing additional or modifying processes and procedures as may be reasonably necessary to address identified security gaps

SECURITY BREACH NOTIFICATION

Topic: ***Security Breach Detection. Investigation, Notification & Mitigation of Improper Disclosures***

1. POLICY

Salus strives to comply with federal and state law regarding security breach notification requirements applicable to a "Security Breach" of "Protected Health Information" (PHI) or "Personal Information" (PI) as such terms are defined under the applicable laws. Specifically, in the event of a Security Breach of PHI and/or PI, Salus follows the applicable standards of:

i. HIPAA, as amended by the HITECH Act, and specifically §13402 (the "Breach Statute");

ii. HHS Final Rule for Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164) (the "Breach Notification Rule");

(collectively, the "Security Breach Notification Laws").

2. PROCEDURES

Detection and Internal Reporting.

i. Salus shall strive to detect potential or actual Security Breaches. Any employee, agent or other Salus vendor who obtains information or has reason to believe that a Security Breach has or may have potentially occurred and involves PHI or PI created or maintained by Salus is expected to report such information to a supervisor or, if needed, directly to Salus' Compliance Officer.

ii. Systems should be audited for evidence of Security Breaches. Work with Information Technology (IT) consultants or vendors in order to develop IT solutions for appropriate detection of security breaches within Salus' systems.

iii. Business Associates (BAs) shall be required to report (and require their subcontractors to report) discovery of any Security Breaches (or potential Security Breaches) as soon as reasonably practicable but in any case within **fourteen (14) business days** from the constructive or actual discovery of the Security Breach by the BA, BAs employees, agents or other workforce members and subcontractors.

iv. Initial and periodic training of employees and agents shall be completed as reasonably necessary in accordance with Salus' Compliance Program.

Investigating and Evaluating. Salus shall investigate and evaluate any and all reports of Security Incidents and/or Breaches, and conduct a Risk Assessment. The Compliance Officer shall be involved in assessing whether or not a Security Incident is a Security Breach within the meaning of the Security Breach Notification Laws. *(Utilize* **Security Breach Risk of Harm Assessment with Breach Log** *to determine whether a Security Incident rises to the level of a Security Breach*

requiring the provision of notice to affected individuals and other entities under HIPAA/HITECH and/or State law.)

Risk Assessment. **Start with a presumption that an impermissible use or disclosure of PHI is a reportable Breach for purposes of HIPAA and HITECH.** Conduct a **Risk Assessment** to determine whether the impermissible use or disclosure resulted in a **"low probability that the PHI was compromised"**. If Salus determines that there is a low probability that the PHI was compromised as a result of the impermissible use or disclosure, Salus may conclude that a Breach did not occur requiring notice as set forth in this Policy. **Consider and assess the following factors when conducting a Risk Assessment:**

i. **The Nature and Extent of the PHI.** For this factor, consider the *type* of PHI involved such as if the PHI was of a more "sensitive" nature. An example is if credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud are involved, then this would ***cut against*** finding that there is "low probability" that the PHI was compromised. With respect to clinical information, consider things like the *nature of the services*, as well as the *amount* of information and *details* involved. "Sensitive" information is not just things like STDS, mental health or substance abuse.

ii. **The Unauthorized Person who Accessed/Used the PHI.** For this factor, consider who the unauthorized recipient is or might be. For example, if the recipient person is someone at another Salus or Business Associate, then this may support a finding that there is a lower probability that the PHI has been compromised since covered entities (CE) and business associates (BA) are obligated to protect the privacy and security of PHI in a similar manner as the CE or BA from where the breached PHI originated. Another example given is if PHI containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low *probability* that the PHI has been compromised.

iii. **Whether the PHI was actually Acquired/Viewed.** For this factor, Salus must investigate and determine if the PHI was *actually* acquired or viewed or, alternatively, if only the *opportunity existed* for the information to be acquired or viewed. One example given here is where a Salus employee mails information to the wrong individual who opens the envelope and calls Salus to say that he/she received the information in error. In contrast, a lost or stolen laptop is recovered and a forensic analysis shows that the otherwise unencrypted PHI on the laptop was never accessed, viewed, acquired, transferred, or otherwise compromised, Salus could determine that the information was *not actually* acquired by an unauthorized individual even though the opportunity existed.

iv. **Mitigation**. For the fourth and final factor, Salus must consider the extent to which, and what steps need to be taken to mitigate, and once taken, how effective the mitigation was. For example, Salus may be able to obtain and rely on the assurances of an employee, affiliated entity, or Business Associate, or another Salus covered entity that the entity or person destroyed PHI it received in error, while such assurances from *certain* third parties may not be sufficient.

Response Procedures for Breaches. If it has been determined that there has been a Security Breach of PHI or PI as set forth, Salus shall notify affected patients reasonably believed to have been affected, law enforcement, media, and federal and state agencies as may be required under the Security Breach Notification Laws and as follows.

i. **Notify Patients**: Notify individuals by mailing a "Notice of Breach" letter to last known address. Substitute notice may be used only if permitted under the Security Breach Notification Laws. *Any information provided to the State Police must be in accordance with Salus' Law Enforcement Requests and Required by Law Policies and Procedures.*

ii. Take steps to **Mitigate** any harm as best as reasonably possible.

iii. Take **corrective actions**, which shall be documented and retained by the Compliance Officer for a period of **six (6) years**. Reasonable and appropriate sanctions shall be assessed against violating employees in accordance with Salus' Sanctions Policy and Procedures.

iv. For Breaches of PHI ONLY:

(1) **Breaches Affecting 500 or More Patients:** If a Security Breach affects 500 or more individuals, Salus shall provide the Secretary of HHS with notice of the breach ***without unreasonable delay*** and in no case later than 60 days from discovery of the breach. This notice must be submitted electronically by completing all information required on the form provided at: http://transparency.cit.nih.gov/breach/index.cfm.

(2) **Breaches Affecting Fewer than 500 Patients: If a Security Breach affects fewer than 500 individuals, log the incident in Salus' Security Breach Log (maintained by the Compliance Officer). Notification to HHS of such incidents (fewer than 500 individuals) shall be submitted annually.** A separate form must be completed for every breach that has occurred during the calendar year. All notifications of breaches occurring in a calendar year must be submitted **within 60 days** of the end of the calendar year in which the breaches occurred. Annual breach notifications must be submitted at: http://transparency.cit.nih.gov/breach/index.cfm.

(3) Notify prominent **Media**, where a Security Breach has affected or is reasonably believed to have affected more than 500 individuals within any given state or jurisdiction.

(4) Notify **Consumer Report Agencies**, where a Security Breach has affected or is reasonably believed to have affected more than 1,000 individuals.

(5) Notify **Law Enforcement**, if otherwise required by law.

PATIENT BREACH NOTIFICATION LETTER

Dear Patient,

Salus takes the security of its patients' personal information very seriously. We have developed and implemented a full privacy and security compliance program aimed at protecting the confidentiality, security and integrity of our patients' information. This program meets the requirements of federal privacy and security laws. Unfortunately, even with all of our careful precautions, Salus has determined that it **[or its Business Associate]** has experienced a "security breach." As a result, some of your personal information may have been accessed, used or disclosed in an unauthorized manner. We are required by law to provide you with this written notice. Salus is offering identity-theft protection in response to this breach. You will be able to sign up for these services, which will be offered free of charge for one year. Information on how to enroll will be posted at [*insert* website]

The security breach occurred on **[*insert* date]** and we learned of the breach on **[*insert* date of discovery]**. **[*insert* brief description of how breach occurred]**. The following types of your personal information may have been accessed in an unauthorized manner: **[full name or SSN or DOB or address or DL number or account numbers, etc.]**.

It is very important to Salus that the risk of harm to you or misuse of the information is minimized. We have attached a checklist of steps you should consider taking in order to protect yourself, under the circumstances, against the potential for misuses of your personal information. The checklist was obtained from the official website of the United States Department of Justice and includes information for contacting the Federal Trade Commission and information about how you can contact credit reporting agencies to place a fraud alert on your consumer report.

We are currently investigating how this security breach occurred and what we can do to protect against any further breaches. For example, we are **[brief description of what is being done]**. If required by law under the circumstances, we have alerted law enforcement, consumer reporting agencies that compile or maintain files on consumers on a nationwide basis and, the U.S. Secretary of the Department of Health and Human Services.

If you have any questions regarding the breach or need additional information, please contact us at **[*insert* contact information]**. We anticipate that you will find the attached checklist helpful and hope that you will not experience any real negative consequences as a result of this security breach. Salus is vitally interested in the well-being of its patients.

Sincerely,

This document has been reprinted from the website of the United States Department of Justice
http://www.usdoj.gov/criminal/fraud/websites/idtheft.html#whatcanido

Identity Theft and Identity Fraud

If you think you've become a victim of identity theft or fraud, act immediately to minimize the damage to your personal funds and financial accounts, as well as your reputation. Here's a list -- based in part on a checklist prepared by the California Public Interest Research Group (CalPIRG) and the Privacy Rights Clearinghouse -- of some actions that you should take right away:

(1) Contact the Federal Trade Commission (FTC) to report the situation, whether –

(2) Online, http://www.consumer.gov/idtheft/victim.htm

(3) By telephone toll-free at 1-877-ID THEFT (877-438-4338) or Direct Dial at 202-326-2502, or

(4) By mail to Consumer Response Center, FTC, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

Under the Identity Theft and Assumption Deterrence Act, the Federal Trade Commission is responsible for receiving and processing complaints from people who believe they may be victims of identity theft, providing informational materials to those people, and referring those complaints to appropriate entities, including the major credit reporting agencies and law enforcement agencies. For further information, please check the FTC's identity theft Web pages . You can also call your local office of the FBI or the U.S. Secret Service to report crimes relating to identity theft and fraud.

You may also need to contact other agencies for other types of identity theft:

(1) Your local office of the Postal Inspection Service if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity;

(2) **The Social Security Administration if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud)**;

(3) The Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).

Call the fraud units of the three principal credit reporting companies:

Equifax:

(1) To report fraud, call (800) 525-6285 or write to P.O. Box 740250, Atlanta, GA 30374-0250.

(2) To order a copy of your credit report ($8 in most states), write to P.O. Box 740241, Atlanta, GA 30374-0241, or call (800) 685-1111.

(3) To dispute information in your report, call the phone number provided on your credit report.

(4) To opt out of pre-approved offers of credit, call (888) 567-8688 or write to Equifax Options, P.O. Box 740123, Atlanta GA 30374-0123.

Experian (formerly TRW)

(1) To report fraud, call (888) EXPERIAN or (888) 397-3742, fax to (800) 301-7196, or write to P.O. Box 1017, Allen, TX 75013.

(2) To order a copy of your credit report ($8 in most states): P.O. Box 2104, Allen TX 75013, or call (888) EXPERIAN.

(3) To dispute information in your report, call the phone number provided on your credit report.

(4) To opt out of pre-approved offers of credit and marketing lists, call (800) 353-0809 or (888) 5OPTOUT or write to P.O. Box 919, Allen, TX 75013.

Trans Union

(1) To report fraud, call (800) 680-7289 or write to P.O. Box 6790, Fullerton, CA 92634.

(2) To order a copy of your credit report ($8 in most states), write to P.O. Box 390, Springfield, PA 19064 or call: (800) 888-4213.

(3) To dispute information in your report, call the phone number provided on your credit report.

(4) To opt out of pre-approved offers of credit and marketing lists, call (800) 680-7293 or (888) 5OPTOUT or write to P.O Box 97328, Jackson, MS 39238.

Contact all creditors with whom your name or identifying data have been fraudulently used. For example, you may need to contact your long-distance telephone company if your long-distance calling card has been stolen or you find fraudulent charges on your bill.

Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge. You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).

Contact the major check verification companies (listed in the CalPIRG-Privacy Rights Clearinghouse checklist) if you have had checks stolen or bank accounts set up by an identity thief. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:

(1) CheckRite -- (800) 766-2748

(2) ChexSystems -- (800) 428-9623 (closed checking accounts)

(3) CrossCheck -- (800) 552-1900

(4) Equifax -- (800) 437-5120

(5) National Processing Co. (NPC) -- (800) 526-5380

(6) SCAN -- (800) 262-7771

(7) TeleCheck -- (800) 710-9898

Where Can I Find Out More About Identity Theft And Fraud?

A number of government and private organizations have information about various aspects of identity theft and fraud: how it can occur, what you can do about it, and how to guard your privacy. To help you learn more about the problem and its solutions, we've attached a list of Web sites that you might find interesting and informative on identity theft and related topics. [Note: All Web sites to which these pages cross-link are included as a service for the reader. Cross-links to non-governmental sites do not constitute an endorsement or approval of their content, or of the organizations responsible for that content, by the Department of Justice.]

Government

Federal Bureau of Investigation - http://www.fbi.gov/

Federal Deposit Insurance Corp - www.fdic.gov/consumers/consumer/news/cnfall97/wallet.html

FTC - Congressional Testimony - http://www.ftc.gov/os/testimony/index.shtml

FTC - Fighting Back Against ID Theft - http://www.ftc.gov/bcp/edu/microsites/idtheft/

United States Postal Inspection Service - http://www.usps.com/postalinspectors/idthft_ncpw.htm

United States Secret Service - http://www.treas.gov/usss/

Non-Government

Better Business Bureau - Alert - http://www.bbb.com/alerts/gwynn.html

Center for Democracy and Technology - http://www.cdt.org/

National Association of Attorneys General - http://www.naag.org/

National Consumers League - http://www.natlconsumersleague.org/

Privacy Rights Clearinghouse - http://www.privacyrights.org/

Business Associate Agreements

PHI may be used and disclosed to external entities referred to as "Business Associates" according to Salus policies and procedures, federal and state regulations, and individual restrictions. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

Definitions:

- Business Associate: an individual or business that, on behalf of Salus, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information. Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. See the definition of "business associate" at 45 CFR 160.103.
- Responsible Party: the employee responsible for authorizing and signing Contracts in specified category on behalf of Salus.

The Responsible Party is responsible for determining if the vendor/individual is a Business Associate. A BAA with a Business Associate shall be obtained at the following times (unless a BAA is not required by law)

1) Prior to any PHI being shared with a Business Associate
2) At the time a new, written or oral contract with a Business Associate is executed.
3) At any other time where PHI must be disclosed to an external entity in connection with services provided on behalf of Salus.

Salus contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). Further information regarding BAAs can be found at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

EXHIBIT A

Sample letter 1

Dear [name of patient]:

Thank you for your request to inspect or copy information that we have about you. Ordinarily, we would be able to respond to your request within 30 days, but due to unusual circumstances we need an additional 30 days in order to respond to you. Accordingly, please expect to hear from us by [insert farthest date].

We look forward to working with you in the future.

Sample letter 2

Dear [name of patient]:

Thank you for your request to inspect or obtain a copy of information that we have about you. We are pleased to be able to grant this request.

If you want to inspect your information or make copies of it yourself, you may do so at our office during our normal business hours. Please let us know what date and time you would like to come. We will do our best to accommodate your requested date and time.

If you would like us to make a copy of your information for you, we are happy to do so. However, we will charge you at the rate of $.20 per page, subject to maximum copying charges as determined from time to time by the Pennsylvania Department of Health. We require payment of these charges in advance, before we start making copies. If you want us to mail the copies to you, we are happy to do so.

If you prefer, we can summarize our information and give that to you instead of having you inspect or copy all of the information. If you want to do this, we will charge $25.00, and we require payment of this amount before we start making the summary.

You requested the information in [format]. We [can/cannot] accommodate that form or format. [Because we cannot accommodate that form or format, we will provide the information to you in hard copy, unless we can agree upon some other format that we can accommodate.]

Thank you again for your request. We look forward to working with you in the future.

Sample letter 3

Dear [name of patient]:

Thank you for your request to inspect or obtain a copy of information that we have about you. Unfortunately, we are unable to permit you to inspect or copy this information.

The reason for this denial is:

[specify]

You are entitled to one review of our decision. If you want to request a review, send a written request to the Compliance Officer at the address shown in our letterhead. The Compliance Officer will look at the information that you want to inspect or copy, and decide if our decision is correct. If it is, you will not be able to inspect or copy the information. If the Compliance Officer concludes that we were wrong in denying you access to the information, you will be able to inspect or copy it, and we will be back in contact with you.

You always have the option to complain to us or to the U.S. Department of Health and Human Services — Office for Civil Rights if you think that we have not properly respected your privacy.

Thank you again for your request. We look forward to working with you in the future.

EXHIBIT B

Sample letter

Dear [name of patient]:

Thank you for your request dated [insert date] to amend information that we have about you.

Unfortunately, we are unable to amend our information because:

[specify permitted reason]

If you are dissatisfied with our decision, you have two options:

(1) You can write a statement disagreeing with our decision and explaining your point of view. We will keep this with your information, and include it in any authorized disclosure of your information from now on. We may decide to write a rebuttal to your statement of disagreement. If we do, it will be included with your information and sent along with any authorized disclosures of it from now on. If you want to do this, send your statement of disagreement to **Compliance Officer, Salus University. 8360 Old York Road, Elkins Park, PA 19027.**

(2) At your option, you could alternatively ask us to simply include your original amendment request with your information. If you do this, we will disclose your original request with any authorized disclosure of your information from now on. If you want to do this, contact the Compliance Officer at the address above.

(3) It is your right to complain to us or to the U.S. Department of Health and Human Services -- Office for Civil Rights.

Thank you and we look forward to working with you in the future.

Sample letter

Dear [name of patient]:

Thank you for your request dated [insert date] to amend information that we have about you. We have made the change that you requested. The corrected information will be sent whenever we are authorized to send your information to anyone from now on.

Please let us know if there is anyone who should get a copy of the corrected information right now. If there is, we will send the corrected information to them as quickly as possible.

Thank you and we look forward to working with you in the future.

Sample letter

Dear [name of patient]:

Thank you for your request to amend information that we have about you. Ordinarily, we would be able to respond to your request within 60 days, but due to unusual circumstances we need an additional 30 days in order to respond to you. Accordingly, please expect to hear from us by [insert farthest date].

We look forward to working with you in the future.

EXHIBIT C

Sample letter

Dear [name of patient]:

Thank you for your request dated [specify date] for an accounting of disclosures that we have made of your protected health information. Ordinarily, we would provide this accounting to you within 60 days of receipt of your written request. Unfortunately, we are unable to provide your accounting within this time because [specify reason]. We will have your accounting ready by [specify date].

Thank you for your patience, and we look forward to working with you in the future.

HIPAA AUTHORIZATION
FOR USE & DISCLOSURE OF HEALTH INFORMATION

I hereby authorize _____("Provider") to use and release my Health Information, as designated below, **to:**

Recipient: _____
Recipient Address: _____
Recipient Telephone Number: _____
Recipient Fax Number: _____

The following Health Information about me may be used and disclosed (*check each either "Yes"or"No/NA"*):

	"Yes"	**"No"*or* N/A**
My entire medical or billing record ……..	☐	☐
HIV/AIDS testing. diagnoses, and treatment…….	☐	☐
Sexually Transmitted Disease testing, diagnosis and treatment……	☐	☐
Mental Illness diagnoses and treatment…….	☐	☐
Drug or Alcohol Addiction diagnoses and treatment ……...	☐	☐
Genetic testing, results and genetic information about me ……..…..	☐	☐
Other: _____	☐	☐

The Health Information checked "yes" above may be used for the following Purpose(s):

☐ At my request, or
☐ For the Purpose of:_____

_____By initialing here, I also specifically authorize my Health Information to be used and disclosed for Marketing purposes. Marketing activities include providing your information to outside third parties, businesses or companies so that they can contact you to sell or promote a product. Salus _____ will receive remuneration for this marketing activity. Salus ____ will not receive remuneration for this marketing activity.

(i*nitial)*

I understand that the terms of this Authorization are governed by the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations ("HIPAA"), as may be amended from time to time. I understand that I have the right to revoke this Authorization, at any time prior to Provider's compliance with the request set forth herein, provided that the revocation is in writing. I further understand that additional information relating to the exceptions to the right to revoke and a description of how I may revoke this Authorization is set forth in Provider's Notice of Privacy Practices. I understand that any revocation must include my name, address, telephone number, date of this Authorization and my signature and that I should send it to: Provider, [CE Street Address] Attn: Privacy Officer

I understand that I am not required to sign this Authorization and that Provider may not condition treatment on my execution of this Authorization. I understand that the information used or disclosed pursuant to this Authorization may be subject to re-disclosure by the Recipient listed above and, in that case, will no longer be protected by HIPAA. This Authorization expires automatically upon Provider's release of my Health Information as needed to fully accomplish the above-described Purpose(s). I hereby acknowledge receipt of a copy of this Authorization.

____/_____/_____ _____ _____
Date Signature of Individual (or Legal Representative) Legal Rep's Authority

☐ ***If the foregoing box is checked, I understand that Provider or its Business Associate will receive remuneration, either directly or indirectly, in exchange for such use and disclosure of my Health Information. I further understand that additional information is available upon my request from the Provider or the Business Associate. _____ (initial)***