2013 Omnibus HIPAA

HITECH Rules

2013 Omnibus HIPAA/HITECH Rules

* * * *

Table of Contents

Policy

It is the policy of Kohll'sRx to safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. Access to information systems to all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to digital and/or electronic protected health information (ePHI) within the organization's information systems and are extended even after termination or other conclusion of access. These safeguards have been established to address the HIPAA Security regulations including the following:

- 164.308a4iiC Access Establishment and Modification
- 164.308a3iiB Workforce Clearance Procedures
- 164.308a4iiB Access Authorization
- 164.312d Person or Entity Authentication
- 164.312a2i Unique User Identification
- 164.308a5iiD Password Management
- 164.312a2iii Automatic Logoff
- 164.310b Workstation Use
- 164.310c Workstation Security
- 164.308a3iiC Termination Procedures
- 164.308a4iiA Isolating Healthcare Clearinghouse Function

Responsible for Implementation:
Privacy/Security Officer

Applicable To:
All workforce members and any other individually provided access. Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Key Definitions:
Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.
Minimum Necessary Information: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The "minimum necessary" standard applies to all protected health information in any form.
Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.

- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Role: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
Workforce: As defined in the HIPAA Privacy Rule, employees, volunteers (board members, community representatives), trainees (students), contractors, and other persons under the direct control of a covered entity.
Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, "workstation" also includes the combination of hardware (i.e., Ethernet ports, hard drive, etc.), operating system, application software, and network connection (including remote and wireless).

Procedures

1) **Access Establishment and Modification** (164.308a4iiC)
   A) Accompany all requests for access to any of the organization's information systems and applications with a "Confidentiality and Information Access Agreement" form (see Appendix 1) completed by the requestor and approved by the requestor's immediate supervisor.
      i) Access is not granted until receipt, review, and approval of a signed "Confidentiality and Information Access Agreement" form.
      ii) The "Confidentiality and Information Access Agreement" form is maintained by the IS Department.
   B) The Human Resources Department is responsible for notifying the IS Department of employees transferred into a new department or new role and facilitating completion of the "Change in Responsibilities Checklist" (see Appendix 2) and the "Information Services Change" form and forwarding it to the IS Help Desk.
      i) The IS Help Desk is responsible for changing the user's access to information systems based on the employee's new role within 24 hours of notification.
2) **Workforce Clearance Procedures** (164.308a3iiB)
   A) The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
   B) All access requests are treated on a 'least-access principle" blanket access is not provided for any user.
3) **Access Authorization** (164.308a4iiB)
   A) Role based access categories for each information system/application are pre-approved by the Technical Security Officer & Privacy Officer (or other designated department). Categories are defined by the importance of the applications running on the information system, the value or sensitivity of the ePHI on the information system, security controls on the information system, security controls on the workstation utilized to access the information system, and the extent to which the information system is connected to other information systems.

B) The IS Help Desk grants the level of access to users based on these pre-determined categories.

4) **Person or Entity Authentication** (164.312d)
   A) Each user has and uses a unique User Login ID and password that identifies him/her as the user of the information system.
5) **Unique User Identification** (164.312a2I)
   A) Access to the organization's information systems/applications is controlled by requiring unique User Login ID's and passwords for each individual user.
   B) Passwords are a minimum of six characters and are alpha numeric (see Appendix 3).
   C) Passwords are not displayed at any time. Password characters are replaced with asterisks "*" when typed.
   D) Users may not select passwords that may be easily guessed or obtained using personal information (ex. names, favorite sports team, etc.) (Refer to Appendix 3 for Password Guidelines).
   E) The IS Department assigns a generic User Login ID and password for each user to utilize for first time access into each information system. The User Login ID and password are forwarded in a sealed envelope stating the user's name to the employee's supervisor. The supervisor distributes the sealed envelope to the user.
   F) Each information system automatically requires users to change their User Login ID and password upon first-time use of the information system.
6) **Password Management** (164.308a5iiD)
   A) User Login IDs and passwords are used to control access to the organization's information systems and may not be disclosed to anyone for any reason.
   B) Users may not allow anyone for any reason to have access to any information system using another user's unique User Login ID and password.
   C) Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the network, system, application, and/or database.
   D) The information systems are programmed to deny user's ability to use a prior password.
   E) Users that do not recall their User Login ID and/or password may contact the IS Help Desk. The IS Help desk provides the employee with a temporary, one-time use User Login ID and password within 24 hours of notification.
   F) Passwords are inactivated immediately upon an employee's termination (refer to the termination procedures in this policy).
   G) If a user believes their User Login ID has been compromised, they are required to immediately report the incident to the Technical Security Officer and /or the IS Department.
7) **Automatic Logoff** (164.312a2iii)
   A) Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
   B) Users log off information systems/applications at the end of their shift, or at the end of their need to use the system/application, whichever is sooner.

C) Information systems automatically log users off the systems after 15 minutes of inactivity. Implement a shortened automatic log off time of 5 or 10 minutes for workstations located in public or high traffic areas.
D) The Technical Security Officer & Privacy Officer pre-approve exceptions to automatic log off requirements.

8) **Workstation Use** (164.310b)
A) Workstations may only be used for authorized business purposes.
B) Place workstations in secure areas away from regular patient traffic and position display screens to minimize unauthorized viewing and/or access.
C) All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI in the information systems at all times.
D) Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
i. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated" Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization's system.
ii. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
iii. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
iv. Participation in chain letters and other such activities is also prohibited.
v. Transmitted messages may not contain material that criticizes organization, its providers, its employees, or others.
vi. Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.

9) **Workstation Security** (164.310c)
A) Workstations are the property of organization and must always remain on the premises, unless prior authorization by the Technical Security Officer has been granted for removal of workstations from the premises.
B) Workstations utilized off organization's premises are protected with security controls equivalent to those for on-site workstations.
C) Users may only access and utilize workstations as assigned by their supervisor.
D) Supervisors are responsible for monitoring use of workstations.
E) All users report unauthorized workstation use to the Technical Security Officer.
F) The organization installs on all workstations anti-virus software to prevent transmission of malicious software. This software is regularly updated.
G) Portable workstations (e.g., workstations (e.g., PDAs, laptops, etc.) are also subject to the same safeguards and protections. Portable workstations are maintained in a safe and secure manner when transported.
H) Networks are secured with a Firewall.

i) Network access is limited to legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
ii) Firewall console and other management ports are appropriately secured or disabled and are located in a physically secure environment.
iii) Mechanisms to log failed access attempts are in place.
iv) The configuration of firewalls used to protect networks are approved by the Technical Security Officer and maintained by the IS Department.

I) Servers are located in a physically secure environment and are on a secure network with firewall protection.
i) The system administrator or root account is password protected.
ii) A security patch and update procedure are established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
iii) All unused or unnecessary services are disabled.

10) **Termination Procedures** (164.308a3iiC)
A) The Human Resources Department (or other designated department), users, and their supervisors are required to notify the IS Help Desk upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist" (refer to Appendix 4).
B) The Human Resources Department, users, and supervisors are required to notify the IS Help Desk to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
i) The user has been using their access rights inappropriately,
ii) A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password)
iii) An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
C) The IS Help Desk will terminate users' access rights immediately upon notification.
D) The IS Department audits and may terminate access of users that have not logged into organization's information systems/applications for a period of over six (6) months.

11) **Isolating Healthcare Clearinghouse Function** (164.308a4iiA)
A) If a health care clearinghouse is part of a larger organization, the clearinghouse implements policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.

Risk Management

1. It is the policy of Kohll'sRx to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health information (ePHI) (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's information security program.

2. Risk analysis and risk management are recognized as important components of Kohll'sRx's corporate compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).
   A. Risk assessments are done throughout IT system life cycles:
      - Before the purchase or integration of new technologies and changes are made to physical safeguards;
      - While integrating technology and making physical security changes; and
      - While sustaining and monitoring of appropriate security controls.
   B. The Kohll'sRx performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.
3. Kohll'sRx implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   A. Ensure the confidentiality, integrity, and availability of all ePHI the organization creates, receives, maintains, and/or transmits,
   B. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI,
   C. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required, and
   D. Ensure compliance by workforce.
4. Any risk remaining (residual) after other risk controls have been applied, requires approval by the senior management or the owner.
5. All Kohll'sRx workforce members are expected to fully cooperate with all persons charged with doing risk management work. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to Kohll'sRx policies.
6. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.

Scope

The scope of the information security risk management process covers the administrative, physical, and technical processes that enable and govern ePHI that is received, created, maintained, or transmitted.

Key Definitions:

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Risk: The likelihood that a threat will exploit vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.

Risk Management Team: Individuals who are knowledgeable about the Organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and

procedures outlined below. This team is comprised of the Physical Plant Security Officer, Privacy/Security Officer, and the Chief Information Officer.

Risk Assessment: (Referred to as *Risk Analysis* in the HIPAA Security Rule); the process:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk Management: Within this policy, it refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

Risk Mitigation: Referred to as *Risk Management* in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

Threat: the potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse, or resources, etc.

Threat Source – Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human, or environmental which can impact the organization's ability to protect ePHI.

Threat Action – The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

1. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of Kohll'sRx's Information Security Officer (or other designated employee), and the identified Risk Management Team.

Risk Assessment: The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

A. Step 1. System Characterization
   i. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration

policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media). (See "Risk Analysis & Risk Management Toolkit – Network Diagram Example and Inventory Asset List" to assist with these efforts)

ii. *Output* – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries.

B. Step 2. Threat Identification

i. In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats. The list should be based on the individual organization and its processing environment. (See "Risk Analysis & Risk Management Toolkit –Threat Overview" for definitions and the "Threat Source List" in the Risk Assessment for examples of threat sources.)

ii. *Output* – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

C. Step 3. Vulnerability Identification

i. The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network. (See "Risk Analysis & Risk Management Toolkit – Risk Assessment Template – Security Questions and Threat Source List.")

ii. *Output* – A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

D. Step 4. Control Analysis

i. The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat-source exploiting a system vulnerability.

ii. *Output* – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

E. Step 5. Likelihood Determination

i. The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls. (See "Risk Analysis & Risk Management Toolkit – Risk Likelihood, Risk Impact, and Risk Level Definitions.")

ii. *Output* – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.

F. Step 6. Impact Analysis

i. The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and

criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data. (See "Risk Analysis & Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions.")

ii. Output – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

G. Step 7. Risk Determination

i. This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management (the mission owners) must take for each risk level. (See "Risk Analysis & Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions.")

ii. *Output* – Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

H. Step 8. Control Recommendations

i. The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. (See "Risk Analysis & Risk Management Toolkit – NIST - Risk Mitigation Activities.")

ii. *Output* – Recommendation of control(s) and alternative solutions to mitigate risk.

I. Step 9. Results Documentation

i. Results of the risk assessment are documented in an official report or briefing and provided to senior management (the mission owners) to make decisions on policy, procedure, budget, and system operational and management changes. (See "Risk Analysis & Risk Management Toolkit –Risk Analysis Report Template")

ii. *Output* – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity, and availability of ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

A. Step 1. Prioritize Actions –

i. Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources

ii. *Output* – Actions ranked from high to low

B. Step 2. Evaluate Recommended Control Options –

i. Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions

for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair.

ii. *Output* – list of feasible controls

C. Step 3. Conduct Cost-Benefit Analysis –

i. Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.

ii. *Output* – Documented cost- benefit analysis of either implementing or not implementing each specific control

D. Step 4. Select Control(s) –

i. Taking into account the information and results from previous steps, the Kohll'sRx's mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.

ii. *Output* – Selected control(s)

E. Step 5. Assign Responsibility –

i. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

ii. *Output* – List of resources, responsible persons, and their assignments

F. Step 6. Develop Safeguard Implementation Plan –

i. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:

   a. Each risk or vulnerability/threat pair and risk level
   b. Prioritized actions
   c. The recommended feasible control(s) for each identified risk
   d. Required resources for implementation of selected controls
   e. Team member responsible for implementation of each control
   f. Start date for implementation
   g. Target date for completion of implementation
   h. Maintenance requirements.

ii. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization's executive management/leadership team (e.g., the Board, senior management, and other key stakeholders).

iii. Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates and project requirements.
iv. *Output* – Safeguard Implementation Plan

G. Step 7. Implement Selected Controls – as controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not eliminate the risk.
   i. Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
   ii. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
   iii. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
   iv. *Output* – Residual Risk

Risk Management Schedule: The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of Kohll'sRx's information security program:

A. Scheduled Basis – an overall risk assessment of Kohll'sRx's information system infrastructure will be conducted annually <or other timeframe>. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.
B. Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
C. As Needed – the Security Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect Kohll'sRx's information systems.

Process Documentation. Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.

Applicable Standards/Regulations:

- 45 CFR 164.308(a)(1)(ii)(A) – HIPAA Security Rule Risk Analysis
- 45 CFR 164.308(a)(1)(ii)(B) – HIPAA Security Rule Risk Management
- 45 CFR 164.308(a)(8) – HIPAA Security Rule Evaluation

Privacy Implementation and Oversight

To comply with the Administrative Simplification Act component of HIPAA Privacy, to secure and maintain the confidentiality of protected health information, maintain sensitive

organizational information at Kohll'sRx and prevent and detect inappropriate and illegal uses and disclosures. Kohll'sRx shall be responsible for implementation of the administrative requirements under the federal privacy rule. Kohll'sRx will designate a privacy official to be responsible for the development and implementation of the policies and procedures of Kohll'sRx. [45 CFR 164.530(a)(1)(i)]

Definitions:

I. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

II. Individually Identifiable Health Information (IIHI). Under Section 160.103 of HIPAA, IIHI is defined as information that is a subset of health information, including demographic information collected from an individual, and:
   A. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
   B. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
      1. That identifies the individual; or
      2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
   C. IIHI includes identifiers of the patient, relatives, employers, or household members such as the following (§164.514):
      1. Names,
      2. Geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code (except for the initial 3 digits of a zip code if, according to the current publicly available data from the Bureaus of the Census the all zip codes with the same 3 initial digits contains more than 20,000 people),
      3. All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older,
      4. Telephone numbers,
      5. Fax numbers,
      6. Electronic mail addresses,
      7. Social security numbers,
      8. Medical record numbers
      9. Health plan beneficiary numbers,
      10. Account numbers,
      11. Certificate/license numbers,
      12. Vehicle identifiers and serial numbers, including license plate numbers,
      13. Device identifiers and serial numbers,
      14. Web Universal Resource Locators (URLs),
      15. Internet Protocol (IP) address numbers,
      16. Biometric identifiers, including finger and voice prints,
      17. Full face photographic images and any comparable images, and
      18. Any other unique identifying number, characteristic, or code.

III. Protected Health Information (PHI). Under Section 164.501 of HIPAA, PHI means IIHI that is transmitted and maintained in electronic media or in any other form or medium.

IV. In compliance with §164.524 contained within the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Kohll'sRx Health Centers maintains a designated record set (DRS). The designated record set includes medical and billing records to which patients and/or their personal representatives have the right to access, inspect, and copy. Records include any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a … provider (§164.501). Refer to Policy 01-65 for a listing of protected health information that consists of the designated record set.

V. The health care records of a patient are the property of Kohll'sRx but the information maintained within the record belongs to the patient.

VI. An Individual, for purposes of HIPAA, is the patient and his/her legal Personal Representative (§164.502(g)).

VII. A Personal Representative is one who under law has the authority to act on behalf of a patient in making decisions related to health care (i.e., a parent, guardian, or legal custodian under WI stat. 48.02(8) and (11)). Personal Representatives may have access to and or request amendment of protected health information relevant to their representative capacity unless there is a reasonable belief that the patient has been or may be subjected to domestic violence, abuse, or neglect by such person, the release could endanger the patient, or in the exercise of professional judgment it is decided that it is not in the best interest of the patient to treat the person as the patient's personal representative [§164.502(g)]

VIII. Treatment. The provision, coordination, or management of health care and related services, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another (§164.501).

IX. Payment. Activities undertaken by Kohll'sRx to obtain or provide reimbursement for the provision of health care. Activities for payment include eligibility of coverage determination, billing, claims management, collection activities, utilization review including precertification, preauthorization, concurrent, and retrospective review of services, and specified disclosures to consumer reporting agencies (§164.501).

X. Health Care Operations. Quality assessment and improvement activities; reviewing the competence, qualifications, performance of health care professionals, conducting training programs, accreditation, certification, licensing, credentialing; underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits; conducting or arranging for medical review, legal services, and audition functions; business planning and development; business management (§164.501).

XI. Workforce. Under Section 160.103 of HIPAA, workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Kohll'sRx, is under the direct control of Kohll'sRx, whether they are paid by Kohll'sRx.

XII. Provider: Under Section 160.103 of HIPAA, a provider of medical or health services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u) and 1861(s) of the Act, 42 U.S.C. 1395x(s)) and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Providers at MAHC are those contracted, subcontracted, or employed and provides services on behalf of MAHC.

I. Kohll'sRx is committed to complying with the HIPAA Privacy Rule efforts throughout the organization focus on maintaining the confidentiality of patients' protected health information through appropriate, authorized access, uses, and disclosures.

II. Kohll'sRx and its business affiliates create, store, maintain, use, transmit, collect, and disseminate protected health information in an environment that promotes confidentiality and integrity without compromising information availability.

III. Confidentiality policies and procedures are reinforced throughout Kohll'sRx and followed by all physicians and workforce members.

IV. The HIPAA Privacy Officer oversees the HIPAA Privacy program. [§164.530(a)(1)(i)].

A. The HIPAA Privacy program may include a team. The following positions are recommended to be considered/involved in the administration of the Privacy Rule.

1. Corporate Compliance Officer, Privacy/Safety Director
2. I/S Decision Support Manager,
3. Physical Plant Security Officer
4. Owner
5. Medical director

V. The HIPAA Privacy Officer is responsible for the facilitation of the following functions which reinforce compliance with the HIPAA Privacy Rule, patient confidentiality, access laws and Kohll'sRx's policies and procedures pertaining to them:

A. Establish and maintain written policies and procedures that place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information from intentional or unintentional uses and disclosures that are in violation of the law [§164.530(c & i)],

1. Update policies and procedures as necessary and appropriate, and in compliance with Kohll'sRx's Notice of Privacy Practices, to comply with changes in the law [§164.530(i)(2-4)].
2. Make necessary changes to Kohll'sRx's Notice of Privacy Practices [§164.530(i)(2 & 3)].
3. Maintain policies and procedures (including any changes made) in written or electronic form for six years from the date of its creation or the date when it last was in effect, whichever is later [§164.530(j)],

B. Make all reasonable efforts to limit incidental uses and disclosures [§164.530(c)(2)(ii)],

C. Provide training for its workforce members of the established policies and procedures as necessary to and appropriate to carry out their job functions and document the training provided [§164.530(b)],

1. To each member of the workforce by no later than the compliance date for Kohll'sRx,
2. To new workforce members during their first month of employment,
3. To existing workforce members annually.
4. To existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective.

D. Maintain a program promoting workforce members and patients to report complaints concerning compliance of the law and Kohll'sRx policies and procedures to (PERSON or OFFICE) [§164.530(a & d)],

1. Promptly and properly investigate and address reported violations, taking steps to prevent recurrence.

2. Document all complaints and follow up documentation and file them [§164.530(d)(2)].

E. Persons, including workforce members and patients, who make reports or participate in an investigation of violations in good faith will not be subject to intimidation, treats, coercion, discrimination against, or any other retaliatory action as a consequence [§164.530(g)],

F. Mitigate, to the extent practicable, any harmful effect that is known to the Kohll'sRx of a use or disclosure of PHI in violation of its policies and procedures or the requirements of the law by Kohll'sRx or its business associate [§164.530(f)],

G. Consistently enforce the law and Kohll'sRx's policies and procedures through appropriate disciplinary mechanisms [§164.530(e)],
   1. Actions taken against a workforce member who failed to comply with the policies and procedures are documented and filed in the Privacy Officer's files [§164.530(e)(2)],

H. Monitor, audit, and reinforce compliance with the law and Kohll'sRx's policies and procedures,

I. Provide assistance to patients and other workforce members about the law and Kohll'sRx policies and procedures [§164.530(a)(1)(ii)],

J. Not require individuals to waive their legal rights as a condition of the provision of treatment or payment [§164.530(h)],

K. Implement, Distribute and Maintain the Notice of Privacy Practices [§164.520(a-e)],
   1. Maintain a copy of the Notice (including changes made) for six years from the date when it was last in effect,
   2. Update the Notice to reflect changes in the law or Kohll'sRx policies and procedures,
   3. Distribute the Notice,
   4. Direct questions regarding the Notice to Allen A Kurland, Compliance/Privacy/Safety Officer.

VI. Kohll'sRx will implement, monitor, and maintain a Business Associate Agreement with affiliate business entities when required by law.

VII. Documentation

A. All documentation related to and/or required by HIPAA, including but not limited to compliance enforcement, activities such as training, policies and procedures, complaint investigations, designated record sets, etc. are maintained for six years from the date of creation, or the date it was last in effect, whichever is later [§164.530(j)]. Documentation may be maintained in written or electronic form [§164.530(j)(1)(ii)].

Security Implementation and Oversight

In accordance with the standards set forth in the HIPAA Security Rule, Kohll'sRx is committed to ensuring the confidentiality, integrity, and availability of all electronic protected health information (ePHI) it creates, receives, maintains, and/or transmits. To provide for the appropriate development, implementation, and oversight of Kohll'sRx's efforts toward compliance of the HIPAA security regulations, Kohll'sRx has a Security Officer [164.308(a)(2)] responsible for facilitating the training and supervision of all workforce members [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any workforce member that is in non-compliance with the HIPAA security regulations [164.308(a)(1)(ii)(c)], and writing, implementing, and maintaining all policies, procedures, and documentation related to efforts toward HIPAA security compliance [164.316(a-b)].

Responsible for Implementation:
Administration and Privacy/Security Officer
Applicable To:
Privacy/Security Officer, leadership, workforce members, and others as assigned
Key Definitions:
Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.
Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Workforce: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether they are paid by the covered entity.

1) **Privacy/Security Officer Responsibilities**. The Privacy/Security Officer is responsible for facilitating the development, implementation, and oversight of all activities pertaining to Kohll'sRx's efforts to be compliant with the HIPAA Security Regulations. The intent of all oversight activities includes those necessary to maintain the confidentiality, integrity, and availability of ePHI. These responsibilities are included in the Privacy/Security Officer's duties and include, but are not limited to, the following:
   a) Oversees and enforces all activities necessary to comply with the Security rule and verifies the activities are in alignment with the requirements.
   b) Establishes and maintains written policies and procedures to comply with the Security rule and maintains them for six years from the date of creation or date it was last in effect, whichever is later.
   c) Updates policies and procedures as necessary and appropriate to comply with the Security rule and maintains changes made for six years from the date of creation or date it was last in effect, whichever is later.
   d) Facilitates audits to validate Security compliance efforts throughout the organization.
   e) Documents all activities and assessments completed to comply with the Security rule and maintains it for six years from the date of creation or date it was last in effect, whichever is later.
   f) Provides copies of the policies and procedures to management, and has them available to review by all other workforce members to which they apply.
   g) Annually, and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security of ePHI.
   h) Provides annual training to all workforce members of established policies and procedures as necessary and appropriate to carry out their job functions, and documents the training provided
   i) Develops and provides periodic security updates and reminder communications for all workforce members.

j) Implements procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it may be accessed.
k) Maintains a program promoting workforce members to report non-compliance with established Security rule policies and procedures.
    i) Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
    ii) Applies consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Kohll'sRx.
    iii) Mitigates to the extent practicable, any harmful effect known to Kohll'sRx of a use or disclosure of ePHI in violation of Kohll'sRx's policies and procedures or business associates.
l) Reports security efforts and incidents to administration in a timely manner.
m) Assists in the administration and oversight of business associate agreements.

2) **Workforce Training**.
a) The Privacy/Security Officer facilitates the training of all workforce members as follows:
    i) New workforce members during their first month of employment.
    ii) Existing workforce members annually.
    iii) Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective.
b) Workforce members sign into the training session.
c) The Security Officer or designee maintains documentation of the training session materials and attendees for a minimum of six years.
d) The training session focuses on, but is not limited to, the following subjects defined in Kohll'sRx's security policies and procedures:
    i) Auditing. Kohll'sRx may monitor access and activities of all users
    ii) Workstations may only be used to perform assigned job responsibilities
    iii) Users may not download software onto Kohll'sRx's workstations and/or systems without prior approval from the Security Officer
    iv) Users are required to report malicious software to the Security Officer immediately
    v) Users are required to report unauthorized attempts, uses of, and theft of Kohll'sRx's systems and/or workstations
    vi) Users are required to report unauthorized access to facilities
    vii) Users are required to report noted log-in discrepancies (i.e., application states users last log-in was on a date user was on vacation)
    viii) Users may not alter ePHI maintained in a database, unless authorized to do so as a part of their job responsibilities
    ix) Users are required to understand their role in Kohll'sRx's contingency plan
    x) Users may not share their user names nor passwords with anyone
    xi) Requirements for users to create and change passwords
    xii) Users must set all applications that contain or transmit ePHI to automatically log off after "X" minutes of inactivity
    xiii) Supervisors are required to report terminations of workforce members and other outside users.
    xiv) Supervisors are required to report a change in a user's title, role, department, and/or location
    xv) Procedures to backup ePHI

xvi) Procedures to move and record movement of hardware and electronic media containing ePHI
xvii) Procedures to dispose of discs, CDs, hard drives, and other media containing ePHI.
xviii) Procedures to re-use electronic media containing ePHI.
xix) Email encryption procedures

e) The Security Officer facilitates the communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:
   i) Latest malicious software or virus alerts
   ii) Kohll'sRx's requirement to report unauthorized attempts to access ePHI
   iii) Changes in creating or changing passwords
f) Additional training is provided to workforce members in the information services department. This training is specific in nature, as to the Kohll'sRx's requirements for their involvement in areas such as the following:
   i) Data backup plans
   ii) System auditing procedures
   iii) Redundancy procedures
   iv) Contingency plans
   v) Virus protection
   vi) Patch management
   vii) Media Disposal and/or Re-use
   viii) Documentation requirements

3) **Supervision of Workforce**. Although the Privacy/Security Officer is responsible for implementing and overseeing all activities related to compliance with the Security rule, it is the responsibility of all leaders to supervise all workforce members and any other user of Kohll'sRx's systems, applications, servers, workstations, etc. that contain ePHI.
   a) Leaders monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.
   b) Leaders assist the Privacy/Security Officer to ensure appropriate role-based access is provided to all users.
   c) Leaders take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and Kohll'sRx's security policies and procedures.
4) **Sanctions**. All workforce members and other users report non-compliance of Kohll'sRx's policies and procedures to the Privacy/Security Officer or other individual as assigned by the Privacy/Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.
   a) The Privacy/Security Officer promptly facilitates a thorough investigation of all reported violations of Kohll'sRx's security policies and procedures. The Privacy/Security Officer may request the assistance from others such as Human Resources, the workforce member's or users' leader, other workforce members, and/or other users.
      i) Complete an audit trail/log to identify and verify the violation and sequence of events.
      ii) Interview any individual that may be aware of or involved in the incident.
         (1) All individuals are required to cooperate with the investigation process and provide information to those conducting the investigation.

(2) Provide individuals suspected of non-compliance of the Security rule and/or Kohll'sRx's policies and procedures the opportunity to explain their actions.

iii) The investigators thoroughly document the investigation as the investigation occurs.

b) Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

i) A violation resulting in a breach of confidentiality (i.e., release of PHI to an unauthorized individual), change of the integrity of any ePHI, or inability to access any ePHI by other users, requires immediate consideration of termination of the user from Kohll'sRx.

c) The Privacy/Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).

d) The Privacy/Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.

Applicable Standards/Regulations:

- 45 CFR §164.308(a)(2) HIPAA Security Rule Assigned Security Responsibility
- 45 CFR §164.308(a)(1)(ii)(c) HIPAA Security Rule Sanction Policy
- 45 CFR §164.308(a)(3)(ii)(A) HIPAA Security Rule Authorization and/or Supervision
- 45 CFR §164.308(a)(5)(ii)(A) HIPAA Security Rule Security Reminders
- 45 CFR §164.316(a-b) HIPAA Security Rule Documentation

Patient Privacy Rights

The purpose of this document is to outline and educate Kohll'sRx employees about the policies and procedures needed to comply with the patient privacy rights enacted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). More detailed documents discussing our policies and procedures for each of these rights are available to all employees. It is the policy of Kohll'sRx to implement the following policies and procedures that will ensure patient privacy rights in accordance with the Privacy Regulations promulgated under HIPAA:

1. **Availability of Kohll'sRx's Privacy Notice:** The patient has the right to receive our privacy notice in a timely manner. Upon request, the patient may at any time receive a paper copy of our privacy notice, even if he or she earlier agreed to receive the notice electronically. We must also post our privacy notice in a prominent location.
2. **Requesting Restrictions on Certain Uses and Disclosures:** The patient has the right to object to, and ask for restrictions on, how his or her health information is used or to whom the information is disclosed, even if the restriction affects the patient's treatment or our payment or health care operation activities. The patient may want to limit the health information that is included in patient directories, or provided to family or friends involved in his or her care or payment of medical bills. The patient may also want to limit the health information provided to authorities involved with disaster relief efforts. However, we are not required to agree in all circumstances to the patient's requested restriction.

3. Kohll'sRx **Receiving Confidential Communication of Health Information:** The patient has the right to ask that we communicate his or her health information to them in different ways or places. For example, the patient may wish to receive information about their health status in a special, private room or through a written letter sent to a private address. We must accommodate requests that are reasonable in terms of administrative burden. We may not require the patient to give a reason for the request.
4. Kohll'sRx's **Access, Inspection and Copying of Health Information:** Patients have the right to inspect and obtain a copy of their health information. In addition, we may charge the patient a reasonable cost-based fee for copies of their health information.
5. **Requesting Amendments or Corrections to Health Information:** If the patient believes their health information is incomplete or incorrect, they may ask us to correct the information. The patient may be asked to make such requests in writing and to give a reason as to why his or her health information should be changed. However, if we did not create the health information that the patient believes is incorrect, or if we disagree with the patient and believe his or her health information is correct, we may deny the request. We must act on the request within 60 days after we receive it, unless we inform the patient of our need for a one-time 30-day extension.
6. **Receiving an Accounting of Disclosures of Health Information:** In some limited instances, the patient has the right to ask for a list of the disclosures of their health information that we have made while we maintained their protected health information in their designated record set. This list must include the date and time of the received request, date, and time of the disclosure, who received the disclosed health information, a brief description of the health information disclosed, and why the disclosure was made. We must furnish the patient with a list within 60 days of the request, unless we inform the patient of our need for a one-time 30-day extension or upon reasonable notice, and we may not charge the patient for the list, unless the patient requests such list more than once in a 12-month period.
7. **Complaints:** Patients have the right to file a complaint with us and with the federal Department of Health and Human Services if they believe their privacy rights have been violated. We will not retaliate against the patient for filing such a complaint. To file a complaint with either entity, the patient should contact Allen A Kurland, who will provide the patient with the necessary assistance and paperwork.

Should the law regarding patient privacy rights under HIPAA change, we will update our organization's policies and procedures regarding those rights, if applicable. All new staff of Kohll'sRx shall receive a copy of this document electronically and at the work-site. All current staff of Kohll'sRx shall receive a copy of this document as part of our HIPAA compliance training session, and upon request.

Validation of Content of Patient Authorization

To ensure the privacy of patient health information, Kohll'sRx obtains a valid patient authorization for uses and disclosures of health information that are not otherwise required or permitted by law. In general, any use or disclosure of protected health information will be limited to the minimum amount of information necessary to carry out the purpose of the use or disclosure. To be valid, an authorization must be written in plain language and contain:

1. A meaningful description of the health information to be used or disclosed;
2. A description of each purpose of the use or disclosure in question;

3. The name or specific identification of the person(s) or class of persons authorized to make the requested use or disclosure;
4. The name or specific identification of the person(s) or class of persons to whom the use or disclosure may be made;
5. An expiration date or event;
6. A statement of the patient's right to revoke the authorization in writing and the limitations on that right;
7. A description of how the patient may revoke the authorization;
8. A statement acknowledging that the health information disclosed pursuant to the authorization may be re-disclosed by the recipient and no longer protected by Kohll'sRx's privacy practices;
9. A statement of Kohll'sRx's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization; and
10. Signature of the patient or the patient's legal representative and the date signed. The signature of a legal representative must be accompanied by a description of the representative's authority to act for the patient.

An authorization is invalid if any of the following occur:

1. The expiration date or event has passed;
2. The authorization lacks any of the required elements; See section A above.
3. The authorization contains missing required information;
4. The authorization contains material information that Kohll'sRx knows to be false;
5. The authorization is known by Kohll'sRx to have been revoked; or
6. The authorization is of a type prohibited by law.

If the organization obtains the authorization, Kohll'sRx must provide the patient with a copy of the signed authorization. Kohll'sRx must document and maintain all patient authorizations for a period of at least six years, or in accordance with state law, whichever is longer.

Obtaining a Written Acknowledgement

HIPAA requires health care providers to obtain a patient's written acknowledgement that the patient received the provider's Notice of Privacy Practices (NPP), or at least make a good faith effort to obtain such acknowledgement.[1] In addition, HIPAA requires providers to document that the provider obtained or made a good faith effort to obtain the patient's written acknowledgement.[2] Subsequent revisions to the Notice of Privacy Practices do not require Kohll'sRx to obtain another written acknowledgement. However, the Notice should be made available upon request on or after the effective date of the revision. This policy will explain how Kohll'sRx's employees should carry out these requirements. A sample Acknowledgement Form is attached to this document.

Note: To avoid duplication, providers may also include sections of the Acknowledgement Form with other consent to treat, registration, acknowledgement or other internal documents delivered to patients at initial and follow-up visits already in use by the provider.

After April 14, 2003, when a patient first receives care from our facility (including service delivered electronically), the workforce member in charge of providing our Notice of Privacy

[1] 45 CFR § 164.520(c)(2)(ii) (2002).
[2] ibid..

Practices* shall make a good faith effort to obtain the patient's written acknowledgement and to ensure the patient received a copy of the Notice of Privacy Practices. Specifically, the workforce member should ensure that the patient receives assistance with the written acknowledgment form and is provided an opportunity to ask questions. The acknowledgement form is located by the cash register/POS system. It is the goal of this facility to have as many patients sign Acknowledgement Forms as possible, even if it takes several attempts for each patient.

Procedure for Obtaining a Patient's Written Acknowledgement:

Situation A. In nonemergency situations where the patient physically visits our facility, the workforce member in charge of providing our Notice of Privacy Practices shall:*
Situation B. In emergency situations when the patient is physically able to sign the Acknowledgement Form, the employee in charge of providing our Notice of Privacy Practices shall, as soon as reasonably practicable after the emergency treatment situation:*
Situation C. In situations when the patient is physically unavailable to sign the Acknowledgement Form (e.g., received services electronically) or the organization chooses to use the electronic notice option under HIPAA, the workforce member in charge of providing our Notice of Privacy Practices shall:*
Situation D: In situations where the patient is incapacitated/unable to sign/understand the Acknowledgement Form, the employee in charge of providing our Notice of Privacy Practices shall:*

Situation A and B	Situation C	Situation D
1. Provide a copy of the Notice of Privacy Practices to the patient within 24 hours of the first delivery date; 2. Provide an opportunity for the patient to ask questions or raise concerns about the privacy of his or her health information; 3. Discuss all questions or concerns; 4. Refer the patient to more knowledgeable, accessible sources if the patient is dissatisfied with the answers to their questions or concerns about the privacy of their health information; 5. Give the patient an opportunity to read the Acknowledgement form; 6. Ensure that the patient or his or her personal representative checks both boxes on the Acknowledgement form, located in the back of the Notice of Privacy	1. Send an electronic notice automatically and contemporaneously in response to the patient's first request for service after April 14, 2003 (an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgement of the notice), otherwise, proceed to the next step. **** 2. Look through the patient's medical record to find contact information; 3. If a patient's contact information is found, attempt to contact the patient by phone, email (secure when possible and if not possible as agreed by the patient) or letter; 4. If patient is successfully contacted, send the Notice of Privacy Practices within 24 hours of the first date of service by mail, fax, email (secure when possible and if not possible as agreed by the patient), or patient portal (whichever method the patient prefers). If unable to contact the patient, send the Notice of Privacy Practices to the patient's last known mailing address; 5. Send the patient the Notice of Privacy Practices along with a note (make a copy of the note for our records) requesting the following: a. That the patient read the Notice of Privacy Practices; b. That the patient calls our Privacy Officer with any questions or concerns (provide the contact information for our Privacy Officer in the note); c. Once the patient reads and understands the contents of the Notice of Privacy Practices, that the patient checks the boxes and sign the	1. Check with the patient's treating physician to verify the patient's incapacity; 2. If incapacity is verified and the patient has a valid personal representative, follow the steps in **Situations A & B**, substituting the personal representative[3] for the patient; 3. If the patient does not have a valid personal representative and his or her incapacity does not improve within a reasonable amount of time to the point where he or she can sign/understand the Acknowledgement Form, do the following: a. Fill out all the items listed in the box on top of the Acknowledgement Form; b. Fill out the bottom half of the Acknowledgement Form, providing a clear, detailed explanation of why the patient did not sign the form and the efforts that were displayed in trying to obtain the patient's signature; c. File the completed Acknowledgement;

[3] HIPAA regulations define "personal representative" as those who, under applicable law, have authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care. 45 CFR § 164.502(g)(2) 2000. Covered entities should consult 45 CFR § 164.502(g) and state law to get a full understanding of the treatment of personal representatives under HIPAA.

Situation A and B	Situation C	Situation D
Practices, and signs his or her name; 7. Fill out all the items listed in the box on top of the Acknowledgement form; 8. Ensure there are two copies of the signed Acknowledgement form, one for the patient and one for our file; and 9. File our copy of the completed form in the patient's medical record or patient admission/billing record in either paper or electronic format.	acknowledgement form located in the back of the Notice of Privacy Practices; d. That the patient drops off, fax or mail the signed acknowledgement form to our facility in the next 30 days**. In the alternative, a patient may email their written acknowledgement to the provider. e. Upon receiving the signed acknowledgement form from the patient, fill out all the items listed in the box on top of the acknowledgement form. In the case of a patient emailing a written acknowledgement, print out the email and place in the patient's medical record; f. Ensure there are two copies of the signed acknowledgement form, one for the patient and one for our file; g. Send a completed form to the patient; and h. File our copy of the completed form in the patient's medical record or patient admission/billing record in either paper or electronic format. 6. If the patient does not return a signed acknowledgement form to our facility within 30 days**, complete an acknowledgement form as follows: a. Fill out all the items listed in the box on top of the Acknowledgement form; b. Fill out the bottom half of the Acknowledgement Form, providing a clear, detailed explanation of why the patient did not sign the form and the efforts that were made in trying to obtain the patient's signature; c. File the completed Acknowledgement Form in the patient's medical record or patient admission/billing record in either paper or electronic format. ***(See NOTE below) 7. If unable to send the patient a Notice of Privacy Practices, do the following: a. Fill out all the items listed in the box on top of the acknowledgement form; b. Fill out the bottom half of the acknowledgement form, providing a clear, detailed explanation of why the patient did not sign the form and the efforts that were displayed in trying to obtain the patient's signature; c. File the completed Acknowledgement Form in the patient's medical record or patient admission/billing record in either paper or electronic format. ***(See NOTE below) 8. If a patient has an unsigned Acknowledgement Form in their medical record and contacts our facility later, attempt to follow the steps in **Situations A or B**, or repeat the steps in **Situation C**, as appropriate. ***(See NOTE below)	d. Form in the patient's medical record or patient admission/billing record in either paper or electronic format. ***(See NOTE below) 4. If the patient's condition does improve to the point where they can sign/understand the Acknowledgement Form, follow the steps in **Situation A & B**.***(See NOTE below) 5. If a patient has an unsigned Acknowledgement Form in their medical record and later is able to sign/understand an Acknowledgement Form, attempt to follow the steps in **Situations A, B, or C**, as appropriate. ***(See NOTE below)

Kohll'sRx must retain the Notice of Privacy Practices, including any changes to the notice, as well as the signed Acknowledgment Form for six years from the date of creation or the date when they were last in effect whichever is later. Documentation maintenance of the Acknowledgement Form may be in the form of a signature on a piece of paper, the electronic scanning of the paper into a computer system, or electronic signature. Furthermore, the written acknowledgement must be retrievable upon request from the patient or any external compliance-monitoring agency.

Applicable Regulations/Standards

- 45 CFR § 164.520(c) & (e)

ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

The privacy of your protected health information is important to us. We have provided you with a copy of our Notice of Privacy Practices. It describes how your health information will be handled in various situations. We ask that you sign this form to acknowledge you received a copy of our Notice of Privacy Practices. This includes the situation where your first date of service occurred electronically. If your first date of service with us was due to an emergency, we will try to give you this notice and get your signature acknowledging receipt of this notice as soon as we can after the emergency.

I received Kohll'sRx's Privacy Notice or was directed where to find it electronically.

_____ _____

Print Name **Unique Identifier**

_____ _____

Patient's Signature or Personal Representative's Signature **Date**

_____

If Personal Representative, describe relationship

For office use only:
Patient Name:_____
Filed electronically: ___Yes ___No

Kohll's staff should complete if Acknowledgement Form is not signed:

1. Does patient have a copy of the Privacy Notice? [ ] Yes [ ] No

2. If you answered "No" above, please explain why the patient did not sign an acknowledgement form and [PROVIDER'S] efforts in trying to obtain the patient's signature (check all that apply):

[ ] Patient Unable to Comprehend
[ ] Patient Communication Barrier
[ ] Legal Representative not Available
[ ] Other:_____
[ ] Patient/Legal Representative Left before Signature Obtained
[ ] Emergency Admission/Patient Not Present for Registration
[ ] Patient bypassed Registration – Not Available

3. Completed by:

_____ _____ _____

Workforce Member Signature Title Date

Patient Right to Access, Inspect, and Copy Protected Health Information (PHI)

It is the policy of Kohll'sRx to honor a patient's right of access to inspect and obtain a copy of their protected health information (PHI) in Kohll'sRx's designated record set, for as long as the PHI is maintained in compliance with HIPPA and Kohll'sRx's retention policy.

1. A patient must make a request to a staff member to access and inspect their protected health information. Whenever possible, this request shall be made in writing and documented on either the "Authorization for Disclosure" form or in the notes of the patient's health record.
2. Determination of accessibility of the information shall be based on:
    a. Availability of protected patient information (i.e., final completion of information, long term storage, retention practices, etc.)[4]
3. The organization must act within a reasonable period or within 30 days after receipt of the request when the PHI is on-site, and within 60 days when the PHI is off-site. One 30-day extension is permitted, if the organization provides the patient with a written statement of the reasons for the delay and the date by which the access request will be processed.
4. The organization must document and retain the designated record sets subject to access, and the titles of persons or offices responsible for receiving and processing requests for access.
5. The patient and the organization will arrange a mutually convenient time and place for the patient to inspect and/or obtain a copy of the requested PHI. Inspection and/or copying of PHI will be carried out within the organization with staff assistance.
6. The patient may choose to inspect the PHI, copy it, or both, in the form or format requested. If the PHI is not readily producible in the requested form or format, the organization must provide the patient with a readable hard copy form, or other form as agreed to by the organization and the patient.
    a. If the patient chooses to receive a copy of the PHI, the organization may offer to provide copying services. The patient may request that this copy be mailed.
    b. If the patient chooses to copy their own information, the organization may supervise the process to ensure that the integrity of the patient record is maintained.
7. Upon prior approval of the patient, the organization may provide a summary of the requested PHI.
8. The organization may charge a reasonable fee to produce copies or a summary of PHI, if the patient has been informed of such charge and is willing to pay the charge.
9. If upon inspection of the PHI the patient feels it is inaccurate or incomplete, the patient has the right to request an amendment to the PHI. The organization shall process requests for amendment as outlined in additional organizational policy/procedures addressing this patient right.
10. The organization must provide a written denial to the patient. The denial must be in plain language and must contain:
    a. The basis for the denial;
    b. A statement, if applicable, of the patient's review rights; and

[4] Comment: See Appendix B relating to access by individual.

c. A description of how the patient may complain to the organization or to the Secretary of Health and Human Services.

11. If access is denied because the organization does not maintain the PHI that is the subject of the request, and the organization knows where that PHI is maintained, the organization must inform the patient where to direct the request for access.
12. The organization must, to the extent possible, give the patient access to any other PHI requested, after excluding the PHI as to which the organization has grounds to deny access.
13. If access is denied on a ground permitted under (HIPAA) §164.524, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the organization to act as a reviewing official and who did not participate in the original decision to deny.
14. The patient must initiate the review of a denial by making a request for review to the organization. If the patient has requested a review, the organization must provide or deny access in accordance with the determination of the reviewing professional, who will make the determination within a reasonable period.
15. The organization must promptly provide written notice to the patient of the determination of the reviewing professional. See #10 above for denial requirements.

- "Checklist of Individual Rights Under HIPAA," Report on Medicare Compliance, April 25, 2002
- AHIMA Practice Brief: Patient Access and Amendment to Health Records, 2002
- Reinhart, Boerner, Van Deuren, Attorneys at Law
- 2002 WEDI – SNIP Security and Privacy Workgroup Privacy Policies and Procedures
- Wisconsin Statute 146.83.
- Chapter 146 HIPAA Privacy Standards Matrix

A patient must make a request to a staff member to access and inspect their protected health information. Whenever possible, this request shall be made in writing and documented on either the "Authorization for Disclosure" form or in the notes of the patient's health record.

HIPAA	Interface
HIPAA allows access upon request.	Follow HIPAA. No statement of informed consent is required for patient access. Only request for access is required.
HIPAA allows CE to require request to be in writing provided CE informs individual of such requirement.	CE may require request in writing and this requirement is at the discretion of the CE. CE must notify individual of "in writing" requirement.
Request made to CE.	CE designates who receives request.

This request shall be made in writing and documented on either the "Authorization for Disclosure" form or in the notes of the patient's health record.

HIPAA	Interface
There are no specific requirements for documentation of a disclosure to patient under the patient right of access other than documentation of the designated record sets that are subject to access and	State law controls. State law requires greater recordkeeping. Disclosures made to the individual must be documented as required by state law.

HIPAA	Interface
the titles of the persons/offices responsible for receiving and processing requests for access. HIPAA does not require that a CE provide an individual with an accounting of disclosures made to the individual.	
No requirement.	Location of the required documentation is at the discretion of the CE and is not regulated by law.

Determination of accessibility of the information shall be based on State and Federal laws.

HIPAA	**Interface**
Access to PHI about the individual in a designated record set with the following exceptions.	HIPAA provides a greater right of patient access to a greater amount of information. HIPAA will regulate the information available through the designated record set definition
Does not allow patient access to psychotherapy notes.	If psychotherapy notes are 51.30 records, 51.30 will control access. If psychotherapy notes are 146 records, access will be provided by state law, 146, superseding HIPAA.
Does not allow access to information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative proceeding	Follow state. Accessible by patient.
does not allow access to protected health information that is subject to CLIA or exempt from CLIA.	Follow state. Accessible by patient.
Unreviewable grounds for denial	Follow state. Disregard unreviewable process.
Reviewable grounds for denial.	Follow state. Disregard reviewable process.
Limits access to information maintained within the record set.	May limit access to what CE maintains/retains.
Limits access to information within the designated record set.	If state law provides greater access, state law will control.

The organization must act within 30 days after receipt of the request when the PHI is on- site, and within 60 days when the PHI is off-site. One 30-day extension is permitted, if the organization provides the patient with a written statement of the reasons for the delay and the date by which the access request will be processed.

HIPAA	**Interface**
Requires action within 30 days of receipt of request (b)(2)(i)	The HIPAA time limits will control unless the WI standard of reasonable notice may be deemed to be shorter and provide a greater right of access. Suggest HIPAA language and "upon reasonable notice," whichever is of shorter duration.
Allows 60 days from date of receipt of request if information is not maintained or accessible to CE on-site (b)(2)(ii)	As above
Allows 30-day extension to above if certain procedural steps are taken	As above

HIPAA	Interface
(b)(2)(iii)	

Remote Access

To establish guidelines and define standards for remote access to Kohll'sRx's information resources (networks, systems, applications, and data including but not limited to, electronic protected health information (ePHI) received, created, maintained, or transmitted by the organization). Remote access is a privilege, and is granted only to remote users who have a defined need for such access, and who demonstrate compliance with Kohll'sRx's established safeguards which protect the confidentiality, integrity, and availability of information resources. These safeguards have been established to address HIPAA Security regulations including:

- Workforce Clearance Procedures [45 CFR §164.308(a)(3)(ii)(B)]
- Access Authorization [45 CFR §164.308(a)(4)(ii)(B-C)],
- Automatic Logoff [45 CFR 164.312(a)(2)(iii)],
- Supervision [45 CFR §164.308(a)(3)(ii)(A)],
- Termination Procedures [45 CFR §164.308(a)(3)(ii)(C)].
- Security Management Process (164.308a1i);
- Security Incident Procedures (164.308a6i-ii);
- Sanction Policy (164.308a1iiC); and
- Health Information Technology for Economic and Clinical Health Act (HITECH), revisions to 45 C.F.R. Parts 160, 162, & 164

Responsible for Implementation:

HIPAA Privacy/Security Officer

Applicable To:

All users who work outside of the Organization's environment, who connect to the organization's network systems, applications, and data, including but not limited to applications that contain ePHI, if applicable, from a remote location. Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

The purpose of this policy is to establish uniform security requirements for all authorized users who require remote electronic access to Kohll'sRx's network and information assets. The guidelines set forth in this policy are designed to minimize exposure to damages that may result from unauthorized use of Kohll'sRx's resources and confidential information. This policy applies to all authorized system users, including members of the workforce, business associates, and vendors, desiring remote connectivity to Kohll'sRx's networks, systems, applications, and data. Users are frequently categorized in one of these user groups:

1. **Workforce members with permanent remote access.** These users are often Information Services (IS), executive, or specific administrative staff, business staff, providers, or teleworkers who require 24-hour system availability and are often called upon to work remotely or who travel often. Their remote access offers the same level of file, folder, and application access as their on-site access.
2. **Workforce members with temporary remote access.** These users typically request short-term remote access due to an extended time away from the office most frequently as

a result of a short-term medical or family leave. Access for these users is typically restricted to only that which is necessary for task completion during time away from the office and may be limited.

3. **Contractors and Vendors offering product support with no access to PHI.** These users have varied access depending upon the systems needed for application or system support, but do not have access to any PHI in the applications or systems. These users access the system on an as needed, or as called upon basis for system troubleshooting.
4. **Contractors and Vendors offering product support and other Business Associates with access to PHI.** These users have varied access to PHI depending on the application or system supported and/or accessed. Appropriate Business Associate Agreements must be on file prior to allowing access, and all such access must be audited on a regular basis.

Key Definitions:

Defined Network Perimeter. Refers to the boundaries of the Kohll'sRx's internal computer network.

Electronic Protected Health Information (ePHI). Protected health information means individually identifiable health information that is: transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.[5]

Firewalls. A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A firewall is a set of hardware and/or related programs providing protection from attacks, probes, scans, and unauthorized access by separating the internal network from the Internet.

Information Resources. Networks, systems, applications, and data including but not limited to, ePHI received, created, maintained, or transmitted by the Kohll'sRx's.

Protected Health Information (PHI). Individually identifiable health information that is received, created, maintained, or transmitted by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual;
- The provision of health care to an individual;
- The past, present, or future payment for the provision of health care to an individual.

Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.[6]

Privileged Access Controls. Includes unique user IDs and user privilege restriction mechanisms such as directory and file access permission, and role-based access control mechanisms.

Remote Access. Remote access is the ability to gain access to a <Organization's> network from outside the network perimeter. Common methods of communication from the remote computer to Kohll'sRx's network includes, but is not limited to, Virtual Private Networks (VPN), web-based Secure Socket Layer (SSL) portals, and other methods which employ encrypted communication technologies.

Role-Based Access. Access control mechanisms based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on the least-privilege principle.

[5] 45 CFR § 164.503.
[6] § 164.502(f).

Teleworker. An individual working at home (or other approved location away from the regular work site) on an established work schedule using a combination of computers and telecommunications.

Virtual Private Network (VPN). A private network that connects computers over the Internet and encrypts their communications. Security is assured by means of a tunnel connection in which the entire information packet (content and header) is encrypted. VPN technology should use accepted standards of encryption, based, for example, on FIPS 140-2.

Web-based Portal. A secure website offering access to applications and/or data without establishing a direct connection between the computer and the hosting system. Web-based portals most often use 128-bit or higher SSL encryption.

Workforce Member. Workforce means employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether they are paid by the covered entity.[7]

1) Gaining Remote Access
   A) Refer to "System Access" policy for definition of roles preapproved for remote access.
   B) Workforce members shall apply for remote access connections by completing a "System Access Request" form (refer to the System Access Policy). Remote access is strictly controlled and made available only to workforce members with a defined business need, at the discretion of the workforce member's manager, and with approval by the Security Officer or designee.
   C) The workforce member is responsible for adhering to all Kohll'sRx's policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for Kohll'sRx.
   D) Business associates, contractors, and vendors may be granted remote access to the network, provided they have a contract or agreement with Kohll'sRx which clearly defines the type of remote access permitted (i.e., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the Security Officer and/or legal department before remote access will be permitted. Remote access is strictly controlled and made available only to business associates and vendors with a defined business need, at the discretion of and approval by the Security Officer or designee.
   E) All users granted remote access privileges must sign and comply with the "Information Access & Confidentiality Agreement" (refer to the HIPAA COW System Access Policy) kept on file with the Human Resources Department or other department as determined by the Kohll'sRx's.
   F) It is the remote access user's responsibility to ensure that the remote worksite meets security and configuration standards established by Kohll'sRx's. This includes configuration of personal routers and wireless networks
2) Equipment, Software, and Hardware
   A) The organization will not provide all equipment or supplies necessary to ensure proper protection of information to which the user has access. The following assists in defining the equipment and environment required. (Edit these lists as appropriate.)
      i) Organization Provided:

[7] 45 CFR § 164.103.

(1) Encrypted workstation
(2) Cable lock to secure the workstation to a fixed object
(3) If using a VPN, an organization issued hardware firewall
(4) If printing, an organization supplied printer
(5) If approved by the organization's Security Officer, an organization supplied phone

ii) User Provided:
(1) Broadband connection and fees
(2) Paper shredder
(3) Secure office environment isolated from visitors and family
(4) A lockable file cabinet or safe to secure documents when unattended

B) Remote users will be allowed access using equipment owned by or leased to the entity, or through the use of the workforce member's personal computer system provided it meets the minimum standards developed by Kohll'sRx's, as indicated above. (The Organization must determine minimum standards based on FIPS 140-2 or its successor.)

C) Remote users utilizing personal equipment, software, and hardware are:
i) Responsible for remote access. Kohll'sRx's will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss.
ii) Responsible for remote access used to connect to the network and meeting Kohll'sRx's requirements for remote access. [Each organization will need to insert appropriate detail for remote access requirements.]
iii) Responsible for the purchase, setup, maintenance, or support of any equipment not owned by or leased to Kohll'sRx's.

D) Continued service and support of Kohll'sRx's owned equipment is completed by IS workforce members. [Each organization will need to insert appropriate detail for remote access requirements]. Troubleshooting of telephone or broadband circuits installed is the primary responsibility of the remote access user and their Internet Service Provider. It is not the responsibility of Kohll'sRx's to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by Kohll'sRx's.

E) The ability to print a document to a remote printer is not supported without the organization's approval. Documents that contain confidential business or ePHI shall be managed in accordance with the Kohll'sRx's confidentiality and information security practices.

3) Security and Privacy

A) Only authorized remote access users are permitted remote access to any of Kohll'sRx's computer systems, computer networks, and/or information, and must adhere to all Kohll'sRx's policies.

B) It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect from Kohll'sRx's network when access is no longer needed to perform job responsibilities.

C) Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to access any ePHI or organizationally sensitive information.

D) Remote access users are automatically disconnected from the Kohll'sRx's network when there is no recognized activity for **[**insert organizational criteria, such as 15 minutes].

E) It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their user's name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.

F) Remote access users must take necessary precautions to secure all Kohll'sRx's equipment and proprietary information in their possession.

G) Virus Protection software is installed on all Kohll'sRx's computers and is set to update the virus pattern daily. This update is critical to the security of all data, and must be allowed to complete, i.e., remote users may not stop the update process for Virus Protection, on organizations or the remote user's workstation.

H) A firewall shall be used and may not be disabled for any reason.

I) Copying of confidential information, including ePHI, to personal media (hard drive, USB, cd, etc.) is strictly prohibited, unless the organization has granted prior approval in writing.

J) Kohll'sRx's maintains logs of all activities performed by remote access users while connected to Kohll'sRx's network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Accounts that have shown no activity for **[**insert organizational criteria, such as 30 days] will be disabled.

K) Electronic Data Security

i) Backup procedures have been established that encrypt data moved to an external media. If there is not a backup procedure established or if Kohll'sRx's has external media that is not encrypted, contact the IS Department or Security Officer for assistance.

ii) Transferring data to the Kohll'sRx's requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Users may not circumvent established procedures when transmitting data to the Kohll'sRx's.

iii) Users may not send any ePHI via e-mail unless it is encrypted. If PHI or ePHI needs to be transmitted through email, IS or the Security Officer must be contacted to ensure an approved encryption mechanism is used.

L) Paper document security

i) Remote users are discouraged from using or printing paper documents that contain PHI.

ii) Documents containing PHI must be shredded before disposal consistent with the "Device, Media and Paper Record Sanitization for Disposal or Reuse" policy and procedure.

4) <u>Enforcement</u>

A) Remote access users who violate this policy are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract. Termination of access by remote users is processed in accordance with Kohll'sRx's termination policy.

B) Remote access violations by Business Associates and vendors may result in termination of their agreement, denial of access to the Kohll'sRx's network, and liability for any damage to property and equipment.

Applicable Standards and Regulations:

- 45 CFR §164.312(a)(2)(iii) – HIPAA Security Rule Automatic Logoff
- 45 CFR §164.308(a)(3)(ii)(B) – HIPAA Security Rule Workforce Clearance Procedures
- 45 CFR §164.308(a)(3)(ii)(C) – HIPAA Security Rule Termination Procedures
- 45 CFR §164.308(a)(4)(ii)(B-C) – HIPAA Security Rule Access Authorization

Federal Information Processing Standard (FIPS) Publication 140-2
Department of Health and Human Services, Centers for Medicare & Medicaid Services (CMS),"HIPAA Security Guidance" (12/28/2006)
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf
SANS (Sysadmin, Audit, Network, Security) Institute
The Health Information Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act of 2009 (ARRA)

Patient/Individual Right to Request Confidential Communications

Patients/Individuals have the right to request restrictions on how and where their protected health information (PHI) is communicated. To comply with HIPAA Privacy Rule sections 164.502 and 164.522(b) regarding confidential communications, Kohll'sRx must permit patients/individuals to request to receive communications of PHI by alternative means or at alternative locations.

1. Kohll'sRx may require that patient/individual requests to receive communications of PHI by alternative means or at alternative locations be made in writing. Writing requirements are detailed in the Notice of Privacy Practices.
2. Patients/Individuals may request to receive communications of PHI by alternative means or at alternative locations at the time of admission, visit, or at any time during the course of their care.
3. Patient/Individual requests may be made to any member of Kohll'sRx's staff.
4. When patients/individuals make a request, either formally or informally, the staff member receiving the request should document it in writing.
5. Kohll'sRx must accommodate patient/individual requests that are reasonable.
6. Kohll'sRx determines whether a request is "reasonable" based solely on the administrative difficulty of accommodating the request. Kohll'sRx should establish policies and procedures to determine whether a request is "reasonable."
7. Kohll'sRx may not require that patients/individuals provide a reason for their request.
8. Kohll'sRx may not deny requests based on its perception of whether patients/individuals have a good reason for making the request. A patient's/individual's reason for making a request cannot be used to determine whether the request is reasonable.
9. Kohll'sRx may deny patient/individual requests if:
    a. The patient/individual does not specify an alternative address or other method of contact.

    b. The patient/individual does not provide information as to how payment, if applicable, will be handled.
10. If Kohll'sRx grants a patient's/individual's request, the decision must be documented by maintaining a written or electronic record of the action taken.
11. If Kohll'sRx grants a patient's/individual's request, it provides appropriate staff with the communication requirements and requires staff to adhere to them.

Patient Privacy-related Complaints

Kohll'sRx shall provide a process for the patient to file a complaint if the patient feels his or her privacy rights have been violated. The patient may also file a complaint concerning Kohll'sRx's privacy policies and procedures, even without alleging a violation of rights. Kohll'sRx shall designate a contact person or office responsible for receiving complaints and shall establish a process for receiving, investigating, and responding to patient complaints. The patient complaint process shall be described in Kohll'sRx's notice of patient privacy. Kohll'sRx also recognizes the patient's right to file a complaint with the federal Department of Health and Human Services. Kohll'sRx shall cooperate with a federal investigation of the patient's complaint. Any intimidation of or retaliation against patients, families, friends, or other participants in the complaint process is prohibited. Employees who violate this policy are subject to disciplinary action, up to and including termination. If the patient's rights have been violated, employees who violated those rights are subject to disciplinary action, up to and including termination. Kohll'sRx shall mitigate, to the extent feasible, any known harmful effects of the violation.

A. Filing a Complaint
    1. A patient may call, write, or present in person to the Privacy/Security Officer or designated person the alleged privacy violation or complaint.
B. Investigation of Complaint
    1. The Privacy/Security Officer or designated person will facilitate the investigation of the complaint.
C. Translators, interpreters, and readers who meet the communication needs of the patient may be provided during the complaint process.
D. Patients are permitted to have a representative of their choice to represent their interests during the complaint process.
E. Occurrences representing potential liability claims will be referred to Risk Management. Patients who request an outside agency to review their complaint may contact the Secretary of the federal Department of Health and Human Services at 200 Independence Avenue, S.W.; Washington, DC 20201, or reach the Secretary by phone at (202) 690-7000.
F. Documentation
    1. All complaints received must be documented.
    2. All complaint dispositions must be documented.
    3. The documentation must be retained for six years.

It is the policy of Kohll'sRx to honor a patient's or a patient's legal representative right to request restrictions on how his or her protected health information (PHI) is used and/or disclosed for the purposes of treatment, payment, and/or healthcare operations and for disclosures permitted under 164.510(b).

1. The Kohll'sRx will inform patients of their right to request restrictions on how their PHI is used and/or disclosed for treatment, payment, and healthcare operations in their published "Notice of Privacy Practices."
2. The patient has the right to request restrictions. Kohll'sRx may require the request to be in writing (Attachment A). Kohll'sRx's Privacy Officer (or designee) reviews each request and makes a determination of final actions. Effective February 18, 2010, the American Recovery and Reinvestment Act (ARRA) allows a patient the right to request that a healthcare provider must comply with the patient's request for restriction of disclosure to

a health plan for purposes of payment or healthcare operations when the patient health information pertains to a service for which the healthcare provider has been paid in full by the patient "out of pocket."

3. Kohll'sRx may agree to a patient's request for restrictions on the use and disclosure of their PHI if the request is determined to be reasonable and, in the patient's, best interests.

When a Request for Restriction(s) Is Accepted:

4. Kohll'sRx will notify the patient of the approval of the request. (See Attachment B for sample letter).
5. Kohll'sRx will inform the patient of any potential consequences of the restriction.
6. Kohll'sRx will inform the patient that the Kohll'sRx will comply with the agreed restriction with the following exceptions:
   a. In an emergency treatment situation when Kohll'sRx may use or disclose information to a health care provider for providing treatment. Kohll'sRx will request the emergency treatment provider not further use or disclose the information.
   b. The restrictions are terminated by either Kohll'sRx or the patient.
   c. If restrictions prevent uses or disclosures permitted or required under 164.502(a)(2)(ii), 164.510(a) or 164.512.
7. If the agreed upon restriction hampers treatment, the Kohll'sRx may ask the patient to modify or revoke the restriction. Kohll'sRx may require written agreement to the modification/ revocation or document the patient's oral agreement.
8. A notice of restriction will be made in writing in the patient's medical record and/or identified in an appropriate field in the computerized patient information system.
9. Kohll'sRx will notify separately any other departments to which the restriction may apply (e.g., marketing, public relations, administration, foundation, etc.) and if necessary, ensure that the patient's name is removed from all applicable mailing lists.
10. Kohll'sRx will notify separately any other business associates to which the restriction may apply.
11. The Kohll'sRx will not use or disclose PHI inconsistent with the agreed restriction, nor will its business associates until the restriction is terminated either by Kohll'sRx or the individual.
12. The Kohll'sRx will restrict use and/or disclosure of PHI consistent with the status of the restriction in effect on the date it is used or disclosed.

When a Request for Restriction Is Denied:

13. If the request for restriction is denied, Kohll'sRx notifies the patient.

Termination:

14. The patient must request in writing to terminate the restriction.
15. If the Kohll'sRx wants to terminate the agreement, the patient must agree to the termination in writing or an oral agreement must be documented. The termination will be effective with respect to PHI created or received after the patient was notified by Kohll'sRx.

Record Retention:

16. All documentation associated with this procedure will be maintained in writing or in electronic format for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

Minors' Privacy Rights

It is the policy of Kohll'sRx to recognize the rights of minors and their parents, legal guardian, or other legally authorized representative to access, inspect and receive copies of their protected health information in compliance with state and federal regulations. At the state level, minors have many rights with regard to consent to their own care in certain situations. However, it is important to understand that these rights may not extend to their ability to control access to their protected health information.

Minor: A minor is a person under the age of 18 years and reliant upon parental support and control. Generally, minors do not have the authority to grant consent or refuse care, with the exceptions outlined below. [Insert Organization's Name]

Emancipated Minor: In most states, lawful marriage is the only circumstance that is statutorily recognized, as a general matter, as grounds for emancipation of a minor. Once emancipated, the minor obtains the legal capacity of an adult.[8] The burden should be placed on the minor to show emancipation. If doubt exists regarding emancipation, parental consent should be secured in addition to the consent of the minor.

Generally, the age at which a minor obtains the right of access to their healthcare information is 18 because at that age the individual is no longer deemed a minor. Several specific state laws grant a minor the right of access to their healthcare information and this right often directs a minor's statutory right to consent to treatment; however, there are exceptions.

The federal Privacy Rule, as delineated in the appendix, also grants a minor access to their healthcare information but as a rule, only through the consent of a legally authorized representative. The federal Privacy Law delineates a process for interfacing the federal and state law when they are different.[9] The federal law allows the state law to preempt and control when state law provides a greater right of access to the individual in relation to their healthcare information. Therefore, state law will control when a minor is provided a greater right of access. Federal law requires that healthcare providers have in place and implement policies and procedures to ensure patients' right to access, inspect and copy protected health information (§164.524). Under the federal Privacy Rule, an individual has the right to access their information in all but a limited number of situations. When federal law limits the right of access interface with state law is required and the law that provides the individual the greater right of access controls. For instance, the Privacy Rule allows denial of access to specific types of healthcare information with or without a review of denial.[10] When state law provides access to a minor or legally authorized individual and the Privacy Rule does not, state law will control. When processing a minor's request for access and there is no statutory authority allowing a minor under the age of 18 access, the authorization for access will be obtained from the minor's legally authorized representative.

The Privacy Rule defers to state law for the definition of a legal representative. State law generally recognizes the minor's parent, guardian, or legal custodian as the legally authorized representative. However, a termination of parental rights or a denial of physical placement by a court of law will affect the status of a parent in relation to a minor. In addition, other specific statutes may define the legal representative of a minor differently. Therefore, it will be necessary to determine what law is controlling to determine who may be the legally authorized representative for a minor regarding access.

[8] When remaining under complete parental support, emancipation may be arguable.
[9] 45 CFR §160 Subpart B Preemption of State Law
[10] 45 CFR §164.524

A minor, or legally authorized representative, must make a request to a covered entity to access and inspect their protected health information. Whenever possible, this request shall be made in writing. The federal Privacy Rule allows the requirement of a written request for access if the individual has received notice of the written requirement in the "Notice of Privacy practices." The request for access may be documented on either the "Authorization for Disclosure" form or in the notes of the patient's health record. The minor's rights to access should be determined based on the following statutory information and whether they are authorized to make the written request without parental/guardian consent.

The law of release of minor records is a matter of some ambiguity and controversy, particularly regarding the circumstances justifying allowing a minor to make decisions about disclosure of protected health information in the absence of parental consent, or to deny parental access to minor records. While the general rule is that parental consent is required until the patient is eighteen years of age, there may be extenuating circumstances justifying a variance from this rule. Legal counsel should be contacted for case-by-case determination of whether such circumstances are present.

1. A parent, legal guardian or other legally authorized representative has the right to access a minor's protected health information on behalf of the minor, unless.
    A. The statutes provide protection from access to the minor's protected health information;
    B. The parent has been denied periods of physical placement with the minor; or
    C. In the case of minors age 14 or older, the minor requests no disclosure of their mental health records.
2. A parent, legal guardian or other legally authorized representative has the right to access a minor's protected health information on behalf of the minor, even where the parent or guardian's consent was not required for treatment, unless
    A. The statutes provide protection from access to the minor's protected health information;
    B. The parent has been denied periods of physical placement with the minor; or
    C. In the case of minors age 14 or older, the minor requests no disclosure of their mental health records.
3. A healthcare provider reserves the right to limit disclosure of protected health information to a minor's parent or guardian if, in the provider's professional judgment, they believe the minor would be in imminent danger if the information was released.
4. The parent's right of access terminates when the minor becomes emancipated or reaches the age of majority.[11] If doubt exists regarding emancipation, parental authorization should be secured in addition to the authorization of the minor. Once a minor becomes emancipated, or reaches the age of majority, the individual has the right to access and

[11] If an authorization is signed by a parent, who is the personal representative of the minor child at the time the authorization is signed, the covered entity may rely on the authorization for as long as it is a valid authorization, in accordance with § 164.508(b). A valid authorization remains valid until it expires or is revoked. This protects a covered entity's reasonable reliance on such authorization. The expiration date of the authorization may be the date the minor will reach the age of majority. In that case, the covered entity would be required to have the individual sign a new authorization form to use or disclose information covered in the expired authorization form (Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules, and Regulations 82651).

authorize to disclosure of protected health information. This includes access to and disclosure of information created while the individual was a minor.

5. The PHI of minors prior to an adoption process is not available for disclosure by the healthcare provider. Requests for access to the PHI of a minor prior to an adoption shall be referred to the respective state's adoption record search agency. Requests for PHI post-adoption shall be processes in accordance with the organization's disclosure of PHI policies.
6. A healthcare provider may disclose a minor's/student's immunization information to a school or daycare upon written or verbal request. Parental or student permission is not required for disclosure. Immunization information may be provided between vaccine providers, including the local health department, without the consent of the parent or student.
7. Documentation of disclosure to the individual is required under some state laws. To maintain consistency and compliance in practice, it is recommended that the following be documented when disclosing healthcare information to the patient: the time and date of request, the name of the inspecting person and the identity of the records released.

Federal Privacy Rule – Access and Denial of Access

An individual has the right to access their information in all but a limited number of situations, which include:

- Psychotherapy notes;
- Information compiled in anticipation of or use in a civil, criminal, or administrative action or proceeding;
- Protected health information subject to the Clinical Laboratory Improvements Amendment (CLIA) of 1988.
- Protected health information exempt from CLIA, pursuant to 42 CFR 493.3(a)(2). In other words, protected health information generated by 1) facilities or facility components that perform testing for forensic purposes; 2) research laboratories that test human specimens but do not report patient-specific results for diagnosis, prevention, treatment, or the assessment of the health of individual patients; 3) laboratories certified by the National Institutes on Drug Abuse (NIDA) in which drug testing is performed that meets NIDA guidelines and regulations.

In the situations above, the covered entity may deny the individual access without providing an opportunity for review.

A covered entity may also deny an individual access without providing an opportunity for review when:

- The covered entity is a correctional institution or a healthcare provider acting under the direction of the correctional institution and an inmate's request to obtain a copy of protected health information would jeopardize the individual, other inmates, or the safety of any officer, employee, or other person at the correctional institution, or a person responsible for transporting the inmate;
- The individual, when consenting to participate in research that includes treatment, agreed to temporary denial of access to protected health information created or obtained by a healthcare provider in the course of research, and the research is not yet complete;
- The records are subject to the Privacy Act of 1974 and the denial of access meets the requirement of that law;

- The protected health information was obtained from someone other than a healthcare provider under a promise of confidentiality and access would likely reveal the source of the information.

A covered entity may also deny an individual access under the following circumstances, provided that the individual is given a right to have such denials reviewed:

- A licensed healthcare professional has determined that the access is likely to endanger the life or physical safety of the individual or another person;
- The protected health information refers to another person who is not a healthcare provider, and a licensed healthcare professional has determined that the access request is reasonably likely to cause substantial harm to such other person;
- The request for access is made by the individual's personal representative and a licensed healthcare professional has determined that access is reasonably likely to cause substantial harm to the individual or another person.

Detailed requirements for denial review are outlined in Section 45 CFR, Section 164.524.

Communication of PHI

The purpose of the Communications Policy is to provide policies and procedures to safeguard and protect the privacy of Protected Health Information (PHI) while using various mediums of communications. This policy has generalized guidelines and procedures that can be associated with all mediums of communications, and contains specific procedures due to the different handling of the mediums within a "Communication Matrix." This is an all-inclusive overview of general communication practices that may need to be broken down into separate policies, based on organizational needs.

PHI can be communicated through various mediums. To comply with the HIPAA Privacy Rule section 164.530 (c)(1) regarding safeguards, and the HIPAA Security Rule section 164.306(a) requiring the safeguarding of the confidentiality, integrity, and availability of electronic PHI (ePHI) an organization creates, receives, maintains, or transmits, the Kohll'sRx must have in place appropriate administrative, technical, and physical safeguards to protect PHI. It is the policy of Kohll'sRx to ensure that PHI is protected from misuse, loss, tampering, or use by unauthorized persons. This policy addresses the safeguarding of PHI received, created, used, maintained, and/or transmitted via the communication mediums listed using minimum necessary requirements for disclosures of PHI to personnel, patients and their personal representatives, other covered entities, public health officials, business associates, etc. set forth by federal, state, and local laws (refer to Kohll'sRx's Release of Information Policy). Verification of identity is attained in accordance with the Identity Verification Policy prior to release of PHI. Accounting of disclosures of PHI is maintained in compliance with Kohll'sRx's Policy. Transmission of ePHI over the organization's own network is managed with internal controls such as unique user ID and Password authentication (refer to System Access Policy).

Definitions

Encryption: the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.

• The provision of health care to an individual.
• The past, present, or future payment for the provision of health care to an individual.

Communication will be clear, concise, and professional. Emotional content, such as anger, sarcasm, harsh criticism, irony, incriminating remarks, and libelous references to third parties is not allowed. Employees should not expect communications they send to be private. Any material sent via Kohll'sRx's equipment is the property of Kohll'sRx. Any violations of this policy will be referred to human resources for disciplinary action.

General Public Information:

Any information that can be given to the general public and can be distributed outside of the Kohll'sRx without any risk, through the various mediums. This is often general information about the Kohll'sRx for marketing or product purposes.

Internal Information Within the Kohll'sRx:

Information that will not seriously impact or adversely affect Kohll'sRx if disclosed about patients, employees or business associates without proper consent or unauthorized disclosure. This may be information such as directories with phone listings, policy manuals that do not disclose PHI of individual patients, and patient educational information.

Non-sensitive and/or Non-urgent PHI:

PHI that can be given by various media, (refer to Kohll'sRx's Release of Information Policy). This information may be used internally within Kohll'sRx and received by the patient, guardian, and/or authorized personal representatives (refer to Kohll'sRx Release of Information Policy for appropriate release processes). Unauthorized disclosure could adversely impact the Kohll'sRx, patients, employees, and business associates. The following are examples:

- Prescription refills,
- Instructions on how to take medications or apply dressings,
- Appointment scheduling,
- Appointment reminders,
- Normal test results (other than HIV test results) with interpretation and advice,
- Care and treatment recommendations,
- Pre- and postoperative instructions,
- Insurance and billing questions,
- As a secondary means of attempting to have patients call the provider to discuss important test results and/or prognosis of a condition,

Sensitive and/or Urgent Confidential PHI:

Sensitive and/or urgent confidential PHI that is intended strictly for use within Kohll'sRx and disclosed only to patients or other entities as required by law (refer to Kohll'sRx's Release of Information Policy). Unauthorized disclosure could seriously and adversely impact Kohll'sRx , patients, employees, and business associates. Obtain an appropriate authorization for disclosures of PHI in this capacity. The following are examples:

- STD and HIV test results and/or treatment,
- First means of notification for confusing or abnormal diagnostic results
- Mental health issues,
- Drug and alcohol abuse and/or treatment,
- Child abuse and/or neglect,
- Domestic abuse,

- Peer review or risk management information
- For marketing and fundraising purposes except when allowed by law (refer to Kohll'sRx Marketing and Fundraising policies), and exercise caution for urgent/time sensitive matters.

The following Communication Matrix shows specific procedures in handling the various mediums of communicating information.

CLASSIFICATION OF INFORMATION FOR Kohll'sRx				
	General Public Information	**Internal Information**	**Non-sensitive and/or Non-urgent PHI** • Active measures taken to prevent the unauthorized disclosure of information from being released • If patient has notified Kohll'sRx by which means to give PHI, must be noted in their medical record, and adhered to • Verification of identity must be attained in accordance with the Identity Verification Policy • Document the release in accordance with the Accounting of Disclosures Policy	**Sensitive and/or Urgent Confidential PHI** • This information may not be released without a separate signed authorization for releasing this specific information • If patient has notified Kohll'sRx by which means to give PHI, must be noted in their medical record, and adhered to • Verification of identity must be attained in accordance with the Identity Verification Policy • Document the release in accordance with the Accounting of Disclosures Policy
Risk Impact	• None	• No serious or adverse effect	• Could result in adverse impact or have possible penalties applied	• Likely have a serious adverse impact. Penalties very likely to occur and could result in loss of business
1. Oral Mediums of Communication **a. Conversations** **b. Telephone** **c. Cell Phone** **d. Answering Machines** (refer to Appendix 1) **e. Overhead Pages** **f. Lobby Announcements**	• No specific precautions	• Reasonable measures should be taken	• Conduct PHI in private settings and use lowered voices, avoiding public areas whenever possible. • If a patient name is needed, first name only basis (when possible) • Do not use a speakerphone for discussion of PHI nor retrieval of voice mail (unless in a private, closed office) • Limit discussions of PHI using a cell phone. Consider that older cell phones are not secure. • Refer to Appendix 1 for leaving messages on an answering machine • Pages and announcements are used only to call the operator back	• Discuss PHI in a controlled manner to limit being overheard, such as in an enclosed area • If a patient name is needed, first name only basis (when possible) • Do not use a speakerphone for discussion of PHI nor retrieval of voice mail (unless in a private, closed office) • Limit discussions of PHI using a cell phone. Consider that older cell phones are not secure. • Refer to Appendix 1 for leaving messages on an answering machine • Pages and announcements are used only to call the operator back

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
2. Mail **a. Internal** **b. External**	• No specific precautions	• Information of this nature should be out of the public areas and not accessible by anyone else, but employees.	• Information being sent meets the minimum necessary requirement for disclosure • Authorized, trained personnel should handle all mail • Clearly label with recipient's name and address information is correct • Mailing item is labeled with Confidential • Tracking mechanism is recommended for external mail • Store all unattended mail in a closed, secure area • Place all types of media containing any form of phi in secured, confidential envelopes and/or containers (internal & external) • Return address on external mail consists of Kohll'sRx name only. Envelope will not contain the department's name, provider's name (unless this is the name of the organization, nor the identity of the enclosed information. For tracking purposes, internal codes may be included on envelopes if it does not in any way relinquish the identity of the department and/or provider to anyone outside of Kohll'sRx	• Information being sent meets the minimum necessary requirement for disclosure • Authorized, trained personnel should handle all mail • Clearly label with recipient's name and address information is correct • Mailing item is labeled with Restricted Confidential • If external, delivery of information and tracking mechanisms is required (FEDEX, messenger, certified, etc.…) • Store all unattended mail in a closed, secure area • Place all types of media containing any form of PHI in secured, confidential envelopes and/or containers (internal & external) • Return address on external mail consists of Kohll'sRx name only. Envelope will not contain the department's name, provider's name (unless this is the name of the organization, nor the identity of the enclosed information. For tracking purposes, internal codes may be included on envelopes if it does not in any way relinquish the identity of the department and/or provider to anyone outside of Kohll'sRx
3. Faxes	• Located in a secure area	• Located in a secure area out	• Located in an area not accessible by the public	• Located in an area not accessible by the public

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
	out of the general public • Use a coversheet with confiden tiality statement • Use reasonable efforts to dial correct number • When using a means to store fax numbers, verify the number with the receiver	of the general public • Use a coversheet with confidentiality statement • Use reasonable efforts to dial correct number • When using a means to store fax numbers, verify the number with the receiver	• Coversheet with confidentiality statement used • Use reasonable efforts in dialing correct number (i.e. testing number before sending phi), preference to using pre-programmed, labeled numbers • When using a means to store fax numbers, verify the number with the receiver • Only personnel with access to restricted area may access these faxes (review Kohll'sRx's Minimum Necessary Policy). Trained workforce member routinely checks fax machine and distributes to appropriate personnel • Faxes transmitted in error: contact person who received the fax to verify destruction of the fax and notated in patient's medical record. Report the breach to the Privacy Officer • Utilize a mechanism to ensure that the transmission went to the intended recipient (Fax logs, verification by phone, etc. If you receive a fax in error, immediately inform the sender and destroy the information received • Consider storing faxes in a queue until staffed.	• Coversheet with confidentiality statement used • Use reasonable efforts in dialing correct number (i.e., testing number before sending phi), preference to using pre-programmed, labeled numbers • When using a means to store fax numbers, verify the number with the receiver • Call prior to faxing to notify recipient of expected confidential fax • Information is immediately routed to appropriate personnel • Only personnel with access to restricted area may access these faxes (review Kohll'sRx's Minimum Necessary Policy). Trained workforce member routinely checks fax machine and distributes to authorized personnel • Faxes transmitted in error: contact person who received the fax to verify destruction of the fax and notated in patient's medical record. Report the breach to the Privacy Officer. • Utilize a mechanism to ensure that the transmission went to the intended recipient (Fax logs, verification by phone, etc.…) • If you receive a fax in error, immediately inform the sender and destroy the information received • Consider storing faxes in a queue until staffed.
4. E-mail **a. Refer to the**	• E-mails may be used for business	• E-mails may be used for business purposes only	• Prior to sending an e-mail to a patient a signed patient E-mail Informed Consent Form is received, filed in	• Prior to sending an e-mail to a patient a signed patient E-mail Informed Consent Form is received, filed in

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
System Access Policy **b. Refer to the E-mail White paper** **c. Refer to Appen dix 4 guidelines for E-mailing PHI** **d. Refer to Appen dix 5 Sample Patient E-Mail Acceptance Form**	purposes only • Confidentiality statement attached to every email • Out-of- office replies are activated during absences of more than 48 hours.	• Information of this nature should be out in the public areas and not accessible by anyone else, but employees. • Confidentiality statement attached to every email • Out-of-office replies are activated during absences of more than 48 hours. • If the information is time-sensitive, verify receipt of email.	patient's medical record, and adhered to (refer to Appendix 5) • Always utilize Kohll'sRx's e-mail application • 128-bit encryption [164.312(a)(2)(iv) & 164.312(e)(2)(ii)] • Utilize only pre-stored addresses • Verify email address prior to storing the address • Use discrete, generic subject headers. Do not include the patient's name in the subject header • List sender's name, title, email address, telephone number, and party who patient may contact with further questions • Attach the Confidentiality statement to every email • Group emails will only be sent in the following situations when utilizing the bcc function: impending shutdown for network maintenance, technical difficulties, recent mail blackouts, new services, change of address and/or telephone number, and change in hours • If the information is time-sensitive, verify receipt of email. • Workforce member routinely checks emails and replies to messages within 48 hours of receipt • Copy of the email, including replies and receipt confirmations are filed in patient's medical records • Out-of-office replies with instructions on whom to contact for immediate assistance are activated during absences of more than 48 hours	patient's medical record, and adhered to (refer to Appendix 5) • Always utilize Kohll'sRx's e-mail application • 128-bit encryption [164.312(a)(2)(iv) & 164.312(e)(2)(ii)] • Utilize only pre-stored addresses • Verify email address prior to storing the address • Use discrete, generic subject headers. Do not include the patient's name in the subject header • List sender's name, title, email address, telephone number, and party who patient may contact with further questions • Attach the Confidentiality statement to every email • Group emails will only be sent in the following situations when utilizing the bcc function: impending shutdown for network maintenance, technical difficulties, recent mail blackouts, new services, change of address and/or telephone number, and change in hours. • If the information is time-sensitive, verify receipt of email. • Workforce member routinely checks emails and replies to messages within 48 hours of receipt • Copy of the email, including replies and receipt confirmations are filed in patient's medical records • Out-of-office replies with instructions on whom to contact for immediate assistance are activated during absences of more than 48 hours

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
Email Cont.….			• If PHI was sent to wrong recipient, notate and document this in the Patient's medical record. Report the breach to the Privacy Officer	• If PHI was sent to wrong recipient, notate and document this in the Patient's medical record. Report the breach to the Privacy Officer
5. PDA's Refer to the System Access policy	• No specific precautions	• Information of this nature should be out of the public areas and not accessible by anyone else, but employees.	• Password protection required, limit number of login attempts • 128-bit encryption [164.312(a)(2)(iv) & 164.312(e)(2)(ii)] • Antivirus software should be in place • Training to staff member with possession of PDA on situations that PDA is lost or stolen • Provide disaster recovery mechanisms • If information is not required to travel off-site or not used, then store PDA in a locked area that is out of site • Information contained in Kohll'sRx's system may only be downloaded onto a PDA owned by Kohll'sRx, not onto a user's personal PDA	• Password protection required, limit number of login attempts • 128-bit encryption [164.312(a)(2)(iv) & 164.312(e)(2)(ii)] • Antivirus software should be in place • Training to staff member with possession of PDA on situations that PDA is lost or stolen • Provide disaster recovery mechanisms • If information is not required to travel off-site or not used, then store PDA in a locked area that is out of site • Information contained in Kohll'sRx's system may only be downloaded onto a PDA owned by Kohll'sRx, not onto a user's personal PDA

	General Public Info.	Internal Information	Non-sensitive and/or Non-urgent PHI	Sensitive and/or Urgent Confidential PHI
6. Transporting Medical Records	• No specific precautions	• Information of this nature should be out of the public areas and not accessible by anyone else, but employees	• Utilize courier bags with a closure mechanism (ex. Velcro, taped, tote with a lid, etc.) • Documentation (Sign out sheet or tracking sheet) for all medical records that leave the facility. Date, who took the medical record, destination location, who received the medical record and a return date, should be on this form. • Medical records are to be promptly returned upon completion of use. • Utilize Kohll'sRx's courier service whenever possible. Cab or delivery service is only used as a last resort. If cab or delivery service is used, place the medical record in a sealed envelope or container. Request the receiver to contact the sender as soon as the chart arrives at the proper destination	• Utilize courier bags with a closure mechanism (ex. Velcro, taped, tote with a lid, etc.) • Documentation (Sign out sheet or tracking sheet) for all medical records that leave the facility. Date, who took the medical record, destination location, who received the medical record and a return date, should be on this form. • Medical records are to be promptly returned upon completion of use. • Utilize Kohll'sRx's courier service whenever possible. Cab or delivery service is only used as a last resort. If cab or delivery service is used, then place the medical record in a sealed envelope. Request the receiver to contact the sender as soon as the chart arrives at the proper destination

References

- 45 CFR 164.306
- 45 CFR 164.312(a)(2)(iv)
- 45 CFR 164.312(e)(2)(ii)
- 45 CFR 164.501
- 45 CFR 164.502
- 45 CFR 164.508
- 45 CFR 164.514 (d-f, h)
- 45 CFR 164.520(b)(1)(iii)(A)
- 45 CFR 164.522(a-b)
- 45 CFR 164.528
- 45 CFR 164.530(c)(1)
- Association of American Medical Colleges – E-mail host security standard sample
- Association of American Medical Colleges – Media and hardcopy protection and transportation standard sample
- American Medical Association – Guideline for Physician-Patient Electronic Communications (last updated 5/8/02)
- Journal of AHIMA – Practice Brief: E-mail Security (February 2000)
- SANS Institute – Securing PDAs in the Health Care Environment (09/06/02)
- HIMSS 2002 Conference – Handhelds, The Holy Grail of Healthcare (Presented by Neil Smithline, MD, FACP)
- Hawaii Health Information Corporation – Data Classification Policy

Minimum Necessary

The purpose of the Minimum Necessary Policy is to provide policies and procedures on the "minimum necessary" of Protected Health Information (PHI) as required by the HIPAA Privacy Regulations. It is to establish guidelines to implement the minimum necessary standard and to determine how the standard impacts the use, disclosure, and request of PHI. This policy and procedure will have generalized policies and procedures that can be associated with organizations. For some of those organizations that have only a small number of the workforce disclosing the PHI or handling the PHI, some of the policy and procedures in this document may not be necessary. Minimum Necessary is the process that is defined in the HIPAA regulations: *When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.* It is Kohll'sRx's policy to ensure the privacy and security of Protected Health Information (PHI) by limiting the use and disclosure of PHI to what is minimum or reasonably necessary to accomplish the intended purpose in the following three areas:

1. Uses and disclosures of PHI by Kohll'sRx's workforce/staff
2. Uses and disclosures made in response to requests for PHI from other organizations
3. Uses and disclosures when requesting PHI from other organizations

This standard applies to all PHI, regardless of its form, character or medium, including, but not limited to electronic, digital, film, tape, paper, or verbal.
HIPAA minimum necessary standard does not apply to the following six circumstances.

Disclosure to requests by a health care provider for treatment

1. Uses or disclosure made to the individual, as permitted in the HIPAA regulations
    a. An individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set (Please see policy and procedure regarding Designated Record Sets), except for:
        i. Psychotherapy notes;
        ii. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
        iii. Protected health information maintained by a covered entity that is:
            1. Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or
            2. Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).
2. Uses or disclosures made pursuant to an authorization
3. Disclosures made to the Secretary of the Department of Health and Human Services
4. Uses or disclosures as required by law, as outlined in §164.512(a, c, e, & f)
5. Uses or disclosures that are required for compliance with this rule

1. Routine and Non-routine Disclosures and Requests: The organization must distinguish routine or recurring disclosures and requests from non-routine or non-recurring disclosures and requests:

A. Routine Disclosures: These are disclosure of PHI made to another entity or requests for PHI made by this organization on a routine or reoccurring basis. For such disclosures or requests.
    i. The organization must implement policies and procedures that limit the amount of PHI disclosed or requested to the amount reasonably necessary to achieve the purpose of the disclosure or request.
    ii. The organization should consider discussing the minimum necessary with the organization responsible for major requests or disclosures to negotiate mutually agreeable disclosures. In this regard, the organizations involved should address:
        1. The types of protected health information to be disclosed;
        2. The types of persons who would receive the protected health information;
        3. The conditions that would apply to such access; and
        4. Standards for disclosures to routinely hired types of business associates (e.g., for medical transcription).

B. Non-routine Disclosures: These are disclosures made occasionally. The organization needs to determine criteria to limit PHI to what is reasonably needed to accomplish the purpose of the disclosure. Non-routine requests are evaluated on a case-by-case basis in accordance with the criteria developed by the organization to ensure minimum necessary.
    i. Develop reasonable criteria to limit the amount of information disclosed to the minimum necessary to accomplish the purpose of the disclosure; and
    ii. Use these criteria to review these disclosures on an ***individual basis***.

2. **Applying the Minimum Necessary Standard to PHI from Other Organizations**: The organization may rely on the judgment of the party requesting the disclosure as to the minimum necessary amount of information needed when the request is made by:
    A. A public official or agency for which a disclosure is permitted under section 164.512 of the Privacy Rule (uses and disclosures for which consent, authorization, or opportunity to agree or object is not required).
    B. Another covered entity (e.g., health care provider, clinic, health plan, etc.)
    C. A professional who is a workforce member or business associate of the organization, if the professional states that the amount requested is the minimum necessary; or.
    D. A researcher with appropriate documentation from an institutional review board or privacy boards.

    A party requesting the "entire medical record," must specifically justify the request as the minimum, or reasonable, amount necessary to meet the needs of the request (e.g., transfer of care, medical history of longstanding condition, etc.) before the organization will disclose the PHI.
3. **Applying the Minimum Necessary Standard When Requesting PHI from Other Organizations**: The organization must limit its requests for PHI to the minimum, or reasonable, amount necessary to accomplish the purpose of the request.
    Upon issuing a request for the "entire medical record," the organization specifically justifies the request as the minimum, or reasonable amount necessary to accomplish the purpose of the request (e.g., transfer of care, medical history of longstanding condition, etc.).
4. **Applying the Minimum Necessary Standard to the Organization/Workforce**:
    A. For uses of PHI that require access by the organization/workforce, the organization must identify:
        i. The person or classes of persons in the workforce who need access to PHI;
        ii. The category or categories of PHI to which access is needed, and
        iii. Any conditions appropriate to such access.
    B. The organization must have in place a process to determine the appropriate scope of the individual's access to PHI that includes:
        i. An assessment of individual's appropriate access to PHI performed by the responsible department director/supervisor and based on:
            1. Job description/position scope
            2. Need to know
            3. Patient care needs
            4. Administrative needs
        ii. Completion of access request form and/or agreement form by the individual and the individual's director/supervisor
        iii. Education and review conducted by the individual's director/supervisor, which covers the individual's responsibilities related to access and includes the minimum necessary standard, confidentiality, security, and the consequences of inappropriate access to PHI or breach of patient confidentiality.
    C. The organization should carry out periodic reviews of access levels to determine (If the organization is a small organization, this may not be necessary due to small staff):
        i. Changes in staff member position or scope of responsibilities, and
        ii. Changes in information available through information components

D. The organization must make reasonable efforts to limit the individual's access to PHI that is necessary to carry out their duties or on a "need-to-know" basis. Individuals with unrestricted access to PHI are limited to accessing information for which they are responsible for providing treatment or carrying out related operational duties (e.g., quality audits, infection control monitoring, risk management activities, utilization review, etc.).
E. Requests for access to PHI not routinely covered in the scope of the individual's position shall be reviewed by leadership (e.g., privacy officer, administration, HIM/IT director, etc.) to determine the nature of the request and the benefit of granted access. Access may be granted on a limited basis and time frame to accommodate the duration of the project. Examples of special requests might include:
    i. Research projects;
    ii. Grant applications;
    iii. Needs assessments;
    iv. Staff performance appraisal and monitoring; or
    v. Accreditor monitoring and evaluation
F. The organization should periodically monitor access to determine appropriateness of staff review of PHI. Tracking incidents of unauthorized access will increase the security of patient's health information and decrease the risk of privacy violations. Methods for auditing access might include:
    i. Conducting random spot-checks of patients to determine appropriateness of access;
    ii. Using exception reports to determine time of access, length of access, access to "confidential" or "VIP" patient PHI;
    iii. Reviewing "role-based" access by position and unit of assignment within the organization; or
    iv. Reviewing requests for and access to "hard copy" patient records.
G. Departments that are responsible for the administration of department-specific modules or information systems such as medication administration or dictation access must also periodically monitor access to determine appropriateness of staff access to PHI.
H. Position transfers that may involve different levels of access to PHI must be reviewed to determine the appropriate new scope of access. This review should be carried out by the

5. **Corrective Action:** Upon determination of inappropriate or unauthorized access to PHI by a staff member, the organization must determine the appropriate corrective action for the misconduct. Please refer to the organization's policy, "Policy Name," regarding failure to comply with privacy practices.

The following is a chart of methods of creating minimum necessary PHI:

Method of Handling PHI	How to create minimum necessary
Electronic	Create security mechanisms to monitor and limit access PHI based on the criteria listed under Uses and Disclosures of PHI within the Workforce/Staff Section 1
Paper	Black out any information not required by the disclosure request.
Verbal	Only disclose the information needed by the request made.

Charging for Copies and Summaries of PHI

The Health Insurance Portability & Accountability Act (HIPAA) of 1996 privacy regulations permits a covered entity to impose reasonable, cost-based fees for responding to requests made by

an individual (patient or legal representative) for copies of protected health information (PHI). The regulations limit the types of costs that may be imposed for providing access to PHI. Additionally, the inclusion of a copying fee is not intended to impede the ability of individuals to obtain copies of their PHI. If the patient has agreed to receive a summary or explanation of his or her PHI, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include cost associated with searching for and retrieving the requested information. State statutes may provide regulation of charges for different types of PHI requests made by an individual (patient or legal representatives) or other third parties. Certain State statutes allow the assessment of "reasonable" costs for record copies requested by individuals other than the patient. HIPAA is silent on copy charges for individuals other than the patient and therefore the state "reasonable" cost fee may be applied. Further copy cost regulation is currently pending and may require updating of this policy and procedure. In addition, other State statues, such as Workers Compensation may conflict with HIPAA regulations and so it is necessary to be aware of both the HIPAA regulations and the state statutes when responding to a request to determine where state statute may preempt HIPAA regulations.

- If an individual requests a copy of PHI, a covered entity may charge a reasonable, cost – based fee for the copying, including the labor and supply costs of copying.
  - If hard copies are made, this would include the cost of paper.
  - If electronic copies are made to a computer disk, this would include the cost of the computer disk.
- Covered entities may not charge any fees for retrieving or handling the information or for processing the request.
- If an individual requests that the information be mailed, the fee may include the cost of postage.
- If an individual requests an explanation or summary of the information provided, and agrees in advance to any associated fees, the covered entity may charge for preparing the explanation or summary.
- If an individual requests an "accounting of disclosures" to identify what PHI has been disclosed to others, the organization must provide the first accounting free in any 12-month period. Subsequent requests in the 12-month period can be charged a reasonable fee based on the organization's costs of providing an accounting. Before charging the fee, the organization must inform the patient and allow them the opportunity to withdraw or modify the request to avoid or reduce the fee.
- As a courtesy, health care providers may waive copy charges for the disclosure of PHI between providers. This practice is at the discretion of the provider.

Factors That May Impact the Cost of Responding to Release of Information Requests: Costs of providing copies of PHI may be impacted by a variety of factors. Charges may differ depending upon the party making the request. HIPAA does allow an organization to charge a reasonable, cost-based fee for copying PHI for the patient/legal guardian, including labor and supply costs; however, covered entities may not charge patients/legal guardians any fees for retrieving or handling the information or for processing the request. The following factors may impact the charges an organization may assess for copies of PHI: [12]

- Labor costs involved with ensuring authorization appropriateness
- Labor costs and software associated with logging of requests to a database
- Labor costs involved in physically retrieving the health information

[12] Dunn, Rose. "Copying Records: The Saga Continues." For the Record, 9, no. 7 (1997): 18-25

- Labor costs associated with refiling retrieved health information
- Labor costs associated with the physical copying of health information
- Expense costs for paper, toner, and equipment maintenance involved in copying
- Capital costs associated with acquiring copying equipment
- Handling expense involved in preparing a document for mailing
- Postal expense for mailing
- Expense associated with invoicing for copies
- Bad debt "write-off" expense
- "Non-billable" request expense
- Real estate costs of storage space and copier work space

Release of PHI to the Media

It is the policy of Kohll'sRx to ensure the privacy and security of protected heath information (PHI) of patients[13] and to ensure that release of PHI to the media is disclosed along the guidelines set forth in this policy and in the best interest of the patients served.

1. All requests for patient PHI made by the media shall be forwarded to the appropriate administrative office/department for review and response. Requests received after regular business hours shall be forwarded to the supervisor in charge for review and determination of appropriate response.
2. The supervisor may determine that administrative review and action is required and contact the administrator-on-call to consult and determine the appropriate response.
3. Kohll'sRx may only respond to a request for specific patient information from the media after receipt and verification of a patient authorization that complies with state and federal law.
4. Kohll'sRx cannot share information with the media on the specifics about sudden, violent, or accidental deaths, as well as deaths from natural causes, without the permission of the decedent's legal representative or spouse or in the event that neither of these parties survive a deceased patient, an adult member of the deceased patient's immediate family.
5. Kohll'sRx will strive to protect the privacy of the patient as well as ensuring the security of the patient. Where knowledge of a patient's location could potentially endanger the patient (i.e., the hospital has knowledge of a stalker or an abusive partner), no information of any kind will be disclosed to the media, including confirmation of the patient's presence at the facility.
6. Kohll'sRx must obtain written authorization from the patient for the following media-related activities:
    - **A.** Reporting of Admissions, Discharges and Births
    - **B.** Detailed statements (beyond "one-word") on the patient's condition.
    - **C.** Photographs/videotapes/other imaging or audio recordings of the patient
    - **D.** Interviews of the patient by media representatives
    - **E.** Interview of Kohll'sRx/patient's provider on the patient's condition
7. Kohll'sRx is not responsible for addressing inquiries that are made as a result of "public record." Matters of public record refer to situations that are reportable by law to public authorities, such as law enforcement agencies, the medical examiner/coroner or public

[13] All patients are equal; celebrities, public figures, public officials, and patients involved in matters of public record are not subject to different standards than other patients when it comes to organizational policies for releasing information to the media.

health officer. Inquiries made from media citing access as a matter of public record should be referred to the appropriate public authority.

8. When appropriate in disaster or mass casualty situations, Kohll'sRx may release general information to the media to help dispel public anxiety. Kohll'sRx may state the number of patients who have been brought to the facility by gender or age group (adults, children, teenagers, etc.). Examples might include:

A. The facility is treating four individuals because of the explosion.

B. The facility is treating six male adults because of a toxic chemical leak.

9. Whenever possible, Kohll'sRx shall select a spokesperson to handle media inquiries to restrict and control information shared with the public.

10. In disaster or mass casualty situations, Kohll'sRx shall strive to work effectively with the media balancing the release of general information with patient privacy rights. A location may be provided for the media to be contained, so that information can be released in a press conference format that does not compromise patient privacy or the facility's need for added security in disaster situations.

Use/Disclosure of PHI for Marketing Purposes

It is the policy of Kohll'sRx to secure an authorization to use or disclose protected health information (PHI) for marketing purposes in compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. [164.501, 164.508(a)(3)]

Per 164.501, marketing is defined as:

1) to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service; or
2) an arrangement involving a covered entity whereby PHI is disclosed by the covered entity in exchange for direct or indirect remuneration, so that the other entity or affiliate can make a communication that encourages the purchase or use of its own product or service.

The following are examples of situations that do not meet the definition of marketing:

1) Communications that are merely promoting good health and not about a specific product or service does not meet the definition of "marketing." So, mailings reminding women to get an annual mammogram, or with information about how to lower cholesterol, about new developments in health care like new diagnostic tools or about health or "wellness" classes, support groups and health fairs are permitted and not considered marketing.
2) Communications about government-sponsored programs do not fall within the definition of marketing. There is no commercial component to communications about benefits available through public programs. So covered entity is permitted to use/disclose PHI to communicate about eligibility for Medicare supplement benefits, or SCHIP.
3) Covered entities may make communications in newsletter format without authorization so long as the content of such does not fit the definition of "marketing."

Exceptions to the Scope of Marketing Activities so Authorization is not needed:

Marketing does not include:

1) oral or written communications that describe Kohll'sRx's network or covered services; or
2) communications about treatment for the patient; or

3) communications about case management or care coordination, or recommendations of treatment alternatives and care options, including health care providers or settings of care.

Procedure for Authorization to Use or Disclose PHI for Marketing Purposes:

1. Kohll'sRx will obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of a:
   b) face-to-face communication with the patient; or
   c) a promotional gift of nominal value provided by Kohll'sRx.
2. If the marketing involves Kohll'sRx receiving direct or indirect remuneration by a third party, the authorization will state that such remuneration is involved.

Fundraising and PHI

Kohll'sRx will comply with state and federal privacy laws while conducting fundraising activities. "Fundraising" encompasses the activities specified in 45 CFR § 164.514(f)(1). Kohll'sRx's fundraising activities protect the privacy of Protected Health Information (PHI) and will include obtaining a written authorization to use or disclose protected health information when required by state or federal law. Kohll'sRx will include in any fundraising materials it sends to patients a description of how to opt out of receiving further fundraising communications.

1. Kohll'sRx will obtain an authorization from the patient to use or disclose PHI for fundraising activities required by state or federal privacy laws. However limited PHI (including a patient's demographic information and dates of service) may be used or disclosed to accomplish limited fundraising activities (including uses or disclosures to a business associate or to an institutionally related foundation for the purpose of raising funds for Organization) without patient authorization. Fundraising activities constitute "health care operations" under 45 C.F.R. sec. Under HIPAA and under Wis. Stat. § 146.82(2)(a), disclosures for health care operations are permitted without patient authorization.
2. Kohll'sRx's Notice of Privacy Practices will include a statement that the patient's PHI will not be used for fundraising activities unless the patient provides an authorization for the fundraising activity.
3. Even when an authorization has been obtained for fundraising activities, Kohll'sRx's fundraising communication must include a statement informing the recipient that he or she may opt out of future fundraising communications or revoke the authorization relating to these activities and a description of how to do so.
4. Kohll'sRx's Fundraising Department will maintain a log of all patients and others who have revoked the fundraising authorization or opted out of receiving future fundraising communications.
5. Kohll'sRx will not send any further fundraising information upon receipt in writing or other written notification that the patient's fundraising authorization has been revoked.
6. Kohll'sRx will make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent any further fundraising communications.

References/Applicable Regulations:

- 45 CFR § 164.514(f)(1)
- 45 CFR §164.501, Section 6(v) of the Definition

Accounting of Disclosures

To ensure patients can receive an accounting of disclosures of their protected health information, not including disclosures for purposes of treatment, payment, or health care operations. Disclosures to business partners must be included in the accounting. Under the Health Insurance Portability and Accountability Act, covered entities must give patients an accounting of disclosures, if requested. Patients may request an accounting of disclosures that were made up to six years prior to the date of request.

1. Maintain an accounting of disclosures of protected health information on each patient for at least six years.
2. Information that must be must be maintained (tracked) and included in an accounting:
    A. Date of disclosure.
    B. Name of individual or entity who received the information and their address, if known.
    C. Brief description of the protected health information disclosed.
    D. Brief statement of the purpose of the disclosure [or a copy of the individual's written authorization[14]] or a copy of the individual's written request for disclosure.
    E. Multiple disclosures to the same party for a single purpose [or pursuant to a single authorization[15]] may have a summary entry. A summary entry includes all information (2 A-E) for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.
3. Information that is excluded from the accounting and tracking rule are disclosures made:
    A. Prior to April 14, 2003 or prior to the entity's date of compliance with the privacy standards.
    B. To law enforcement or correctional institutions as provided in state law.
    C. For facility directories.
    D. To the individual patient.
    E. For national security or intelligence purposes.
    F. To people involved in the patient's care.
    G. For notification purposes including identifying and locating a family member.
    H. For treatment, payment, and healthcare operations.
    I. [Pursuant to an individual's authorization[16]]
4. All other disclosures of protected health information must be tracked. Disclosures are not limited to hard-copy information but any manner that divulges information, including verbal or electronic data release.
5. Disclosures may be tracked by a variety of internal processes that ensure accurate and complete accounting of disclosures.
    A. Computerized tracking systems that have the ability to sort by individual and/or date.
    B. Manual logs with one log per patient maintained in the patient's health record *(see sample "Disclosure Log" attached to this policy).*
    C. Authorization forms maintained in the patient's health record.

[14] Under the Department of Health and Human Services' Notice of Proposed Rulemaking (NPRM) issued March 27, 2002, disclosures made pursuant to an individual's authorization under 45 CFR 164.508 would be excluded from the accounting requirements.
[15] See note #1 above.
[16] See note #1 above.

6. All systems must be maintained and accessible for a period of at least six years to meet the requirement of providing an accounting of disclosures for that time period.
7. Disclosures that are not accompanied by [an authorization or [17]] a written request must be tracked by alternative computerized or hard-copy mechanisms.
8. A patient may make the request for an accounting in writing or orally. If the request is made orally, the organization should document such on the general "Authorization" form or a "Request for an Accounting of Disclosures" form *(see sample "Request of Accounting of Disclosures" form attached to this policy).* The organization must retain this request and a copy of the written accounting that was provided to the patient, as well as the name/departments responsible for the completion of the accounting.
9. A patient may authorize in writing that the accounting of disclosures be released to another individual or entity. The request must clearly identify all information required to carry out the request (name, address, phone number, etc.).
10. Provide the individual with an accounting of disclosures within 60 days after receipt of the request.
    A. If the accounting cannot be completed within 60 days after receipt of the request, provide the individual with a written statement of the reason for the delay and the expected completion date. Only one extension of time, 30 days maximum, per request is permitted.
    B. Requests can cover a period of up to six years prior to the date of the request.
11. Provide the accounting to the individual at no charge for a request made once during any twelve-month period. A reasonable fee can be charged for any additional requests made during a twelve-month period provided that the individual is informed of the fee in advance and given an opportunity to withdraw or modify the request.
12. Maintain written requests for an accounting and written accountings provided to an individual for at least six years from the date it was created.
    A. Maintain the titles and names of the people responsible for receiving and processing accounting requests for a period of at least six years.

Patient Photography, Videotaping, Other Imaging, and Audio Recording

To establish guidelines for patient consent to, and Kohll'sRx's use of, patient photography, videotaping, other imaging, and audio recording. Kohll'sRx uses a variety of media to collect health information and obtains the patient's informed consent in writing before creating photographs, videotapes, other images, or audio recordings of the patient.

"Consent" means written documentation of the patient's agreement to be photographed, videotaped, otherwise imaged, or recorded. Written consent establishes a reliable record of patient consent in case consent is later questioned. Written consents become part of the patient's health care record. Consents are valid for only a reasonable period, e.g., the duration of the immediate health concern. A new consent should be obtained if the situation surrounding the imaging or recording has changed. In addition, the patient has the right to withdraw the consent at any time, provided the withdrawal is in writing. Photographs, videotapes, other images, and audio recordings, which were obtained before the patient withdrew consent, are part of the patient's health record and shall be maintained according to Kohll'sRx's retention policy.

1. Except under very limited circumstances (see 6.a. below), images and recordings may not be created for any purpose without the written consent of the patient.

2. As part of obtaining consent, the patient is given an explanation of:
    a. The purpose of the photographing, videotaping, imaging, or audio recording,
    b. Any proposed use of the images or recordings for commercial, educational, promotional, or legal purposes,
    c. The security mechanisms to be used to protect patient privacy, and
    d. The duration of retention of the images recordings.
3. Kohll'sRx provides the patient with the above information in sufficient detail and understandable language to enable him or her to give informed consent to the proposed imaging or recording as a free and knowledgeable choice.
4. A health care provider (physician, registered nurse, physician assistant, psychologist, counselor, etc.) is responsible for providing the patient with an appropriate explanation of the imaging or recording and obtaining his or her informed consent in writing.
5. The clinician must document the following in the clinical record:
    a. When the explanation was provided;
    b. The details of the explanation; and
    c. The clinician's impression of the patient's understanding of the explanation.
6. Circumstances that may involve patient imaging or recording include:
        a. Documentation of abuse and neglect: Reportable cases of actual or suspected abuse and neglect do not require consent from the patient prior to photography, videotaping, and other imaging. These images may be submitted to the investigating agency with appropriate authorization/court order, but are not to be used for other purposes without consent.
        b. Research: Consent for imaging or recording must be explicitly stated in the patient's consent for participation in the research protocol. Kohll'sRx's institutional review board or privacy board must approve the creation of images and recordings as part of a research protocol
        c. Telemedicine (including e-mail) and Internet transmission: Consent for Kohll'sRx to use images or recordings for these purposes must be explicitly stated in the patient's written consent. The images or recordings, along with the medical record, should be encrypted to protect the patient's privacy
        d. Medical education or teaching: Consent for Kohll'sRx to use images or recordings for these purposes must be explicitly stated in the patient's written consent.
        e. Marketing/Publicity/Media requests: Authorization/consent for Kohll'sRx to use images or recordings for these purposes must be explicitly stated in the patient's written authorization/consent.
        f. Law enforcement or legal purposes: Consent for Kohll'sRx to use images or recordings for these purposes must be explicitly stated in the patient's written consent.
        g. Videotaping for Trauma Certification/Performance Improvement Purposes: Videotaping as a documentation "tool" for peer review, performance improvement activities, or trauma certification may be carried out with patient authorization. However, viewing is limited to authorized staff as per Kohll'sRx guidelines. The videotapes are not considered a part of the

patient's health information and will be erased following completion of the performance i

h. Photography of Newborns: Consent of the parent must be obtained prior to the taking of photographs of newborns as a courtesy or for sale.
i. Family/Friends: Documented consent is not needed for imaging or audio recording done by the patient's family members or friends. However, if a family member or friend has the consent of the patient to videotape a birth or procedure, for example, this should be done only with the agreement of the attending physician and acknowledgement that the individual may be required to discontinue taping if the attending physician deems it necessary.

7. Kohll'sRx may not release images and recordings to individuals or Kohll'sRx s outside Kohll'sRx without specific authorization from the patient, except when required by law or when the images or recordings have been "de-identified" and are no longer considered individually identifiable health information.
8. Kohll'sRx may determine that images and recordings are not individually identifiable health information only if identifiers, including full-face photographic images and any comparable images of the individual or of relatives, employers, or household members of the individual, are removed. (See Kohll'sRx De-identification Policy.)
9. Storage and retention of images and recordings:
    a. Images and recordings must be clearly identified with the patient's name, identification number and/or date of birth, and date of image or recording. Media must be stored securely to protect the patient's confidentiality. If used to document patient care, images and recordings will be stored in compliance with the Kohll'sRx's retention policy and state law. (See Kohll'sRx Retention Policy.)
    b. Still images and recordings created for medical purposes may be filed with the patient's health care record.
    c. Sensitive images and recordings may be stored in sealed envelopes within the patient's health care record.

Facility Access

To safeguard the confidentiality, integrity, and availability of protected health information (PHI), business, and proprietary information within Kohll'sRx's information systems/applications by controlling access to the physical buildings/facilities that house these systems/applications in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. Physical access to all Kohll'sRx's facilities is limited to only those authorized in this policy. To safeguard PHI, the facility(s), and systems/applications from unauthorized access, tampering, and theft, access is allowed to designated areas only to those persons authorized to be in them and with escorts for unauthorized persons. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Kohll'sRx's facility(s) to areas containing information systems/applications.

Responsible for Implementation

Privacy/Security Officer

Applicable To

All workforce members.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and

procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Key Definitions

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Restricted Area: Those areas of the building(s) where protected health information and/or sensitive organizational information is stored or utilized at any time. These areas include, but are not limited to the following examples:

A. Check-in desks/stations,
B. Nursing/Patient Care stations/desks,
C. Patient Care hallways,
D. Patient Care rooms or other designated area,
E. Employee meeting rooms/kitchens located in patient care areas,
F. Offices,
G. Cubicles,
H. Storage closets and cabinets (including medication storage areas),
I. Information Services equipment rooms,
J. Business Office
K. Human Resources
L. Administration offices.

Unrestricted Area: those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized there on a regular basis. These areas include the following:

1. Lunch rooms,
2. Conference rooms,
3. Building parking lots,
4. Building entry ways,
5. Main hallways, and
6. Restrooms.
7. Other public areas.

Vendors: persons from other organizations marketing or selling products or services, or providing services to Kohll'sRx. Examples include, but are not limited to the following:

1. Pharmaceutical Representatives,
2. Equipment Repair Service Personnel,
3. Food Services, and
4. Independent Contractor for Kohll'sRx.

Workforce: As defined in the HIPAA Privacy Rule, employees, volunteers (board members, community representatives), trainees (students), contractors, and other persons under the direct control of a covered entity.
Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, "workstation" also includes the combination of hardware, operating system, application software, and network connection.

10) **Security of Restricted Areas**
   A) Restricted areas and facilities are locked and alarmed when unattended (where feasible).
   B) Only authorized workforce members receive keys to access restricted areas (as determined by the Security Officer through Departmental requests).
      i) Workforce members are required to return the key(s) to the Human Resources department (or Supervisor) on their last day of employment/last day of contracted work or services being provided.
   C) Workforce members must report a lost and/or stolen key(s) to the Security Officer.
      i) The Security Officer facilitates the changing of the lock(s) within 24 hours of a key being reported lost/stolen

11) **Identification of Persons at Kohll'sRx**
   A) All persons, excluding patients and visiting family and friends, wear Kohll'sRx identification badges in addition to their own organization's id badges they may have.
      i) Workforce members always wear a Kohll'sRx identification badge while at any Kohll'sRx facility.
         (1) Workforce members are required to return their Kohll'sRx identification badge to the Human Resources department (or Supervisor) on their last day of employment/last day of contracted work or services being provided.
      ii) Visiting vendors register (sign in and out) on the Vendor Sign-in Log (Appendix 1) and obtain Visitor identification badges from the department they are visiting. Vendors are instructed to return the Visitor identification badge and sign out prior to leaving the premises.

12) **Persons Allowed in Restricted Areas**
   A) Workforce members as approved by their supervisor and as needed to perform their job duties.
   B) Patients with an escort of an authorized workforce member into and out of the areas.
   C) Family members and friends briefly visiting workforce members with an authorized workforce member's escort.
   D) Vendors with a workforce member's escort into and out of the areas.
   E) Vendors at Kohll'sRx on a long-term contract, once acclimated to the areas, without an escort.

13) **Persons Allowed in Unrestricted Areas**
   A) Workforce members.
   B) Patients.
   C) Vendors.
   D) Workforce family members and friends.
   E) All visitors.

Enforcement

F) Escort violators out of restricted areas immediately and either have them register and obtain a visitor ID badge or escort them to the area they are trying to get to.
G) Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
H) Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
I) Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Kohll'sRx.

14) **Workstation Security**

A) Workstations may only be accessed and utilized by authorized workforce members wearing appropriate identification to complete assigned job/contract responsibilities. Third parties may be authorized by the Technical Security Officer to access systems/applications on an as needed basis.
B) All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
C) All Kohll'sRx computer mainframes, servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devises which alert the Technical Security Officer of any problems. Access to these rooms is limited to authorized IS and facility services workforce as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from the Technical Security Officer and only with an escort by an authorized IS or facility services workforce member.
D) Permanent Workstations (i.e., desktop computer, printers, and monitors) may only be moved by authorized IS workforce members.
E) All wiring associated with a workstation may only be installed, fixed, upgraded, or changed by an authorized IS workforce member or other individual authorized by the Technical Security Officer.

15) **System/Application Access Control**

A) All systems/applications purchased by Kohll'sRx are the property of Kohll'sRx and are distributed to users by the Information Systems department only.
B) Prior to downloading, all software must be registered to Kohll'sRx and must be approved in advance by the IS department. To prevent computer viruses from being transmitted through Kohll'sRx's information systems, there will be no unauthorized downloading of any unauthorized software.
C) The Information Systems department is responsible for downloading all upgrades, testing upgrades, and for supporting Kohll'sRx systems/applications.

Facility Repairs and Maintenance

In accordance with the standards set forth in the HIPAA Security Rule, Kohll'sRx is committed to ensuring the confidentiality, integrity, and availability of all electronic protected health information (ePHI) it creates, receives, maintains, and/or transmits. To establish documentation guidelines for maintenance, repairs, and modifications to the physical components of its facilities when related to the security of the ePHI [164.310(a)(2)(iv)] as well as limit physical access to

electronic information systems and the facility(s) in which they are housed, while ensuring that properly authorized access is allowed [164.310(a)(1)].

Responsible for Implementation:

Privacy/Security Officer

Applicable To:

Privacy/Security Officer, leadership, and workforce members

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Key Definitions:

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

1) **Identify ePHI Security Risk(s)**. Prior to approving plans to repair, modify, or schedule maintenance any of Kohll'sRx's owned or leased facilities the Lead Project Coordinator works with the Privacy/Security Officer, or other designated workforce member, to determine whether the scheduled maintenance, repairs, changes, or the construction process itself, increases the security risk of ePHI. These security risks include, but are not limited to, the following and include work completed on the internal and/or external perimeter of the facilities (entryways, external and internal doors, locks, controlled access systems, walls, removing windows, etc.):
    a) Has the potential to or will limit or remove an authorized user's ability to access workstations and systems in which ePHI is created, received, stored, or transmitted during regularly scheduled hours and at regularly scheduled locations.
    b) Increases the potential for unauthorized access to ePHI.
    c) Otherwise has the potential to decrease the security, confidentiality, and/or integrity of the ePHI in any way.
2) **Reduce or Eliminate the ePHI Security Risks(s)**. If the changes indicate an increased security risk to ePHI, the Lead Project Coordinator amends the plans to contain the following conditions:
    a) All users that need access to ePHI have access to ePHI during their regularly scheduled hours and at their scheduled locations.
        i) If, however, any user will not have access to ePHI during their regularly scheduled hours, the Lead Project Coordinator notifies that user's supervisor prior to the unavailability of the ePHI. The Lead Project Coordinator, supervisor, and Privacy/Security Officer develop a plan to accommodate necessary changes. Document all decisions made and followed as required in this policy.
        ii) If any user will not have access to ePHI at their regularly scheduled location, the Lead project person notifies that user's supervisor prior to the unavailability of the ePHI. The Lead Project Coordinator, supervisor, and Security Officer develop a plan to accommodate necessary changes. Document all decisions made and followed as required in this policy.
        iii) If the plans increase the potential for unauthorized access to ePHI, the Lead Project Coordinator works with the Privacy/Security Officer, or other designated information systems workforce member, to identify ways to secure ePHI throughout the project

from unauthorized access. This may include requiring measures such as 24-hour monitoring of the area with security guards or cameras, changing locks and distributing keys to individuals on the project to limit the number of individuals with access, creating new entryways for workforce members and/or patients, etc. Document all decisions made and followed as required in this policy.

iv) If the plans otherwise decrease the security, confidentiality, and/or integrity of the ePHI in any way the Lead Project Coordinator works with the Privacy/Security Officer, or other designated information systems workforce member, to identify ways to secure ePHI throughout the project. Document all decisions made and followed as required in this policy.

3) **Monitor for Additional Risks**. The Lead Project Coordinator continuously monitors the project and immediately notifies the Security Officer of any increase or change in security risks of ePHI noted during the project. Document all decisions made and followed as required in this policy. If a violation of Kohll'sRx's security policies and procedures is identified, it is reported and investigated according to Kohll'sRx's Security Incident Policy.

4) **Documentation of the Project**. The Lead Project Coordinator facilitates documentation of all meetings and other efforts made to protect the confidentiality, integrity, and availability of ePHI throughout the project.
   a) Documentation includes, at a minimum, the following information:
      i) Description of the repair or modification including a summary of the original plans, any changes made to the plans, and reasons for any changes made to the plans.
      ii) Reason for the repair or modification.
      iii) Repair or modification start and end dates.
      iv) Individual(s) that completed the repair or modification.
      v) Summary of all steps taken to eliminate or decrease the identified security risk(s) to ePHI (including those identified before, during, and after the work was completed). At a minimum, this summary includes:
         (1) Description of the identified security risk.
         (2) Date the security risk was identified.
         (3) Specifically, what was done to eliminate or reduce the security risk(s).
         (4) Dates and times steps were taken to eliminate or reduce the security risk(s).
         (5) Individuals involved in eliminating or reducing the security risk(s).
   b) After completion of the project, the Lead Project Coordinator forwards all documentation to the Privacy/Security Officer.
      i) The Security Officer maintains all documentation received by the Lead Project Coordinator for a minimum of six years.

Applicable Standards/Regulations:

- 45 CFR §164.310(a)(1) – HIPAA Security Facility Access Controls
- 45 CFR §164.310(a)(2)(iv) – HIPAA Security Rule Maintenance Records

Business Associate Agreement

To establish guidelines for Kohll'sRx to identify those vendor/business relationships which meet the HIPAA definition of a "business associate" and provide direction in establishing formalized business associate agreements. Kohll'sRx shall implement the required procedures and ensure

documentation to establish satisfactory assurance of compliance. HIPAA requirements for business associates are addressed in the following standards:

- 45 CFR § 164.308(b)(1) – HIPAA Security Rule Administrative Safeguards Business Associate Contracts and Other Arrangements
- 45 CFR §164.314 – HIPAA Security Rule Organizational Requirements Business Associate Contracts or Other Arrangements
- 45 CFR § 164.502(e)(1) – HIPAA Privacy Rule Uses and Disclosures of Protected Health Information: General Rules – Disclosures to Business Associates
- 45 CFR §164.504 – HIPAA Privacy Rule Uses and Disclosures: Organizational Requirements

The standards define the concept of a business associate relationship and outline the required elements to be addressed in a business associate agreement (as addressed in this policy).
Responsible for Implementation: Privacy/Security Officers **and** Administration
Applicable To: All Departments/Units Involved with External Business Associates

Key Definitions:
Business Associate (BA): Under the HIPAA Privacy and Security Rules, a person (or entity) who is not a member of the covered entity's workforce and who performs any function or activity involving the use or disclosure of individually identifiable health information or who provides services to a covered entity that involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc.
Business Associate Agreement (BAA): Under the HIPAA Privacy and Security Rules, a legally binding agreement entered into by a covered entity and business associate that establishes permitted and required uses and disclosures of protected health information (PHI), provides obligations for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation. Refer to 45 CFR § 164.502(e)(1) to determine when the standard is not applicable.
Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.
Protected Health Information (PHI). Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.
-

Procedures:
1) The organization shall determine responsible oversight for the management business associate relationships and agreements. Responsibility may be delegated to:
   a) Privacy Officer.
   b) Security Officer.
   c) HIPAA Privacy & Security Team.

2) The organization's departments/business units are responsible for facilitating the assessment of both existing and future vendor/business relationships to determine whether the relationship meets the criteria for a HIPAA business associate agreement (BAA) (See Appendix 1). The following criteria define a business associate under HIPAA:
    a) The vendor/business' staff members are not members of the organization's workforce.
    b) The vendor/business' is doing something on behalf of the organization;
    c) That "something" involves the use and/or disclosure of PHI.
    d) Note that there are certain disclosures to vendors/businesses that do not require establishment of a BAA (see 45 CFR § 164.502(e)(1). These disclosures include:
        i) Disclosures to disclosures by a covered entity to a health care provider concerning the treatment of the individual;
        ii) Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or
        iii) Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.
3) The organization may determine the need for BAA's through:
    a) Mapping the flow of PHI and identifying where PHI is used or disclosed or created by external entities.
    b) Reviewing contract management documents/software and identifying where PHI is disclosed to external entities.
    c) Reviewing 1099 tax forms to identify vendors and then identify vendors with business arrangements where PHI is disclosed to external entities or used internally by vendor.
    d) Assessing new vendor/business arrangements to determine if PHI will be used and/or disclosed.
4) When it has been determined that a BA arrangement exits, the department/business unit leader shall contact the responsible individual/team to initiate a BAA document. The department/business unit leader shall provide the following information to "customize" the BAA:
    a) The name and contact information of the BA.
    b) A general description of the type of service being provided by the BA.
    c) Permitted uses and disclosures as applicable to the arrangement.
    d) The name of the organization's department/business unit and leader who established the BAA.
    e) Date of establishment of the business associate relationship and BAA.
    f) Name/signature line for the department/business unit leader or Privacy Officer.
    g) Name/signature line for the business associate contact.
5) If a vendor/business relationship requiring a BA agreement/addendum is in the process of contract negotiation and development, the provisions of the BAA may be incorporated into the contract as an option (a separate BAA would not be required).

6) Obligations and activities which must be addressed in the BAA document.

Privacy Rule Provisions (45 CFR § 164.504(e)(2):

a) Stated Purposes for Which Business Associate May Use or Disclose Protected Health Information: Business Associate is permitted to use and disclose Protected Health Information it creates or receives for or from the organization for the purposes as described in the addendum. Business Associate may also use Protected Health Information it creates or receives for or from the organization as minimally necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities.

b) Limitations on Use and Disclosure of Protected Health Information: Business Associate agrees it shall not use or disclose, and shall ensure that its directors, officers, employees, contractors, and agents do not use or disclose Protected Health Information for any purpose other than as expressly permitted by the BA Agreement, or required by law, or in any manner that would constitute a violation of the Privacy Standards if used by the organization.
   i) The BAA may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate; and
   ii) The BAA may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

c) Disclosure by Others: To the extent Business Associate is authorized by this Agreement to disclose Protected Health Information to a third party, Business Associate must obtain, prior to making any such disclosure, reasonable assurances from the third party that the Protected Health Information will be held confidential as provided pursuant to the Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and an agreement from the third party to immediately notify Business Associate of any breaches of confidentiality of the Protected Health Information, to the extent it has obtained knowledge of such breach.

d) Minimum Necessary: Business Associate shall disclose to its subcontractors, agents or other third parties, and request from the organization, only the minimum Protected Health Information necessary to performing or fulfilling a specific required or permitted function.

e) Safeguards Against Misuse of Information: Business Associate will establish and maintain all appropriate safeguards to prevent any use or disclosure of Protected Health Information other than pursuant to the terms and conditions of the Agreement.

f) Reporting of Disclosures of Protected Health Information: Business Associate shall, within [0] days of discovery of any use or disclosure of Protected Health Information in violation of the Agreement, report any such use or disclosure to the organization.

g) Agreements by Third Parties: Business Associate shall enter into an agreement with any agent or subcontractor that will have access to Protected Health Information that is received from, or created or received by Business Associate on behalf of, the organization pursuant to which such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to Business Associate pursuant to the Agreement with respect to Protected Health Information.

h) Access to Information: Within [0] days of a request by the organization for access to Protected Health Information about an individual contained in a Designated Record Set,

Business Associate shall make available to the organization the Protected Health Information it requests for so long as that information is maintained in the Designated Record Set. If any individual requests access to Protected Health Information about the individual directly from Business Associate, Business Associate shall make available and provide a right of access to the Protected Health Information to the individual, at the times and in the manner required by the Privacy Standards (see 45 C.F.R. § 164.524, or its successor as it may be amended from time to time). After receiving the request, Business Associate shall notify the organization within "0" days of such request.

i) Availability of Protected Health Information for Amendment: Business Associate agrees to make Protected Health Information available for amendment and to incorporate any such amendments in the Protected Health Information, at the times and in the manner required by the Privacy Standards (see 45 C.F.R. § 164.526, or its successor as it may be amended from time to time).

j) Accounting of Disclosures: Within [0] days of notice by the organization to Business Associate that it has received a request for an accounting of disclosures of Protected Health Information regarding an individual during the six years prior to the date on which the accounting was requested, Business Associate shall make available to the organization such information as is in Business Associate's possession and is required for the organization to make the accounting required by the Privacy Standards (see 45 C.F.R. § 164.528, or its successor as it may be amended from time to time). At a minimum, Business Associate shall provide the organization with the following information: the date of the disclosure; the name of the entity or person who received the Protected Health Information, and, if known, the address of such entity or person; a brief description of the Protected Health Information disclosed; and a brief statement of the purpose of the disclosure which includes an explanation of the basis for the disclosure. If the request for an accounting is delivered directly to Business Associate, Business Associate shall within "0" days forward the request to the organization. The organization is responsible for preparing and delivering the accounting requested. Business Associate agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

k) Availability of Books and Records: Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, the organization available to the Secretary for purposes of determining the organization's and Business Associate's compliance with the Privacy Standards.

l) If the organization (covered entity) and the business associate are both governmental entities, additional implementation specifications must be addressed (See 45 CFR § 164.504(e)(3).

Security Rule Provisions (45 CFR § 164.314):

m) Implementation of Safeguards: Business associate agrees to implementation of administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, and transmits on behalf of the organization.

n) Agents and Subcontractors: Business associate agrees that any agent, including a subcontractor, to which the business associate provides ePHI, agrees to implement reasonable and appropriate safeguards to protect the ePHI.

o) Security Incidents: Business associate agrees to report to the organization any security incident of which it becomes aware.
p) Termination: Business associate agreement authorizes termination of the contract by the organization, if the organization determines that the business associate has violated a material term of the contract.
q) The organization may want to seek legal counsel guidance prior to entering a BAA that includes language addressing:
    i) Insurance responsibilities.
    ii) Indemnification requirements.
r) If the organization chooses to terminate the arrangement with the business associate or the business associate chooses to terminate the arrangement with the organization, the agreement must be terminated as outlined in the provisions of the business associate agreement/addendum or contract.
s) Upon termination or expiration of the business arrangement between the BA and the organization, the BA shall either return or destroy all PHI received from the organization or created or received by BA on behalf of the organization that the BA still maintains in any form as outlined in the provisions of the business associate agreement/addendum or contract.

7) The organization does not have a statutory obligation to monitor the activities of its business associates. The organization, however, must respond to reported privacy breaches and security incident events should they occur and take reasonable steps to cure any potential breach or end the violation
8) The organization may serve as a BA to another covered entity and may be asked to review and sign that covered entity's external BA agreement/addendum or contract. As a BA, the organization should:
    a) Forward the external information to the Privacy Officer[18] to review the submitted BA agreement to ensure that the provisions outlined are consistent with those set forth in this policy**.**
    b) If the BA agreement is not consistent with this policy or contains additional provisions or provisions that are inconsistent with the privacy regulation, the Privacy Officer may recommend to the following alternatives.
        (1) Agree to the additional provisions and sign the agreement.
        (2) Refer the agreement to legal counsel to determine appropriateness before signing.
        (3) Refuse to agree to the provisions and notify the covered entity to establish a resolution.
9) To meet the documentation requirements of the Security Rule, the responsible individual/team shall maintain a file/electronic spreadsheet business associate agreements/addendums/contracts. This file shall include the following information, and shall be available for review as needed:
    a) Date BAA need identified/received by responsible individual/team.
    b) Name of Individual/organization which forwarded the agreement/identified need.
    c) Name of organization for which BAA is needed.
    d) Description of organization's operations that the BA is involved with.
    e) Initiation date of original contract (if applicable).
    f) Term of contract.

g) Date BAA signed by responsible individual.
h) Location of BAA.
i) Any additional notes.

10) All BAA documentation shall be maintained for a period of six years beyond the date of when the BAA relationship is terminated.
11) The BAA shall be effective for the length of the relationship between the BA and the organization, unless otherwise terminated under the provisions outlined in the agreement.

Attachments to Policy:

- Appendix 1: Examples of Business Associates
- Appendix 2: Business Associate Agreement Checklist

Applicable Standards/Regulations:

- 45 CFR § 164.308(b)(1) – HIPAA Security Rule Administrative Safeguards Business Associate Contracts and Other Arrangements
- 45 CFR §164.314 – HIPAA Security Rule Organizational Requirements Business Associate Contracts or Other Arrangements
- 45 CFR § 164.502(e)(1) – HIPAA Privacy Rule Uses and Disclosures of Protected Health Information: General Rules – Disclosures to Business Associates
- 45 CFR §164.504 – HIPAA Privacy Rule Uses and Disclosures: Organizational Requirements

APPENDIX 1: EXAMPLES OF BUSINESS ASSOCIATES

EXAMPLES OF BUSINESS ARRANGEMENTS THAT MAY INVOLVE DISCLOSURE OF PHI & REQUIRE BA AGREEMENTS/ADDENDUMS OR CONTRACT PROVISONS	
Accrediting/Licensing Agencies (JCAHO) Accounting Consultants/Vendors Actuarial Consultants/Vendors Agents/Contractors Accessing PHI (Consultants) Application Service Providers (i.e., prescription mgmt.) Attorneys/Legal Counsel Auditors Benchmarking Organizations Benefit Management Organizations Claims Processing/Clearinghouse Agency Contracts Coding Vendor Contracts Collection Agency Contracts Computer Hardware Contracts Computer Software Contracts Consultants/Consulting Firms Data Analysis Consultants/Vendors Data Warehouse Contracts Emergency Physician Services Contracts Hospitalist Contracts Insurance Contracts (Coverage for Risk, Malpractice, etc.) Interpreter Services Contracts IT/IS Vendors Legal Services Contracts Medical Staff Credentialing Software Contracts Microfilming Vendor Contracts Optical Disc Conversion Contracts	Pathology Services Contracts Paper Recycling Contracts Patient Satisfaction Survey Contracts Payer-Provider Contracts (Provider for Health Plan) Physician Billing Services Physician Contracts Practice Management Consultants/Vendors Professional Services Contracts Quality Assurance Consultants/Vendors Radiology Services Contracts Record Copying Service Vendor Contracts Record Storage Vendors Release of Information Service Vendor Contracts Repair Contractors of Devices Containing PHI Revenue Enhancement/DRG Optimization Contracts Risk Management Consulting Vendor Contracts Shared Service/Joint Venture Contracts with Other Healthcare Organizations Statement Outsource Vendors Telemedicine Program contracts Third Party Administrators Transcription Vendor Contracts Waste Disposal Contracts (Hauling, Shredding) Health Plan Relationships: Pharmaceutical Benefits Management Contracts Preauthorization Management Contracts Case Management Contracts Third Party Administrator (TPA) Contracts Wellness Promotion Contracts

EXAMPLES OF ARRANGEMENTS THAT ARE NOT BUSINESS ASSOCIATE RELATIONSHIPS AND DO NOT REQUIRE BA AGREEMENTS/ADDENDUMS OR CONTRACT PROVISIONS	
Banks Processing Credit Card Payments Blood Bank/Red Cross (Provider) Clinics (Provider Relationships) Courier Services Delivering Specimens Device Manufacturers Require PHI to Produce Pacemakers, hearing aids, glasses, etc. (Treatment) Cleaning/Janitorial Services DME for Equipment for Treatment Purposes Educational/School Programs (Student Privacy Education Required as Workforce Member) Health Plans Contracting With Network Providers (Covered Entity to Covered Entity) Health Plans for Purposes of Payment Hospitals Housekeeping/Environmental Services (Incidental Exp.) Infusion Provider for Treatment Law Enforcement Agencies Members of an Affiliated Covered Entity Members of the Organization's Organized Health Care Arrangement (OHCA) Pharmacy (Healthcare Provider/Treatment) Providers (Involved in Care & Treatment of Patient)	Members of the Organization's Workforce Organ Procurement Organizations Nursing Homes Quality Improvement Organization –Agent of CMS (Meta Star) Rental Employee Agencies (No PHI Shared – Employees Need Privacy Training) Repair Contractors (Maintenance, Copy Machine, Plumbing, Electricity, etc. – No PHI involved) School Health Nurses Supply Services Support Services Agreements for Supplies/Tx Purposes Tissue Banks U.S. Post Office and Other Couriers Volunteers (Board Members, Ethics Committee Members, IRB Members, etc.)

Breach Notification for Covered Entities

To provide guidance for breach notification by covered entities when impermissive or unauthorized access, acquisition, use and/or disclosure of the organization's patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (Omnibus Rule), as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule was originally effective September 24, 2009 with full compliance required by February 22, 2010.[19]

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacted the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH required notification of certain breaches of unsecured PHI to the following:

[19] 16 CFR Part 318 Available at: http://www.ftc.gov/os/2009/08/R911002hbn.pdf.

individuals, Secretary of the Department of Health and Human Services (HHS), and the media. The effective implementation date for these provisions was September 23, 2009.
In January of 2013, the "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules" (Omnibus Rule) modified the HITECH definition of a breach to eliminate the previous "harm" standard. **Effective September 23, 2013**, it states that an "acquisition, access, use, or disclosure in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to the disclosure was made;
3. Whether the protected health information was acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated. [20]

Definitions:

Access: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.[21]

Agent: An agent of the organization is determined in accordance with federal common law of agency. The organization is liable for the acts of its agents. An agency relationship exists if the organization has the right or authority of the organization to control the agent's conduct while performing a service on behalf of the organization (i.e., give interim instructions, direct the performance of the service).

Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI and is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to the disclosure was made;
3. Whether the protected health information was acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.[22]

Breach excludes:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to

[20] 45 CFR §164.402
[21] 45 CFR §164.304.
[22] 45 CFR §164.402

another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.[23]

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.[24]

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.[25]

Individually Identifiable Health Information: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[26]

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.[27]

Organization: For the purposes of this policy, the term "organization" shall mean the covered entity to which the policy and breach notification apply.

Protected Health Information (PHI): Protected health information means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium (see regulations for complete definition and exclusions)[28]

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security rule using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.[29] The following encryption processes meet this standard.

---

[23] ARRA/HITECH Title XIII Section 13400; §164.402,
[24] 45 CFR § 160.103.
[25] 45 CFR § 160.103.
[26] 45 CFR § 164.503.
[27] 45 CFR § 164.103.
[28] 45 CFR § 164.503.
[29] 45 CFR Parts 160 and 164; Final Rules Issued 8/19/09.

A. Valid encryption processes for data at rest (i.e., data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
B. Valid encryption processes for data in motion (i.e., data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.

2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
   A. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
   B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.[30] Refer also to HIPAA COW Security Networking Group policy: Device, Media, and Paper Record Sanitization for Disposal or Reuse.

Workforce: Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether they are paid by the covered entity or business associate.[31]

1. Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which an incident that may have resulted in a breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the organization's business associates). The organization shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (e.g., a business associate acting as an agent of the organization) of the organization (see attachment for examples of breach of unsecured protected heath information). Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response), conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by the organization to have been accessed, acquired, used, or disclosed as a result of the breach. The organization shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. Breach Investigation: The organization shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator

[30] HHS issued guidance on protecting personally identifiable healthcare information; document was the work of a joint effort by HHS, its Office of the National Coordinator for Health Information Technology and Office for Civil Rights, and the CMS (Issued 4/17/09).
[31] 45 CFR § 164.103.

shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment and notifications made, shall be retained for a minimum of six years.[32]

3. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. An "acquisition, access, use, or disclosure in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of at least the following factors:
    A. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    B. The unauthorized person who used the protected health information or to the disclosure was made;
    C. Whether the protected health information was acquired or viewed; and
    D. The extent to which the risk to the protected health information has been mitigated. [33]
4. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The organization may make breach notifications without completing a risk assessment.
5. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the business associate involved that is acting as the organization's agent. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.
6. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:
    A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or

[32] 45 CFR §164.530(j)(2).
[33] 45 CFR §164.402

B. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.[34]

7. Content of the Notice: The notice shall be written in plain language and must contain the following information:
   A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
   B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
   C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
   D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
   E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.
8. Methods of Notification: The method of notification will depend on the individuals/ entities to be notified. The following methods must be utilized accordingly:
   A. Notice to Individual(s): Notice shall be provided promptly and in the following form:
      1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the organization knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out. Limited examples (refer to preamble for more examples):
         a. The organization may send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan who are affected by a breach, if they all reside at a single address and all individuals to which the notice applies are clearly identified on the notice. When a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, however, address a breach notice to the dependent himself or herself.
         b. In the limited circumstance that an individual affirmatively chooses not to receive communications from a health care provider at any written addresses or email addresses *and* has agreed only to receive communications orally or by

[34] 45 CFR § 164.412.

telephone, the provider may telephone the individual to request and have the individual pick up their written breach notice from the provider directly. In cases in which the individual does not agree or wish to travel to the provider to pick up the written breach notice, the health care provider should provide all the information in the breach notice over the phone to the individual, document that it has done so, and the Department will exercise enforcement discretion in such cases with respect to the ''written notice'' requirement.

2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
    a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
    b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization's website, or a conspicuous notice in a major print or broadcast media in the organization's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.
3. If the organization determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area (of the breached patients) when the breach of unsecured PHI affects 500 or more of the organization's patients of a State or jurisdiction.
1. The Notice shall be provided in the form of a press release.
2. What constitutes a prominent media outlet differs depending upon the State or jurisdiction where the organization's affected patients reside. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a

monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State[35].

C. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.[36]

1. For breaches involving 500 or more individuals, the organization shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
2. For breaches involving less than 500 individuals, the organization will maintain a log of the breaches. The breaches may be reported during the calendar year or no later than 60 days after the end of that calendar year in which the breaches were discovered (e.g., 2012 breaches must be submitted by 3/1/2013 – 60 days). Instructions for submitting the logged breaches are provided at www.hhs.gov.[37]

9. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected.[38] The following information should be collected/logged for each breach (see sample Breach Notification Log):
   A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
   B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
   C. A description of the action taken regarding notification of patients, the media, and the Secretary regarding the breach.
   D. The results of the risk assessment.
   E. Resolution steps taken to mitigate the breach and prevent future occurrences.
10. Business Associate Responsibilities: In 2013, the Omnibus Rule extended liability for compliance to the HIPAA Privacy and Security Rules to business associates and their subcontractors. With these modifications, business associates are now directly liable for impermissible uses and disclosures, provision of breach notification to the covered entity, completing breach risk assessments, breach documentation requirements, and civil and criminal penalties for violations. The business associate (BA) of the organization that accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys, or

[35] (HHS Federal register comments, p. 5653, 1/25/13)
[36] Note: If the breach involves "secured" PHI, no notification needs to be made to HHS.
[37] For calendar year 2009, the organization is required to submit information to the HHS secretary for breaches occurring after the September 23, 2009 effective implementation date.
[38] The organization shall delegate this responsibility to one individual (e.g., Privacy Officer).

otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach (when the business associate is an agent of the organization, this notification must be provided within a shorter timeframe as specified in the Business Associate Agreement policy). Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach.[39] The BA shall provide the organization with any other available information that the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the organization will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is the responsibility of the Covered Entity to document this notification).

11. Workforce Training: The organization shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and promptly report breaches within the organization, as well as return or destroy PHI, as appropriate for the incident. Workforce members that assist in investigating, documenting, and resolving breaches are trained on how to complete these activities.
12. Complaints: The organization must provide a process for individuals to make complaints concerning the organization's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the organization's breach notification processes.[40]
13. Sanctions: The organization shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.
14. Retaliation/Waiver: The organization may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Applicable Federal/State Regulations:

- Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (Omnibus Rule)
- ARRA Title XIII Section 13402 – Notification in the Case of Breach
- FTC Breach Notification Rules - 16 CFR Part 318
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules

Original Version: October 1, 2009; Revised for Minor Changes: 10/15/09; 6/23/10; 8/19/10; 1/3/11; Major Revision HIPAA/HITECH Omnibus Rule: 3/5/1

[39] Business associate responsibility under ARRA/HITECH, and the Omnibus Rule for breach notification should be included in the organization's business associate agreement (BAA) with the associate (See www.hipaacow.org for BAA information).

[40] The organization may want to consider adding this right to complaint about the breach notification process to their Notice of Privacy Practices.

Security Incident Response

An information security incident response process is implemented to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

This policy has been developed to address the HIPAA Security Rule standard for security incident procedures [§ 164.308(a)(6)].

It is the policy of Kohll'sRx to safeguard the confidentiality, integrity, and availability of operational and patient protected health information through an established information security incident response process. The information security incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders

Responsible for Implementation:

- HIPAA Privacy/Security Officer
- Senior Management
- Information Systems Staff
- Building and/or Facilities Management Staff

Other Individuals which may be needed include representation from:

- Public Affairs
- Legal/Compliance Department
- Internal Audit/Risk Management
- Other workforce members involved in the incident or needed to fix/resolve it.
- Contractors (as necessary)

Applicable To:

All workforce members/staff, departments, contractors, and business partners of Kohll'sRx must adhere to the Security Incident Response Policy.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

This policy applies to the following security incidents:

- Technical security incidents (e.g., computer intrusions, denial of service to authorized users, etc.)

- Non-technical security incidents (e.g., administrative, and physical incidents including, but not limited to theft, unlocked doors, unauthorized facility entry, unauthorized computer access, etc.)

Key Definitions:

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Event: An ***event*** is defined as an occurrence that does not constitute a serious adverse effect on the organization or its operations, though it may be less than optimal. Examples of events include, but are not limited to:

- A hard drive malfunction that requires replacement
- Systems become unavailable due to power outage that is non-hostile in nature
- Accidental lockout of an account due to incorrectly entering a password multiple times
- Network or system instability

Indication: A sign that an incident may have occurred or may be occurring at the present time. Examples of indications include:

- The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS "hits" are also false positives and are neither an event nor an incident.
- The antivirus software alerts when it detects that a host is infected with a worm.
- The Web server crashes.
- Users complain of slow access to hosts on the Internet.
- The system administrator sees a filename with unusual characteristics.
- The user calls the help desk to report a threatening e-mail message (and it is determined by Information Services that it is a legitimate risk issue).

Precursor: A sign that an incident may occur in the future. Examples of precursors include:

- Suspicious network and host-based IDS events/attacks.
- Alerts because of detecting malicious code at the network and host levels.
- Alerts from file integrity checking software.
- Alerts from third party monitoring services.
- Audit log alerts.

Security Incident: A ***security incident*** is an occurrence that exercises a significant adverse effect on people, process, technology, data, or facilities. Security incidents include, but are not limited to:

- A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious
- Unauthorized disclosure
- Unauthorized change or destruction of ePHI (i.e., delete dictation, data alterations not following Kohll'sRx's procedures)
- Denial of service not attributable to identifiable physical, environmental, human or technology causes
- Physical threat to staff members or external entities at the site
- Biological threat to staff members or external entities at the site (e.g., bioterrorism attacks, such as those conducted through use of toxins such as anthrax)
- Disaster or enacted threat to business continuity

- Information Security Incident[41]: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to, the following:
    - **Denial of Service:** An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
    - **Malicious Code**: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
    - **Unauthorized Access/System Hijacking:** A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations.
    - **Inappropriate Usage:** A person violates acceptable computing use policies.
    - **Unplanned Downtime:** The network, system, and/or applications are not accessible due to any unexplainable circumstance causing downtime (e.g., system failure, utility failure, disaster situation, etc.).
    - **Multiple Component:** A single incident that encompasses two or more incidents (e.g., a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts).
- Other examples of observable information security incidents may include, but are not limited to:
    - Use of another person's individual password and/or account to login to a system.
    - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment).
    - Leaving workstations unattended while actively signed on.
    - Installation of unauthorized software.
    - Falsification of information.
    - Theft of equipment or software.
    - Destruction of tampering with equipment or software.
    - Posting of PHI on the Internet from a web portal.
    - Discarding of PC hard drives, CDs or other devices including PHI without following approved destruction/disposal guidelines.
    - Terminated workforce member accessing applications, systems, or network.

The security incident response process that follows reflects the process recommended by SANS, an industry leader in security (www.sans.org). Process flows are a direct representation of the SANS process. Review Appendix 1 for a flowchart identifying each phase.

1) **Identification Phase**:
    A) Immediately upon observation workforce members report suspected and known precursors, events, indications, and security incidents in one of the following ways (note: each organization needs to define how these need to be reported that best suits the organization's infrastructure):
        i) Report through technical means, such as an Information Services Help Desk.
        ii) Direct report to management, the HIPAA Security Officer, Privacy Officer, or other.

[41] Definition based on NIST 800-61; HIPAA Security Rule - *Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system (164.304).

iii) Email.
iv) Phone call.

B) The individual receiving the report facilitates completion of an Incident Identification form (refer to Appendix 4) and notifies the HIPAA Security Officer (if not already done).

C) Working with the Media: Certain types of information security incidents may generate the attention of the news media. The organization may also choose initiate contact with the news media in certain circumstances. The organization's designated media relations contact should serve as the liaison between the organization and the news media. In the absence of a media relations contact person, administration designates a media relations contact or seek assistance from the corporate office in working with the news media. The media relations contact can serve as a single point of contact for the news media, which eliminates the need to involve the SIRT members and leaves them free to manage the security incident. The IS leader or a member of the SIRT should be prepared to share information with the media relations contact. Key Considerations When Working With the Media Relations Contact/News Media:
   i) Contact the organization's legal counsel if unsure of legal issues.
   ii) Establish a single point of contact (media relations contact) when working with the news media to ensure that all inquiries and statements are coordinated.
   iii) Keep the level of technical detail very low – do not provide attackers with information.
   iv) Be as accurate as possible.
   v) Do not speculate.
   vi) Ensure that any details about the incident that may be used as evidence are not disclosed without the approval of investigative agencies.

D) The HIPAA Privacy/Security Officer determines if the issue is a precursor, incident, event, or security incident.
   i) If the issue is an event, indication, or precursor the HIPAA Security Officer forwards it to the appropriate resource for resolution.
      (1) Physical Intrusion: Facilities manager and law enforcement (if necessary for protection).
      (2) Non-Technical Event (minor infringement): the HIPAA Security Officer completes an SIR Form (see Appendix 2) and investigates the incident.
      (3) Technical Event: Assign the issue to an IS resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a small office or lack of expertise in the area.
   ii) If the issue is a security incident the HIPAA Security Officer activates the Security Incident Response Team (SIRT) (review the list of individuals at the beginning of this policy to identify potential team members) and notifies senior management. Notification may be made on an Incident Communication Log (refer to Appendix 4).
      (1) If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
         (a) Once the investigation is completed, progress to Phase V, Follow-up.
      (2) If the issue is a technical security incident, commence to Phase II: Containment. Note: If there is no internal expertise to assist with security incident response (i.e., a small office), request an outside vendor to assist with the technical work.

Identify potential partners for this work prior to discovery of a security incident. Technical resources can be identified from www.sans.org, www.foundstone.com, www.securityfocus.com, or other sites.

(a) The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.

(b) Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.

(c) The lead member of the SIRT team facilitates initiation of a Security Incident Report (SIR) Form (See Appendix 2 for sample format) or an Incident Survey Form (See Appendix 4). The intent of the SIR form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.

2) **Containment Phase (Technical)**: In this Phase, Kohll'sRx's information services department (or IT consultant) attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process, including the use of appropriate Chain of Custody procedures (See Appendix 3). This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

A) The SIRT reviews any information that has been collected by the HIPAA Security Officer or any other individual investigating the security incident.

B) The SIRT secures the physical and network perimeter.

C) The Information Services department performs the following:

i) Load a trusted shell.

ii) Retrieve any volatile data from the affected system.

iii) Determine the relative integrity and the appropriateness of backing the system up.

iv) If appropriate, back up the system.

v) Change the password(s) to the affected system(s).

vi) Determine whether it is safe to continue operations with the affect system(s).

(1) If it is safe, allow the system to continue to function;

(a) Complete any documentation relative to the security incident on the SIR Form.

(b) Move to Phase V, Follow-up.

(2) If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.

vii) The individual completing this phase provides written communication to the SIRT on the SIR Form or the Incident Containment form (See Appendix 4).

D) Continuously apprise Senior Management of progress.

3) **Eradication Phase (Technical)**: The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

A) Determine symptoms and cause related to the affected system(s).

B) Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed). This may include the following:

i) An increase in network perimeter defenses.

ii) An increase in system monitoring defenses.
iii) Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.
iv) Others.

C) Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
   i) If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.

D) Complete the Eradication Form (see Appendix 4)

E) Update the SIR Form with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).

F) Apprise Senior Management of the progress.

G) Move to Phase IV, Recovery.

4) **Recovery Phase (Technical):** The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

A) The technical team determines if the affected system(s) have been changed in any way.
   i) If they have, the technical team restores the system to its proper, intended functioning ("last known good").
      (1) Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
      (2) If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
   ii) If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.

B) Update the SIR Form with the detail that was determined during this phase.

C) Apprise Senior Management of progress.

D) Move to Phase V, Follow-up.

5) **Follow-up Phase (Technical and Non-Technical):** The Follow-up Phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.

A) Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.
   i) Create a "lessons learned" document and attach it to the completed SIR Form.
   ii) Evaluate the cost and impact of the security incident to the organization using the documents provided by the SIRT and the technical security resource.
   iii) Determine what could be improved.
   iv) Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.
   v) Carry out recommendations approved by Senior Management; sufficient budget, time and resources should be committed to this activity.

vi) Close the security incident.

B) **Periodic Evaluation:** It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding the organization's expectation for them, relative to security responsibilities.

6) **Retention of Security Incident Documentation**: Maintain all documentation surrounding every security incident, to include all work papers, notes, incident response forms, meeting minutes and other items relevant to the investigation in a secure location for a period of six (6) years

Attachments to Policy:

Chain of Custody Procedures
Security Incident Response Flow

Applicable Standards/Regulations:

- 45 CFR §164.308(a)(1) – HIPAA Security Rule Information System Activity Review

Sources:

- SANS (Sysadmin, Audit, Network, Security) Institute, Sample Incident Handling Forms, http://www.sans.org
- "Security Incident Response," Eric Sinclair, CISSP, Information Security Specialist, United Government Services, September, 2004
- NIST Computer Security Incident Handling Guide, Special Publication 800-61
- *Incident Response: Investigating Computer Crime*, Kevin Mania and Chris Prosise, Foundstone

CHAIN OF CUSTODY PROCEDURES

The Chain of Custody procedure that follows quotes the process detailed in *Incident Response: Investigating Computer Crime* by Kevin Mania and Chris Prosise, Foundstone, an industry leader in security.

Create an evidence tag for each piece of evidence gained during the security incident, as follows:

*Tag front**:***

- The time and date of the action
- The number assigned to the case
- The number of the particular evidence tag
- Whether consent is required and the signature of the person who owns the information being seized
- Who the evidence belonged to before the seizure, or who provided the information
- A complete description of the evidence

Back of the evidence tag:

- Who the evidence was received from
- The date of receipt
- The reason the evidence was given to another person
- Who received the evidence and where it was received and subsequently located to
- The individuals occupying the office
- The names of employees that may have access to the office
- The location of the computer systems in the room
- The state of the system (whether it was powered on, and what is visible on the screen
- Network connections or modem connections
- The people present at the time forensic duplication was performed
- The serial numbers, models and makes of the hard drives and the components of the system
- The peripherals attached to the system

Security Incident Response Flow