Allscripts Enterprise

INFORMATION PRIVACY & SECURITY POLICIES: HIPAA PRIVACY POLICY

Revision: 6.0

Approval Date: July 29, 2019

Approval Authorities: PSEC

For any comments or feedback related to this Policy, please email PandSCompliance@allscripts.com

Summary of Changes

Date	Version	Summary of Changes	Author
18-Apr-13	1.0	CPC Draft	Wright
25-Jul-14	2.0	Legal Privacy Draft	Wright/Ross
27-Oct-15	3.0	New Section 12.2 and editorial changes	Wright/Ross/Carter
7-Apr-17	4.0	Annual Review	P&S Team
12-Jun-18	5.0	Annual Review	P&S Team
29-Jul-19	6.0	Annual Review, revisions to align with other Allscripts Policies, removed redundant verbiage	P&S Team

Approval Log

Date	Version	Authority
3-May-13	1.0	PSEC
7-Aug-14	2.0	PSEC
27-Oct-15	3.0	PSEC
7-Apr-17	4.0	PSEC
12-Jun-18	5.0	PSEC
29-Jul-19	6.0	PSEC

Allscripts

Table of Contents

1 Purpose and Scope

The HIPAA Privacy Rule contains privacy and breach notification requirements that apply to individually identifiable health information created, received, maintained, or transmitted by health care providers who engage in certain electronic transactions, health transactions, health plans, health care clearinghouses, and their business associates.

The Office for Civil Rights (OCR) is the Departmental component responsible for implementing and enforcing the HIPAA Rules.

1.1 Purpose

Allscripts HIPAA Privacy Policy implements the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, 45 CFR Parts 160 and 164, in the context of Allscripts' overall business activities and obligations (both under law and contract) as a Covered Entity and a Business Associate. This Policy defines the procedures and protocols for management and Workforce members who have access to Protected Health Information (PHI) and are subject to HIPAA.
The HIPAA Privacy Rule contains privacy and breach notification requirements that apply to individually identifiable health information created, received, maintained, or transmitted by health care providers who engage in certain electronic transactions, health transactions, health plans, health care clearinghouses, and their business associates.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is the Departmental component responsible for implementing and enforcing the HIPAA Rules.

1.2 Scope

All members of the Workforce are required to comply with this Policy. Individuals who violate these requirements are subject to disciplinary action, up to and including termination or dismissal.

1.3 Responsibilities

A. Chief Privacy & Security Counsel:

1. Ensures that requirements in this document are maintained in accordance with HIPAA, 45 CFR Parts 160 and 164.

2. Is available for consultation in accordance with these requirements.

3. Makes a determination of, including but not limited to:
    a. Whether a use or disclosure of PHI is permitted and/or required by law.
    b. What constitutes the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure, or request.
    c. Whether a Business Associate Agreement ("BAA") is required and, if so, drafts and/or reviews BAAs.
    d. Whether a breach by a Business Associate was material, such that additional action is required.
    e. Whether a requested disclosure of PHI is limited to a limited data set of PHI, and ensures that a valid Data Use Agreement is in place before Allscripts provides a limited data set to another entity.
    f. What action to take to remedy the violation of a Data Use Agreement, including the possibility of discontinuing disclosure of PHI to the recipient and/or reporting the recipient to the Secretary of the Department of Health and Human Services.

4. Provides guidance to ensure a disclosure is limited to the relevant requirements of the law in accordance with the minimum necessary standard and applicable State law, where appropriate.

5. Receives requests:
    a. From law enforcement officials when PHI is part or the entire request, and coordinates review and response with appropriate Legal team members;
    b. For disclosure of PHI to a third-party for research, public health or healthcare operations purposes;
    c. For disclosure of PHI from public officials, other covered entities, and from other requestors seeking access to PHI belonging to someone other than himself/herself;
    d. For access or amendment of a patient's PHI;
    e. From patients disagreeing with a request that is denied, and forwards such to the appropriate Covered Entity client, if known;
    f. For PHI related to health oversight activities;
    g. For use or disclosure of PHI for non-routine purposes;
    h. For use or disclosure of de-identified information pursuant to these requirements; and,
    i. For any other requests to use and/or disclose PHI not specified herein.

6. Provides guidance on written notification to Covered Entity client when a request for access, amendment, restriction, or accounting has been received from an individual.

7. Authorizes Allscripts to make requested amendments to PHI in a Covered Entity client's designated record set, so long as the Covered Entity client has provided written authorization. Advises Allscripts as to the documentation required from Covered Entity clients to request amendments to PHI.

8. Reviews requests by Allscripts workforce members for assistance by vendors who may have access to PHI.

9. Attempts to ensure that PHI received from, or created by or on behalf of, Allscripts is destroyed or returned at the termination of a contract.

10. Upon receiving notice of a material breach, if a Business Associate cannot or will not take action to cure the breach and/or end the violation in a timely manner, reviews if termination of the contract is feasible and/or appropriate and makes recommendations to the Chief Compliance Counsel and General Counsel accordingly.

11. Investigates and determines whether a privacy incident has occurred.

12. Advises the company regarding appropriate action to mitigate, to the extent practicable, harmful effects that are known to Allscripts stemming from a use or disclosure of PHI in violation of this Policy and other relevant Allscripts requirements.

13. Maintains documentation required by this Policy including but not limited to the following:
    a. Written requests for restrictions on the use or disclosure of PHI in written or electronic form for six (6) years or other length of time required by HIPAA;
    b. Other documentation relevant to this Policy, including written requests for access to records and designated record sets that are subject to access by patients; and,
    c. Records in accordance with requirements, including receiving requests for amendments; forwarding requests to appropriate Covered Entity clients; and amending the PHI in designated record sets upon written direction from Covered Entity clients.

14. Prior to making a disclosure pursuant to any request under HIPAA, the CPSC or his/her designee will ensure that any such disclosure meets the requirements of this Policy, verifies the terms of the BAA with the specific Covered Entity client and the identity and authority of the requestor who seeks access to the PHI.

15. If a disclosure is to be made in response to a lawful request made under HIPAA, such disclosure shall be made pursuant to the requirements of this Policy and logs the disclosure.

16. Acts as the repository for privacy-related complaints and investigates merits of a complaint.

17. Provides the opportunity for and directs workforce members to comply with HIPAA training required by Allscripts. Ensures that the proper documentation exists to verify workforce members' training. Retains evidence of such training for at least six (6) years.

18. Recommends, after investigation, appropriate disciplinary action against an employee or member of the workforce who is engaged in a breach of privacy or who fails to comply with Allscripts Privacy and Security Policies. Any disciplinary action will be in accordance with the Progressive Disciplinary Action for Compliance Violations Policy.

19. When determining appropriate disciplinary action, Chief Privacy & Security Counsel ("CPSC") will consider relevant evidence, including the work history of the employee and the severity of the breach.

20. May designate another individual to function in his/her capacity with regard to the requirements set forth in this Policy.

B. Allscripts Workforce:

1. Ensures that PHI is only accessed, used, and disclosed in accordance with the Minimum Necessary requirements of applicable law and this Policy. This includes appropriate de-identification of Sensitive Information, which shall require approval of the CPSC.

2. Notifies the CPSC:
    a. When there is a question as to whether a particular use or disclosure of a patient's PHI should be made.
    b. When a workforce member receives a request for disclosure of PHI for public health purposes.
    c. When there is a question as to whether a disclosure of PHI without an authorization for judicial and/or administrative proceedings would require an authorization.
    d. When a request for disclosure of PHI relating to a worker's compensation or similar matter is received.
    e. When a patient requests a restriction with regard to the use or disclosure of the individual's PHI.
    f. When there is a question regarding minimum amount of PHI necessary for a particular use or disclosure.
    g. When a patient request is received in writing for access to, amendment of, or accounting of disclosures of his/her records.
    h. When a request to receive communications by alternative means or at an alternative location is received from a patient.
    i. When there is a question regarding the verification of the identity and authority of a person requesting PHI.
    j. When a workforce member becomes aware of a pattern of activity or practice by a recipient that constitutes a material breach or violation of a contract, BAA, NDA, CSA, or HIPAA.
    k. When it might be necessary to execute a BAA.
    l. When any other questions relating to the use and disclosure of Sensitive Information may arise.
    m. When any question regarding the use of de-identified data or statistician certification pertaining to data de-identification may arise.

3. If Allscripts workforce members discovers a matter that might constitute a breach or violation of a Business Associate Agreement, such workforce members must report the misconduct to the Chief Compliance Counsel, CPSC, CSO, Compliance Speak Freely Line and/or Redball Incident Management Tool.

4. May not use or disclose PHI other than as provided in this document.

5. May use or disclose PHI as authorized by, and to the extent necessary to comply with, laws relating to workers' compensation or other similar programs, established by law, if so authorized by Human Resources.

6. Verifies the identity and authority of persons requesting PHI from a Covered Entity client or Vendor.

2 Reasonable Safeguards to Protect the Confidentiality of Protected Health Information

Allscripts provides reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and the confidentiality, integrity, and availability of ePHI. For example, to ensure that PHI stored on computers is safeguarded, laptops where PHI can be potentially accessed are, at all times, encrypted and equipped with security that time-activates a password-protected screen saver or logoff.

2.1 Requirements

A. Allscripts workforce members maintain the following physical safeguards to protect the privacy of PHI and the confidentiality, integrity, and availability of ePHI, including, but not limited to the following:

   1. Workforce members access Allscripts facilities where PHI is accessed through an entrance secured by use of a keycard. Keycard access is limited to those who have business in or authority to enter the facility.

   2. Workforce members do not allow non-workforce members to access their personal work-area unless PHI has been reasonably and appropriately secured. Workforce members alert their manager and/or security to the presence of unauthorized persons in areas of the Allscripts office where PHI may be present.

   3. Each individual member of the Allscripts workforce is responsible for the security of PHI in his or her workspace. Workforce members take reasonable and appropriate precautions to safeguard access to PHI including, but not limited to, compliance with security measures required by the Security Policy and other guidance issued by the CPSC and CSO.

B. Allscripts must obtain reasonable assurance with its Business Associates through contracts/BAAs that the Business Associate will appropriately use and disclose PHI by adhering to the following practices:

1. When Allscripts enters into a BAA with a vendor, supplier, agent, consultant, subcontractor, or any other third-party, the Business Associate is required to have policies and procedures that appropriately protect patients' PHI.

2. If Allscripts provides a limited data set to another entity pursuant to a Data Use Agreement, the recipient of the limited data set is required to use appropriate safeguards to prevent the use or disclosure of information in a manner other than as provided for by the Data Use Agreement.

3 When Business Associate Agreements are Necessary

Protocols for management and workforce members regarding contracting with vendors who have access to PHI are defined in this section. Such vendors are known as Business Associates.

3.1 Business Associate

A. A Business Associate is a person or entity that accesses, creates, receives, maintains, or transmits PHI, or performs certain functions or activities for or on behalf of Allscripts, including, but not limited to the following:
   1. Claims processing or administration
   2. Data center hosting
   3. Product development
   4. Data analysis, processing or administration
   5. Billing
   6. Benefits management

B. A Business Associate also includes those providing the following services to Allscripts:
   1. Legal
   2. Auditing
   3. Actuarial
   4. Accounting
   5. Consulting
   6. Data aggregation
   7. Management
   8. Administrative, Accreditation, or Financial services
   9. Other types of Business Associates include the following:
   10. Health Information Organizations
   11. E-prescribe Gateways
   12. One that offers Personal Health Records to individuals on behalf of a Covered Entity
   13. Patient Safety Organizations
   14. Subcontractors
   15. Others that provide data transmission services and that require access to PHI on a routine basis

3.2 Use and Requirements of Business Associate Agreements

A. When Allscripts requires the services of a third party, the following actions are taken:

1. Business Unit determines if the third-party will perform a function, activity, or service for which the third party may have access to PHI.
2. Business unit consults with the CPSC or Allscripts Legal.
3. CPSC/Legal determines whether a BAA is necessary.
4. CPSC ensures that Allscripts executes a BAA with the Business Associate and that the BAA is appropriately retained.

B. BAAs must satisfy the following requirements:
1. When Allscripts contracts with a Business Associate, Allscripts must ensure that the terms meet or exceed the applicable requirements that clients have required of Allscripts.
2. Contents of the BAA are to be dictated by regulation and client contractual requirements.
3. All BAAs must have an Effective Date from at least March 23, 2013, if not, a new BAA is required.
4. All BAAs must be reviewed and approved by Privacy Counsel.

3.3 Breach of a Business Associate Agreement

A. In the event any Allscripts workforce member becomes aware of any problem with a Business Associate that may constitute a breach or violation of the Business Associate's obligations under its contract or of HIPAA, the workforce member must report the misconduct to the CPSC, CSO, Chief Compliance Counsel, and/or Compliance Speak Freely Line or Redball Incident Management Tool.

B. The CPSC, CSO, and Chief Compliance Counsel take reasonable steps to cure the breach or to end the violation, as applicable, in accordance with Section 4.0 of this Policy, Disclosure and Review of Privacy Violations Committed by a Business Associate.

4 Disclosure and Review of Privacy Violations Committed by an Allscripts Business Associate

The following actions will be taken when there is a potential breach of a BAA by an Allscripts Business Associate:

A. Upon discovery of a potential breach of a BAA, including privacy incidents, security incidents, or Breaches, the individual who discovered the potential Breach (workforce member, vendor, etc.) reports the Business Associate to the CPSC, Compliance Speak Freely Line and/or Redball Incident Management Tool.

B. CPSC investigates to determine the scope of the breach and whether additional action is necessary.

C. If the CPSC determines that the breach was material, CPSC works with the business unit to inform the Business Associate of the breach and attempts to have the Business Associate cure the breach and/or end the violation.

D. If the Business Associate continues to breach the BAA, CPSC, in consultation with Chief Compliance Counsel and other appropriate resources may recommend contract termination or take other appropriate steps to meet Allscripts' compliance obligations and appropriate protect PHI.

5 Disclosure and Review of Privacy Violations Committed by Allscripts as a Business Associate

The following actions will be taken when there is a potential breach of a BAA by Allscripts as a Business Associate:

A. Upon discovery of a potential breach of a BAA, including privacy incidents, security incidents, or Breaches, the individual who discovered the potential Breach (workforce member, vendor, etc.) reports the breach or suspected breach to the CPSC, Compliance Speak Freely Line and/or Redball Incident Management Tool.

B. CPSC investigates to determine the scope of the breach and whether additional action is necessary.

C. If the CPSC determines that the breach was material, works with the business unit to inform the Covered Entity of the breach and attempts to cure the breach and/or end the violation.

6 De-Identification of Protected Health Information

A. The purpose of this section is to provide information for management and workforce members regarding the circumstances under which PHI can be de-identified by removing certain individual identifiers in accordance with HIPAA and can be used and disclosed without authorization.

B. PHI received, maintained, created, transmitted or held on behalf of Covered Entity clients may not be de-identified for any purpose without prior, specific, written authorization from the Covered Entity client.

C. Business units seeking to de-identify Covered Entity client data for internal or external purposes shall first submit a written request to the CPSC. Such request shall include, at a minimum, the following information:

1. Each Covered Entity client whose patient information is requested to be de-identified.

2. The methodology for de-identifying the PHI, either by removal of 18 patient identifiers or by receiving a statistician's certification.

3. The business reason for using the de-identified PHI.

4. The length of time the de-identified data will be needed.

D. PHI can be de-identified by one of the following methodologies:

1. Safe Harbor. Removal of all 18 identifiers which requires elimination of the following information regarding the patient and relatives, employers and household members of the patient, if known:

   - Names
   - Addresses (not including State)
   - Dates (except year) directly related to the individual, including birth date, admission date, discharge date, treatment date, and date of death
   - Ages over 89
   - Telephone numbers
   - Fax numbers
   - E-mail addresses
   - Social security numbers
   - Medical record numbers
   - Health plan beneficiary numbers
   - Account numbers
   - Driver's license numbers
   - Vehicle identifiers and serial numbers, including license plate numbers
   - Device identifiers and serial numbers
   - URLs
   - IP addresses
   - Biometric identifiers (including fingerprints and voice prints)
   - Full face photographs and any comparable images
   - Other unique identifiers *And* requires that Allscripts does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual.

2. Expert Determination. Receiving an independent statistician's certificate, all requests shall clearly state that a statistician's certificate is preferred, which will be reviewed by the CPSC.

6.1 Receipt of a Request for Use or Disclosure of Protected Health Information

The following actions will be taken when a request is received for a use or disclosure of PHI for a purpose other than those permitted by this Policy:

A. Upon receipt of a request for a use or disclosure of PHI for a purpose other than those permitted by this Policy, the recipient forwards the request to the CPSC for consideration.
B. CPSC will review the request and determine whether it is appropriate.
C. If the Use or Disclosure is determined to be appropriate, then the CPSC will provide guidance regarding how the request can be satisfied.

7 Permitted Uses and Disclosures of Protected Health Information

A. Allscripts workforce members may use or disclose PHI only as described herein according to the following:

    1. To support the treatment, payment, or healthcare operations of Covered Entity clients, as directed by Covered Entity clients, as consistent with any applicable Business Associate Agreement, and in accordance with the provisions of this Policy or
    2. Incident to a use or disclosure otherwise permitted or required by this Policy.

B. Questions regarding whether a use or disclosure of PHI is appropriate shall be directed to the CPSC or Allscripts Legal.

7.1 Other

A. Subject to Section 21.0 or Section 22.0, as applicable, Allscripts workforce members may use and disclose its PHI as follows:

    1. For Allscripts quality assurance activities so long as a client has not prohibited Allscripts from doing so;

    2. As necessary for legal or financial review of Allscripts operations; and,

    3. For internal administrative activities.

B. Allscripts workforce members shall direct questions as to whether a particular use or disclosure of PHI is permitted pursuant to this Policy to the CPSC.

8 Disclosure of Protected Health Information as Required by Law

8.1 Requirements

A. Allscripts workforce members may not disseminate PHI without an authorization, other than as provided in Section 7.0 of this document, Permitted Uses and Disclosures of Protected Health Information, or as permitted by this section.

B. Allscripts is permitted to make disclosures of PHI without an authorization pursuant to the applicable requirements of 45 C.F.R. §164.512.

1. Disclosures about victims of abuse, neglect, or domestic violence, and
2. Disclosures for judicial and administrative proceedings.
3. Disclosure to comply with State laws requiring disclosure of PHI, as applicable.

8.2 Victims of Abuse, Neglect, or Domestic Violence

In the event that a requestor seeks PHI pertaining to a disclosure about victims of abuse, neglect, or domestic violence, Allscripts workforce members shall direct the request to the CPSC, who determines whether or not the PHI may be released without an authorization.

8.3 Judicial and Administrative Proceedings/Pursuant to Process

In the event that a requestor seeks PHI in the course of a judicial or administrative proceeding and/or pursuant to process, Allscripts workforce members contact the CPSC and shall otherwise follow Section 11.0 of this Policy, Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings, or Section 12.0 of this document, Disclosure of Protected Health Information for Law Enforcement Purposes.

A. If the request is made by a non-governmental official, policy Section 11.0 of this Policy governs.

B. If the request is made by a governmental official or a person acting on behalf of a governmental official, Section 12.0 of this Policy governs.

9 Disclosure of Protected Health Information for Certain Public Health Activities

A. Generally, Allscripts workforce members may use or disclose PHI only in accordance with Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information.

B. Allscripts workforce members may disclose PHI to the following entities, without obtaining authorization from the Covered Entity client or patient:

1. A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions, or

2. At the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.

3. Such requests shall be reviewed and approved by the CPSC l before any PHI is shared.

10 Disclosure of Protected Health Information for Certain Health Oversight Activities

A. As a general rule, Allscripts workforce members may not disseminate PHI other than as provided in Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information, without authorization from the Covered Entity client or the patient. In addition, Allscripts workforce members may disclose PHI to a health oversight agency for oversight activities authorized by law. Health oversight agencies include agencies or authorities of the United States, a State or territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting on behalf of such public agency, that is authorized by law to oversee the healthcare system (whether public or private). Health oversight activities include, but are not limited to: audits; civil, administrative or criminal investigations; inspections; and licensure or disciplinary actions.

B. All requests to Disclose PHI for Health oversight activities shall be directed to the CPSC for review and response.

10.1 Requirements

Disclosures made during the course of routine inspections for health oversight and/or accreditation purposes are included in a log of disclosures.

10.2 Compliance with Legal and Professional Standards

A. Allscripts workforce members shall report conduct that may be unlawful or otherwise violates professional standards to the Chief Compliance Counsel, Compliance Speak Freely Line or Redball Incident Management Tool.

B. In the event that an Allscripts workforce member desires to report unlawful or substandard conduct to a third-party investigator or enforcement agency, such disclosure of PHI made in the context of reporting unlawful or substandard conduct does not result in violation of the requirements of this Policy, provided that:

1. The workforce member believes in good faith that Allscripts or a workforce members member has engaged in conduct that is unlawful or otherwise violates professional standards, or that the services, or conditions provided by Allscripts or a workforce member potentially endanger one or more patients, workforce members, or the public, and

2. The disclosure is to:

a) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Allscripts;
b) An appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Allscripts; or,
c) An attorney retained by or on behalf of the workforce member for the purpose of determining the legal options of the workforce members with regard to the conduct described previously.

11 Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings

This section governs requests for PHI made by persons other than governmental officials or those acting on their behalf. When Federal or State officials are involved, Section 12.0 of this Policy, Disclosure of Protected Health Information for Law Enforcement Purposes, governs.

11.1 Requests for Disclosure of Protected Health Information

A. In the event Allscripts workforce members receive a request for disclosure of PHI in the context of a judicial or administrative proceeding, the following actions are taken:

1. Forward the request to the CPSC. Note: Requests must be in writing.

2. CPSC determines whether Allscripts may disclose PHI without obtaining an authorization from the Covered Entity client and/or patient.

12 Disclosure of Protected Health Information for Law Enforcement Purposes

12.1 Law Enforcement Officials

A. Law enforcement officials include officers or employees of an agency or authority of the United States, a State or a territory, a political subdivision of a State or territory, or an Indian tribe who is empowered 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.

B. Requests for PHI including, but not limited to court orders, warrants, etc., from law enforcement officials shall be directed to the CPSC, Chief Compliance Counsel, or General Counsel to evaluate and respond to the request.

12.2 Law Enforcement Delay

If a law enforcement official states to Allscripts that a notification, notice, or posting that HIPAA otherwise requires would impede a criminal investigation or cause damage to national security, CPSC shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the law enforcement official; or
2. If the statement is made orally, CPSC shall document the statement, including the identity of the law enforcement official making the statement, and delay the notification 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.

12.3 When Protected Health Information can be Disclosed by Workforce Members

Allscripts workforce members may disclose PHI for a law enforcement purpose to a law enforcement official in the following circumstances with the approval of CPSC:

1. As required by law, including laws that require the reporting of certain types of wounds or other physical injuries, but not including laws pertaining to public health governed by Section 9.0 of this Policy, Disclosure of Protected Health Information for Certain Public Health Activities or domestic violence governed by Section 14.0 of this Policy, Disclosure of Protected Health Information in Situations Presenting a Serious Threat to Health or Safety.

   AND

2. In compliance with and as limited by the relevant requirements of:
   a. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer,
   b. A grand jury subpoena, or
   c. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
      i. The information sought is relevant and material to a legitimate law enforcement inquiry;

      ii. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and,

iii. De-identified information could not reasonably be used in accordance with Section 6.0 of this Policy, De-Identification of Protected Health Information.

13 Disclosure of Protected Health Information for Military or National Security Purposes

Allscripts workforce members may not disseminate PHI except as provided in Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information. In the event Allscripts workforce members receive a request for disclosure of PHI for a military or national security purpose, such workforce members shall direct the request to the CPSC who determines whether to disclose PHI in response to the request.

14 Disclosure of Protected Health Information in Situations Presenting a Serious Threat to Health and Safety

In the event Allscripts workforce members receive a request for disclosure of PHI for one of the reasons below, such workforce members shall direct the request to the CPSC who determines whether to disclose PHI in response to the request:

1. Abuse, neglect, or domestic violence;
2. Serious threat to the health or safety of the public;
3. Identification and location purposes (e.g., disclosure of PHI in response to a request by law enforcement for purposes of locating a missing person or a material witness);
4. Victims of a crime other than abuse, neglect, or domestic violence;
5. Criminal conduct is suspected in the death of an individual; and,
6. Crime has taken place on Allscripts premises.

15 Disclosure of Protected Health Information as Necessary to Comply with Workers' Compensation Laws

When a request from State agencies, or similarly situated entities, pertaining to PHI purportedly necessary to resolve workers' compensation claims is received, Human Resources, in consultation with the CPSC, reviews and responds to the request.

16 Use of Limited Data Sets

The purpose of this section is to inform management and workforce members of the circumstances under which Allscripts workforce members may use or disclose PHI other than as provided in Section 27.0, Right to Request Amendment of Protected Health Information, through Section 26.0, Accounting of Disclosures, and without an authorization, and in other than de-identified form.

16.1 Limited Data Set

A. A Limited Data Set (LDS) is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

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

Generally, Allscripts does not maintain LDS on behalf of its Covered Entity clients. If Allscripts does maintain a Covered Entity client's LDS, Allscripts shall agree to terms and conditions regarding maintenance of such LDS, in consultation with and with approval of the CPSC, in a written agreement signed by both the Covered Entity client and Allscripts.

16.2 Data Use Agreement

In the event that Allscripts maintains the LDS of its Covered Entity client data, a Data Use Agreement is required before the LDS is shared. A Data Use Agreement is intended to ensure that the recipient of the LDS uses or discloses the PHI for limited purposes. Requests for Data Use Agreements are submitted to the CPSC.

16.3 Requirements

Allscripts workforce members may use or disclose the LDS maintained by Allscripts as a Covered Entity only for research, public health, or healthcare operations purposes if Allscripts enters into a Data Use Agreement with the entity receiving the limited data set.

16.4 Request to Disclose Protected Health Information

The following describes the actions taken when a request is received to disclose PHI to a third party for research, public policy or healthcare operations purposes.

1. Allscripts receives a request to disclose PHI.
2. The workforce member who receives the request forwards the request to the CPSC to determine whether the disclosure is warranted and, if so, whether a LDS may achieve the result for which the PHI was requested.
3. CPSC ensures that an appropriate Data Use Agreement is in place with the receiving entity.

17 Right to Request Additional Restrictions on the Use or Disclosure of Protected Health Information

The purpose of this section is to provide information for management and workforce members regarding requests from patients to restrict the use and disclosure of PHI and/or to make confidential communications.

1. Patients requesting restrictions on Uses and Disclosures of their PHI are informed that such requests must be made directly to their providers.

2. Written requests from patients for restrictions on Uses and Disclosure of their PHI are promptly forwarded to the CPSC.

3. CPSC promptly notifies the appropriate Covered Entity client of the patient's request. The Provider is responsible for reviewing and responding to the patient's request.

18 Uses and Disclosures of Protected Health Information for which an Authorization is Required

A. Allscripts may only use or disclose PHI about a patient if the disclosure is authorized by the Covered Entity client or, in special cases, the patient or the patient's personal representative, pursuant to an authorization form which complies with the requirements of this Policy or is otherwise permitted or required by another Allscripts procedure. The CPSC Counsel must be consulted before Allscripts initiates a use or disclosure requiring the patient's authorization.

B. A patient's (or personal representative's) request to access his or her own PHI is subject to Section 25.0 of this Policy, Right to Access Records, rather than the procedure outlined below.

18.1 Authorization

18.1.1 General Procedure

A. Except as permitted by Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information, regarding uses and disclosures for treatment, payment and healthcare operations, and Allscripts' other procedures regarding uses and disclosures of PHI, a patient's PHI may only be used and disclosed if the Covered Entity client, patient, or the patient's personal representative completes and signs an authorization form approved by the CPSC. Allscripts may accept an authorization form signed by the patient (which is not the approved authorization form) only if the authorization form contains each of the elements set forth in Section 18.1.2 of this Policy. If Allscripts workforce members have questions as to whether the use or disclosure of PHI requires an authorization, such workforce members consult with the CPSC.

B. Allscripts Workforce members may not disclose information pursuant to an authorization without ensuring the validity of the authorization by following the procedures set forth below.

18.1.2 Elements of Patient Authorization

A. If a use or disclosure of PHI requires a patient's authorization, Allscripts may only make the use or disclosure pursuant to an authorization written in plain language and containing the following elements:

1. The authorization contains a description of the information to be used or disclosed that identifies the information in a specific and meaningful way. If Allscripts intends to use or disclose substance abuse treatment program records, information about mental health or developmental disability services, HIV/AIDS test results or other highly confidential information, the patient specifically authorizes the use or disclosure of each type of highly confidential information (e.g., by checking or initialing the appropriate box on the authorization form).

2. The authorization contains the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

3. The authorization contains the name or other specific identification of the person(s), or class of persons, to whom Allscripts may make the requested use or disclosure.

4. The authorization contains a description of each purpose for which PHI is to be used or disclosed. This description must be specific enough to provide a patient with the facts that he/she needs to make an informed decision whether to allow release of the PHI. The statement "at the request of the individual" is a sufficient description of the purpose only when an individual initiate the authorization and does not (or elects not to) provide a statement of the purpose.

5. The authorization contains an expiration date or an expiration event that relates to the patient or purpose of the use or disclosure.

6. The authorization contains a statement of the patient's right to revoke the authorization in writing and either:
    a. A statement of the exceptions to the patient's right to revoke an authorization; and
    b. A description of how the patient may revoke the authorization; or
    c. A reference to Allscripts' Notice of Privacy Practices, if the Notice of Privacy Practices describes the exceptions to the patient's right to revoke an authorization and the authorization revocation process.

7. While State and Federal law prohibits the re-disclosure of certain records and information, the authorization contains a statement that PHI used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and may no longer be protected by the HIPAA privacy standards.

8. If the authorization is for a marketing activity and if Allscripts has received or will receive financial remuneration above costs in connection with such marketing activity, the authorization states that Allscripts is receiving financial remuneration in connection with such marketing activity.

9. The authorization contains a signature of the patient or the patient's authorized personal representative and the date of the signature.

10. If the authorization is signed by a personal representative of the patient, a description of such personal representative's authority to act for the patient is to be included.

B. Allscripts may not disclose PHI pursuant to an authorization without first verifying the validity of the authorization form under State and Federal law by consulting with the CPSC.

18.2 Revocation of Authorization

A patient may revoke an authorization at any time. To revoke an authorization, the patient submits the revocation in a writing that specifies the authorization to be revoked. A revocation is effective immediately unless the patient specifies a future date in his or her written revocation. The revocation is not valid where Allscripts has already relied upon the authorization.

18.3 Documentation Requirements

The CPSC retains the original authorization from the patient or patient's representative.

18.4 Historical Patient Information

Notwithstanding the foregoing, if approved by the CPSC and in accordance with contractual requirements, Allscripts may use or disclose PHI that it created or received prior to April 14, 2003 pursuant to an authorization or other express legal permission obtained from a patient prior to April 14, 2003 if:

1. The authorization or other express legal permission specifically permits such use or disclosure, and
2. There is no agreed upon restriction in accordance with Section 17.0 of this Policy, Right to Request Additional Restrictions on Use or Disclosure of Protected Health Information.

19 Uses and Disclosures of Protected Health Information for Marketing Purposes

Allscripts generally does not use or disclose a patient's PHI for marketing Allscripts' or a third party's products or services. Questions or requests for exceptions shall be directed to the CPSC.

19.1 Exceptions to the General Rule on Marketing

Under certain circumstances, Allscripts may make a marketing communication without first obtaining a patient authorization. Allscripts does not need a patient authorization if the requirements of Section 19.2 of this document, Payment in Exchange for Marketing, are met and the communication is made to describe a health-related product or service that is provided by the Covered Entity making the communication.

19.2 Payment in Exchange for Marketing

A. The following are exceptions to the general rule on marketing described in Section 19.0 of this Policy:
    1. Communications made to an individual by a Covered Entity/provider during a face-to-face interaction
    2. To provide promotional gifts of only a nominal value to the individual
    3. Communications made to describe a healthcare-related product or service (or payment for the product/service) that is provided by the Covered Entity
    4. Communications made for the treatment of the individual
    5. Communications made for case management, care coordination, or to recommend alternative treatments/therapies, providers, or settings.

B. If the communication meets an exception under this Section, the CPSC assesses whether Allscripts receives or has received direct or indirect financial or other remuneration in exchange for making the communication, and whether such remuneration is a reasonable cost-based fee.

C. If Allscripts has not received financial or other remuneration or has received financial remuneration at a reasonable, cost-based fee for making the communication, the communication may be made.

D. If Allscripts has received financial or other remuneration for making the communication, the CPSC assesses whether such communication concerns only a drug or treatment currently provided to the patient receiving the communication, and whether the financial remuneration is a reasonable cost-based fee. If both requirements are met, the communication may be made.

19.3 Highly Confidential Information

Allscripts may not use or disclose substance abuse treatment program records, information about mental health or development disability services, HIV status, or other highly confidential information for marketing purposes unless permitted by the law requiring special protections for the highly confidential information or Allscripts has obtained a valid authorization.

19.4 No Remuneration

Allscripts may not request, receive, or pay cash or other remuneration in exchange for PHI, except that Allscripts may be paid for activities that involve the exchange of PHI that Allscripts undertakes on behalf of and at the specific request of a Covered Entity pursuant to a BAA. Other exceptions to this procedure are made on a case-by-case basis by the CPSC.

20 Limitations on the Sale of Protected Health Information

Allscripts does not directly or indirectly receive remuneration in exchange for PHI from a third-party unless in accordance with this Policy.

20.1 Patient Authorization

If Allscripts wishes to enter into a relationship with a third party by which it receives remuneration in exchange for an individual's PHI, Allscripts consults with the CPSC who determines whether an exception set forth in Section 20.2 of this Policy applies and whether an authorization from the Covered Entity client and the patient is required. If the CPSC determines that an exception does not apply, Allscripts obtains an authorization from the Covered Entity client and an authorization from the patient that permits Allscripts to receive

remuneration in exchange for the patient's PHI in accordance with Section 18 of this Policy, Uses and Disclosures of Protected Health Information for which an Authorization is Required, before providing the PHI to the third party.

20.2 Exceptions Not Requiring an Authorization

A. Allscripts may directly or indirectly receive remuneration in exchange for an individual's PHI without first obtaining the patient's authorization in accordance with Section 20.1 of this document if the purpose of the exchange is one or more of the following:

1. For public health activities, as described in 45 CFR 164.512(b);
2. For research and the price charged reflects the costs of preparation and transmittal of the data for such purpose;
3. For the sale, transfer, merger, or consolidation of all or part of the Covered Entity or Allscripts with another Covered Entity;
4. For remuneration that is provided by a Covered Entity to a Business Associate for activities involving the exchange of PHI that the Business Associate undertakes on behalf of and at the specific request of the Covered Entity pursuant to a BAA; or,
5. To provide an individual with a copy of the individual's PHI pursuant to Section 25.0 of this Policy, Right to Access Records.

21 Minimum Necessary Protected Health Information for Routine Disclosure

The purpose of this section is to provide information for management and workforce members to conform to the requirements regarding the use and disclosure of the minimum amount of PHI necessary to provide services and support to Covered Entity clients and to ensure that management and workforce members have access to the information necessary for their jobs.

21.1 Requirements

As indicated in Section 23 of this document, Minimum Necessary Access to Protected Health Information by Job Description, Allscripts grants User IDs for accounts capable of accessing PHI only to those workforce members who need such information to perform their job duties. If Allscripts workforce members have questions regarding the minimum amount of PHI necessary for a particular use or disclosure, such workforce members contact the CPSC

21.2 Minimum Necessary Requirements

A. Except with regard to use and disclosure of PHI as otherwise set forth in Section 21.3 of this Policy, Allscripts workforce members may use or disclose only the minimum amount

of information necessary to perform the payment and healthcare operations activities on behalf of Covered Entity clients or Allscripts Covered Entity activities permitted under Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information.

B. In determining whether the amount of PHI requested is the minimum necessary for a specific payment or healthcare operation purpose, Allscripts workforce members may rely, if reasonable under the circumstances, on statements by public officials, other Covered Entities or their Business Associates that they are requesting the minimum PHI necessary to achieve the stated purpose of the request. Allscripts workforce members also may rely on the statements of Allscripts' own Business Associates or professionals within its workforce (such as IT security executives, attorneys, or internal auditors) that the information requested to provide professional services to Allscripts is the minimum necessary for such purposes.

C. Allscripts workforce members may disclose the following amounts of PHI in each of the contexts described herein:
    1. Allscripts workforce members may disclose such information to its Business Associates as contractually agreed to between Allscripts and each Business Associate.
    2. In performing the following activities, also known as "standard transactions," Allscripts workforce members may disclose information contained in the standard Centers for Medicare and Medicaid Services (CMS) billing form and in mandatory or situational fields of HIPAA-required electronic transaction format (current version of National Council for Prescription Drug Programs), as may be amended from time to time:
        a. Healthcare claims or equivalent encounter information,
        b. Healthcare payment and remittance advice,
        c. Coordination of benefits,
        d. Healthcare claim status,
        e. Eligibility,
        f. Referral certification or authorization, and
        g. Health claims attachments.

21.3 Exceptions to Minimum Necessary Requirement

The minimum necessary standard does not apply in the following circumstances:

1. Disclosures to a Covered Entity client regarding the Covered Entity client's patients to the extent necessary for services and support.
2. Uses or disclosures made pursuant to an authorization.
3. Uses or disclosures made in mandatory or situational fields of a HIPAA transactions standard (e.g., those elements set forth by the National Council for Prescription Drug Programs).
4. Disclosures to the Department of Health and Human Services (HHS) when required by HHS for compliance and enforcement purposes.
5. Uses or disclosures that are required by law.

21.4 Entire Medical Record

As a general rule, Allscripts may not use, disclose or request an entire medical record of a patient unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

21.5 Department of Health and Human Services (HHS) Guidance

To the extent practicable, Allscripts abides by HHS guidance on what constitutes "minimum necessary" amount of PHI for a purpose once issued. Such guidance is required by the Health Information Technology and Economic and Clinical Health (HITECH) Act.

22 Determining Minimum Necessary Protected Health Information for Non-Routine Disclosures

When using or disclosing PHI, and when requesting PHI from another entity, Allscripts workforce members shall make reasonable efforts to use, disclose or request the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure or request.

22.1 Determining Whether to Make a Non-Routine Disclosure of Protected Health Information

A. In making a determination as to whether a non-routine disclosure of PHI should be made, the CPSC, assesses the request based on criteria that includes the following:

    1. Determines who is receiving the information and the purpose for the proposed disclosure.
    2. Confirms that the applicable documents, including contracts, permit the requested use and/or disclosure.
    3. Verifies the identity or authority of the Requestor, as required by Section 29.0 of this Policy, Verification of Identity or Authority.
    4. Determines whether HHS has issued a minimum necessary guidance that is relevant to the proposed disclosure and follows the guidance, if practicable.
    5. Determines the minimum necessary PHI to accomplish the requested purpose under the following criteria:
        a. The purpose of the request or disclosure;
        b. The nature and extent of PHI requested or to be disclosed;
        c. The trustworthiness of the person who receives the PHI;
        d. Whether the disclosure presents a risk of financial or other harm to the patient;
        e. The extent to which requested PHI can be extracted from the rest of the record without undue burden and without viewing unnecessary parts of the record; and,

f. The immediacy or urgency of the need for the PHI

B. In making this determination, the CPSC may rely on statements, if reasonable under the circumstances:

1. By public officials, other Covered Entities or their Business Associates, that they are requesting the minimum PHI necessary to achieve the stated purpose of the request; and,
2. Of Allscripts' own Business Associates or professionals within its workforce that the information requested to provide professional services to Allscripts represents the minimum necessary for such purposes.

23 Minimum Necessary Access to Protected Health Information by Job Description

A. Allscripts employees and other workforce members may only access PHI that they need to perform their job functions. To the extent technically feasible, Allscripts implements technical controls and other safeguards to assure that workforce members only access the PHI necessary for their job functions.

B. Allscripts grants User IDs for accounts capable of accessing PHI only to those workforce members who need such information to perform their job duties.

C. When granting new access to PHI, Allscripts determines the proper scope of access to PHI.

24 Dissemination of Notice Privacy Practices

As a healthcare clearinghouse and Business Associate, Allscripts is not required by the HIPAA Privacy Rule to maintain and disseminate a Notice of Privacy Practices. (See 45 CFR 164.520.)

25 Right to Access Records

A. Patients have the right, at their own expense, to receive a copy of the PHI that Allscripts maintains in a designated record set, for as long as Allscripts maintains the designated record set.

B. Generally, Allscripts does not maintain designated record sets for its Covered Entity clients, and all requests from patients for access to records in a designated record set shall be forwarded directly to the Covered Entity client to respond.

25.1 Receipt of an Oral Request to Access Records

When an oral request is received by Allscripts from a patient seeking to access his/her records, Allscripts shall direct the patient to his/her healthcare provider to review and respond to the request.

25.2 Granting Access to Protected Health Information

25.2.1 Process

The following actions will be taken when the Covered Entity client directs Allscripts to provide the Covered Entity client access to a patient's designated record set, in whole or in part.

1. Covered Entity client requests Allscripts, in writing to copy the patient's designated record set.
2. The Covered Entity client may request a copy of the PHI in an electronic format and may direct Allscripts to transmit the copy directly to an entity or person designated by the Covered Entity client (based on the patient's request), provided that the choice is clear, conspicuous, and specific. Allscripts may impose a fee for providing the Covered Entity client with a copy of the PHI if such copy is in an electronic form that is no greater than Allscripts' labor costs in responding to the request for the copy.
3. Allscripts provides the electronic copy of the PHI, in a secure manner, via traceable means, e.g., FedEx, secure VPN with audit trail, in person with signed receipt, to the Covered Entity client or other entity or individual as the Covered Entity client may direct.

25.2.2 Fee Schedule

The Business Unit maintains a fee schedule. The fee may only include the cost of the following:

1. Copying, including the cost of supplies for and labor of copying the PHI requested; and,
2. Postage, if the patient has requested the copy, summary, or the explanation is mailed.

25.3 Denial of Access to Protected Health Information

There are several exceptions to a patient's right to access his/her enrollment form and invoice records. The Covered Entity client determines whether a request for access from a patient will be denied.

25.3.1 Notification of Denial

The Covered Entity client is responsible for notifying the patient if his/her request is denied.

25.3.2 Patient Requested Review of Denial

If a patient requests a review of a denial, such request for review of denial shall be promptly forwarded to the appropriate Covered Entity client for review and response.

26 Accounting of Disclosures

Upon request, Allscripts workforce members, in consultation with the CPSC, provide Covered Entity clients with a written accounting of uses and disclosures of an individual patient's PHI made by Allscripts as required by law. However, such accounting need not include the following disclosures of PHI by Allscripts, if such disclosures are known to Allscripts:

1. Made for treatment, payment, or healthcare operations purposes;
2. Made to the individual;
3. Made to caregivers of the individual;
4. Incident to a use or disclosure otherwise permitted or required by this Policy
5. Pursuant to a valid authorization;
6. For national security or intelligence purposes;
7. To correctional institutions or law enforcement officials; or
8. As part of a Limited Data Set

26.1.1 Disclosure Log Maintenance

A. On an on-going basis, the CPSC or his/her designee, maintains a properly secured log of each type of disclosure for which an accounting is required. These include disclosures made pursuant to the following sections of this Policy:

   1. Section 4.0 Disclosure and Review of Privacy Violations Committed by a Business Associate
   2. Section 8.0 Disclosure of Protected Health Information as Required by Law
   3. Section 9.0 Disclosure of Protected Health Information for Certain Public Health Activities
   4. Section 10.0 Disclosure of Protected Health Information for Certain Health Oversight Activities
   5. Section 11.0 Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings
   6. Section 12.0 Disclosure of Protected Health Information for Law Enforcement Purposes
   7. Section 14.0 Disclosure of Protected Health Information in Situations Presenting a Serious Threat to Health or Safety
   8. Section 15.0 Disclosure of Protected Health Information as Necessary to Comply with Workers' Compensation Laws

B. Allscripts workforce members are responsible for notifying the CPSC when PHI disclosures pursuant to one of the Sections above are made.

26.1.2 Disclosure Log Contents

Such log contains information that is disclosed in an accounting, which includes the following:

1. The date of the disclosure;
2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed; and,
4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement, a copy of a written request for disclosure, if any.

26.1.3 Disclosure Log Security

The log itself, because it contains protected information, is secured from unauthorized access, disclosure of modification, and, if in electronic form, is maintained in the same manner as protected ePHI.

26.1.4 Documentation

The CPSC is responsible for accounting of PHI disclosures by documenting such disclosures, and documenting and maintaining a copy of the following:

1. The required information to be included in an accounting of disclosures.
2. The written accounting that is provided to the Covered Entity client for the individual requesting an accounting of disclosures.
3. The titles of the persons or offices responsible for receiving and processing requests for an accounting by Covered Entity clients for patients.

26.1.5 Timing of Requests

A. The CPSC acts on a Covered Entity client's request for an accounting for a specific individual no later than 30 days after receipt of such requests or as otherwise agreed to with the Covered Entity client in writing.

B. Within the required time, the CPSC provides the Covered Entity client with the accounting requested; or, if he/she is unable to provide the accounting within the time period, he/she may extend the time to provide the accounting by up to 30 days, provided that the following occur:

    1. The CPSC, within the time, provides the Covered Entity client with a written statement of the reasons for the delay and the date by which he/she will provide the accounting; and,

2. The CPSC uses only one such extension of time for action on a request for an accounting.

26.2 Process

The following describes the actions taken when Allscripts workforce members receive an oral request for an accounting:

1. If the request is from a patient or patient's representative, directs the individual to make the request to the patient's healthcare provider.
2. Promptly directs written requests for an accounting to the CPSC.
3. The CPSC works with the Covered Entity client and other appropriate Allscripts team members to accommodate the request for an accounting in accordance with this Policy/procedure and the BAA with the Covered Entity client.
4. *Exception*: Allscripts temporarily suspends a Covered Entity client's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides Allscripts with a written statement that such an accounting to the Covered Entity client would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
5. If the agency or official statement is made orally, Allscripts shall: (a) document the statement, including the identity of the agency or official making the statement; (b) promptly inform the CPSC or Chief Compliance Counsel of the agency or official statement; (c) temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and, (d) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

26.3 Content of the Accounting

A. If Allscripts makes multiple disclosures during the period covered by the accounting, the CPSC provides a summary accounting to the Covered Entity client requesting the accounting on behalf of an individual.

B. Multiple disclosures include the following:
   1. For a single purpose to the Department of Health and Human Services for the purpose of ascertaining Allscripts' compliance with the rules; or,
   2. To the same person or entity for a single "national priority purpose," defined as:

      1. Disclosures required by law;
      2. Disclosures for certain public health activities;
      3. Disclosures for certain health oversight activities;
      4. Disclosures made pursuant to judicial or administrative proceedings;
      5. Disclosures for law enforcement purposes;
      6. Disclosures for military or national security purposes;

7. Disclosures deemed necessary to comply with laws governing workers' compensation; and,
8. Disclosures made in situations presenting a serious threat to health or safety.

C. When a summary accounting is provided, it contains the following information:
    1. The information required for the first disclosure during the accounting period;
    2. The frequency, periodicity, or number of the disclosures made during the accounting period; and,
    3. The date of the last such disclosure during the accounting period.

26.4 Charges and Fees

A. Allscripts provides the first accounting to a Covered Entity client in a 12-month period without charge.

B. Allscripts may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same Covered Entity client within the 12-month period, provided that Allscripts carries out the following:

    1. Informs the Covered Entity client in advance of the fee; and,
    2. Provides the Covered Entity client with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

27 Right to Request Amendment of Protected Health Information

Covered Entity clients may, if Allscripts maintains the Designated Record Set" (DRS) for the Covered Entity client, request that Allscripts amend information collected and maintained about Covered Entity clients' patients in the DRS for as long as the PHI is maintained in the DRS by Allscripts. Generally, Allscripts does not maintain DRS on behalf of its Covered Entity clients. However, in some limited circumstances, Allscripts may have responsibility for maintaining the Covered Entity client's DRS. Allscripts requires Covered Entity clients seeking amendment of PHI maintained in the DRS by Allscripts to make a request to amend the PHI in writing and to provide reasoning to support the request for amendment. A patient seeking amendment to his/her PHI in the DRS shall be referred to the healthcare provider to receive and review the patient's request. Allscripts workforce members shall, without delay, refer written requests to amend PHI to the CPSC.

27.1 Amendment Requests

27.1.1 Granting an Amendment Request

The following steps will be taken when an amendment request is granted:

1. Covered Entity client, in writing, submits or approves a requested amendment, in whole or in part.
2. CPSC, or delegate, directs appropriate Allscripts workforce members to make the appropriate amendment to the PHI that is the subject of the request.
3. Allscripts amends the PHI or record by identifying the records in the DRS that are affected by the amendment and appends or otherwise provides directions to the location of the amendment.
4. CPSC directs appropriate Allscripts workforce members to inform the Covered Entity client of the completed amendment in a timely manner.

27.1.2 Another's Granting of an Amendment

The following steps will be taken if Allscripts is informed by a payer or non-Covered Entity client provider of an amendment that it has made to an individual's PHI within the outside entity's DRS:

1. Direct the information to the CPSC.
2. CPSC directs appropriate Allscripts workforce members to notify Covered Entity client of the amendment.
3. If the Covered Entity client decides to amend its DRS, follow process in 28.1.1 of this Policy.

27.2 Denying an Amendment Request

Generally, Allscripts does not maintain a DRS on behalf of Covered Entity clients. It is the Covered Entity's responsibility to maintain its own DRS. Denial of an amendment request is the responsibility of the Covered Entity provider and not Allscripts. Workforce members shall instruct individuals requesting amendments to their PHI to contact their healthcare providers directly.

27.3 Written Denial

Denial of an amendment request is the responsibility of the Covered Entity-provider and not Allscripts.

27.4 Written Statement of Disagreement

The following steps will be taken if a written statement of disagreement is received (and if Allscripts is responsible for any action related to this statement of disagreement):

1. Promptly forward written statement of disagreement to the CPSC.
2. Within 5 business days or as otherwise agreed to in the BAA, CPSC forwards the statement to the Covered Entity client to review and respond directly to the patient.

3. Covered Entity client may submit to the CPSC written direction for Allscripts to append or otherwise links the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any, to the designated record set.
4. Within 5 business days of receiving written direction from Covered Entity client per above, the CPSC directs appropriate Allscripts workforce members to include the patient's request for an amendment, the denial of the request, the patient's statement of disagreement and the rebuttal, if any, or an accurate summary of such information, with subsequent disclosure of the PHI to which the disagreement relates.

28 Right to Request Alternative Communications

Allscripts workforce members shall refer requests made by patients to receive disclosures of PHI by Allscripts by alternative means or at alternative locations to a patient's healthcare provider. Allscripts shall inform any patient seeking to receive a disclosure of PHI by alternative means or alternative locations that the patient must submit such request directly to his/her healthcare provider.

29 Verification of Identity or Authority

The purpose of this section is to provide information for management and workforce members of the procedure that is followed when disclosing PHI to an unknown requestor.

29.1 Identity and Authority of a Public Official

29.1.1 In-Person Contact

When a public official requests PHI in person on a visit to/inspection of Allscripts, Allscripts workforce members require such official to present his/her agency identification in the form of a badge, other official credentials, or other proof of government status.

29.1.2 Written Statement

For requests made in writing by a public official, Allscripts requires a written statement on appropriate government letterhead that the person requesting the PHI is acting under the government's authority. Such written statement shall be forwarded to the CPSC without delay.

29.1.3 Requests Connected to a Judicial or Administrative Proceeding

Requests made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority and is processed in accordance with Section 12.0, Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings (if no State action is involved) or Section 13.0, Disclosure of Protected Health Information for Law Enforcement Purposes (if State action is involved).

29.1.4 Disclosures under Technical HIPAA Policy Exceptions

A request for a disclosure under the following technical HIPAA exceptions is processed in accordance with the documents referenced below or referred to the CPSC for approval prior to the disclosure:

1. Disclosures required by law – Section 9.0 this Policy, Disclosures of Protected Health Information as Required by Law;
2. Disclosures for public health activities – Section 10.0 of this Policy, Disclosures of Protected Health Information for Certain Public Health Activities;
3. Disclosures for health oversight activities – Section 11.0 of this Policy, Disclosures of Protected Health Information for Certain Healthcare Oversight Purposes;
4. Disclosures to law enforcement officials – Section 13.0 of this Policy, Disclosures of Protected Health Information for Law Enforcement Purposes;
5. Disclosures for health or safety – Section 15.0 of this Policy, Disclosures of Protected Health Information in Situations Presenting a Serious Threat to Health or Safety;
6. Disclosures for specialized government functions (such as military and veteran's activities, for national security and intelligence activities and for protective services for the president and others) – Section 14.0 of this Policy, Disclosure of Protected Health Information for Military or National Security Purposes;
7. Disclosures to comply with workers' compensation programs – Section 16.0 of this Policy, Disclosures of Protected Health Information as Necessary to Comply with Workers' Compensation Laws;
8. Disclosures to report victims of abuse, neglect or domestic violence are approved by CPSC, in consultation with the Covered Entity client, in advance of the disclosure;
9. Disclosures about decedents are approved by the CPSC, based upon written permission by the Covered Entity client, in advance of the disclosure;
10. Disclosures to facilitate organ and tissue procurement are approved by the CPSC, based upon written permission from the Covered Entity client, in advance of the disclosure; or,
11. Disclosures to correctional institutions about inmates or other individuals are approved by the CPSC, based upon written direction from the Covered Entity client, in advance of the disclosure.

29.2 Identity and Authority of Private Persons

29.2.1 Written Contact

The following describes how Allscripts verifies the identity or authority of a private person writing to request PHI on his/her own behalf:

1. Attempt to identify the individual's healthcare provider.
2. Forward to the healthcare provider, by secure means, the written request from the patient.
3. Promptly forward to the CPSC, by secure means, the written request from the patient.
4. If unable to identify the individual's healthcare provider, so notify the CPSC.
5. CPSC shall determine if it is appropriate to contact the person to inform him/her to contact his/her provider directly.

29.2.2 Telephone Contact

Allscripts teams most likely to receive calls from patients shall be trained to direct patients directly to their healthcare providers for any change, release, amendment to PHI.

30 Internal Enforcement of Privacy and Security Requirements

The following describes the actions taken when a possible violation has occurred as set forth in this Policy and Allscripts Code of Conduct:

1. CPSC, CSO, or Allscripts Compliance receives a report of possible privacy and/or security violations by a workforce member.
2. Investigation of complaint conducted by CPSC, CSO, and/or Allscripts Compliance.
3. Upon determination that an employee has committed a privacy and/or security violation CPSC, in consultation with CSO, Chief Compliance Counsel, business manager, and/or Human Resources, consider relevant evidence in considering what constitutes appropriate disciplinary action, including the following:
    a. The work history of the employee;
    b. The severity of the violation; and,
    c. Allscripts general disciplinary practices
4. Employee is subject to appropriate disciplinary action as determined by employee's manager, legal counsel, and Human Resources.
5. CPSC takes appropriate action to mitigate, to the extent practicable, harmful effect that is known to Allscripts officials stemming from a use or disclosure of PHI in violation of the BAA, HIPAA/HITECH, this Policy, and other Allscripts requirements.

30.1 Sanctions

A. Sanctions imposed are those that may be imposed under Allscripts policy and include, but are not limited to, the following:
    1. Informal counseling
    2. Verbal warning
    3. Written warning
    4. Suspension
    5. Termination

B. When determining an appropriate disciplinary action recommendation, the CPSC will consider relevant evidence, including the work history of the employee and the severity of the breach.

C. The final sanction imposed is at the discretion of the individual's manager. A record of the event and discipline imposed is maintained in the employee's Human Resources file.

31 Handling Privacy-Related Complaints

The following describes the actions taken when a Covered Entity client or patient alleges that Allscripts has violated its obligations to the Covered Entity client under contract, BAA, the HIPAA Privacy Rule, or other State or Federal law dealing with privacy or confidentiality of health information:

1. Instruct the individual that a complaint (aka Redball) may be filed with the Chief Compliance Counsel of Allscripts or the Speak Freely Help Line (866.353.6238)
2. Upon receiving a privacy-related complaint the CPSC, in consultation with the CSO, and/or Chief Compliance Counsel, undertakes an investigation to determine whether a breach of privacy has occurred.
3. If a breach of privacy has been determined to have occurred, CPSC, in consultation with CSO, Chief Compliance Counsel, and Human Resources determines appropriate disciplinary action to recommend, or other appropriate steps to mitigate any harm or otherwise remedy any issues.
4. Employees or workforce members found to be in violation of these requirements or who breach the confidentiality of a patient's PHI are subject to disciplinary action, up to and including termination or dismissal.

32 Training on HIPAA-Related Standard Operating Procedures

A. Allscripts Workforce members attend and complete applicable education, training, and/or courses as defined and required by Allscripts. Any Workforce member who is required

or likely to access PHI as a part of his/her job duties must complete all required HIPAA training prior to accessing any PHI. The CPSC, in collaboration with Human Resources, directs all Allscripts Workforce members to receive such training within 30 days of joining Allscripts workforce. Allscripts management shall conduct a periodic review of this Policy and train department Workforce members on requirements applicable to job duties.

B. If training cannot be completed within the first 30 days of employment, an exception must be sought and received in writing from the Chief Compliance Counsel.

33 Maintenance of HIPAA-Required Documentation

The following describes the information Allscripts retains, in writing or in electronic copy, as documentation of its compliance with the requirements of the HIPAA Privacy Rule.

1. Right to Request Additional Restrictions on Use or Disclosure of PHI. Six (6) Years
2. The logbook of information required to be included in an accounting, as set forth in Section 26.0 of this Policy
3. Accounting of Disclosures. Six (6) Years
4. Copies of written accounting provided to an individual. Six (6) Years
5. Signed authorizations. Six (6) Years

33.1 Titles of Persons Responsible

Allscripts hereby documents the following titles of persons responsible for certain HIPAA compliance activities, as required by the Privacy Rule.

1. Chief Privacy & Security Counsel
2. Chief Security Officer
3. Chief Compliance Counsel

34 Document Information

34.1 Attachments

None.

34.2 Regulatory References

- 45 CFR Parts 160, 162 and 164 - Health Insurance Portability and Accountability Act (“HIPAA”)

- Pub. L. No. 111-5, Title XIII - Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009 ("HITECH")
- 45 CFR Parts 160 and 164 – Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

34.3 Policy References

- Allscripts Privacy Policy
- Allscripts Information Security Policy
- Allscripts Privacy & Security Incident Response Policy
- Allscripts Global Information Classification and Handling Policy
- Allscripts Code of Conduct
- Allscripts Associate Handbook (for each geographic region)

35 Definitions

"HIPAA Terms" - Allscripts adopts the definitions in 45 CFR §160.103 and 45 CFR §164.103, the HIPAA Privacy and Security Rules. In the event a definition in this Policy is in conflict with the HIPAA Privacy and Security Rules, the Rules shall take precedence.

"Business Unit" is a formally defined area of Allscripts representing a specific business function (such as Finance, Solutions Development, Sales, Support, etc.). This could be a department or subset of a department.

"CPSC" is the Chief Privacy & Security Counsel who is also the Chief Privacy Officer.

"CSO" is the Chief Security Officer and is the individual designated in writing to act on behalf of Allscripts for all administrative, physical, and technical security issues as defined in 45 CFR §164.308(a)(2).

"**Designated Record Set (DRS)**" is defined at 45 CFR 164.501.

"Individually Identifiable Health Information" means information, including demographic information, related to:

- an individual's past, present or future physical or mental health condition;
- the provision of health care to an individual; or,
- the past, present, or future payment for provision of health care to an individual that identifies an individual or for which there is a reasonable basis to believe that it can be used to identify an individual. Individually Identifiable Health Information includes common patient identifiers.

"Privacy Policy" refers to the Allscripts Privacy Policy that provides the framework for safeguarding and protecting Sensitive Information, including PHI for the Company.

"Privacy Procedures" directly support the Privacy Policy and this HIPAA Privacy Policy and are a detailed set of instructions for various groups of individuals, such as the general Workforce, management, Human Resources, and Business Units. These

procedures outline the detailed steps, establish timelines, and document specific behaviors for Workforce members who are required to comply with this Policy.

"Protected Health Information (PHI)" means Individually Identifiable Health Information held or transmitted by a Covered Entity or its business associate, in any form or media, whether it is electronic, paper or oral.

"Sensitive Information" is a class of data, that relates to an identified or identifiable individual or entity that is sensitive, confidential, or proprietary to such person or entity and may potentially cause harm to such person or entity if lost or accessed, or used or disclosed by unauthorized persons, either internal or external to Allscripts. "Sensitive Information" includes, but is not limited to, Protected Health Information, Personal Information, Personal Health Information, Personal Data, and Personally Identifiable Information (as those terms are defined in applicable law).

"Systems" are any computing assets that may create, access, or store sensitive data, including those used internally and those developed and sold as a product.

"Workforce" and/or "**Workforce Member"** means full-time or temporary employees, contractors, third party users, volunteers, interns, trainees, agents, and other persons whose conduct, in the performance of work for Allscripts, is under the direct control of Allscripts, whether they are on-site or off-site, and whether or not they are paid by Allscripts.