Allscripts Enterprise

INFORMATION PRIVACY & SECURITY POLICIES: HIPAA PRIVACY POLICY

Revision: 8.0

Approval Date: August 02, 2021

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
28-Jul-20	7.0	Annual review, clarification and alignment of responsibilities, removed duplicative information and requirements covered in other Policies	P&S Team
08-Jul-21	8.0	Annual review, minor edits for clarity	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
12-Aug-20	7.0	PSEC
02-Aug--21	8.0	PSEC

Allscripts

Table of Contents

1 Purpose and Scope

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 PHI 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 Workforce members are required to comply with this Policy. Individuals who violate these requirements are subject to disciplinary action, up to and including termination or dismissal in accordance with the Progressive Disciplinary Action for Compliance Violations Policy.

1.3 Responsibilities

A. Chief Privacy & Security Counsel:

1. Ensures that requirements in this Policy are maintained in accordance with HIPAA, 45 CFR Parts 160 and 164 and any amendments and rules.

2. Provides advice and consultation to Workforce members regarding the requirements in this Policy.

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

5. 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.

6. Advises Workforce members when assistance is requested by vendors who access PHI.

7. 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/or General Counsel.

8. Leads investigations to determine whether a privacy incident has occurred.

9. 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.

10. Ensures that record retention and destruction information is included in the Allscripts Record Management Policy and Retention Schedule for certain documentation as required by HIPAA.

11. 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.

12. Directs the investigation of privacy-related complaints and ensures appropriate retention of records related to the investigation.

13. Conduct a review of this Privacy Policy and related corporate policies, standards, and procedures annually or each time there is a significant and material change in laws or regulations regarding the privacy of Sensitive Information.

14. In collaboration with Human Resources, designs and ensures the provision of adequate training to all Workforce members, including to every new hire as a part of the on-boarding process, on this Policy and related policies and procedures.

Ensures that the proper documentation exists to verify completion of such training by Workforce members.

15. Recommends disciplinary action for any Workforce member who fails to comply with Allscripts Privacy and Security Policies.

16. 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 PHI, which must be done in accordance with the Allscripts PHI Use and De-Identification Policy and Procedure.

2. Consults the CPSC or other Privacy Counsel for any questions about this Policy, how to comply with this Policy, or other privacy matters.

3. Reports any privacy or security incident that might constitute a violation of a Business Associate Agreement (BAA) 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. 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

A. Allscripts provides reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy, confidentiality, integrity, and availability of PHI.

B. Allscripts must obtain reasonable written assurances that its Business Associates will appropriately use and disclose PHI by requiring appropriate safeguards including policies, procedures and practices.

C. 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 allowed by the Data Use Agreement.

3 When Business Associate Agreements are Necessary

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 may also include 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

C. Other types of Business Associates may include the following:
   1. Health Information Organizations
   2. E-prescribe Gateways
   3. One that offers Personal Health Records to individuals on behalf of a Covered Entity
   4. Patient Safety Organizations
   5. Subcontractors
   6. 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 counsel.
   3. CPSC/Legal counsel 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 Violation of a Business Associate Agreement

A. In the event any Workforce member becomes aware of any issue with a Business Associate that may constitute a violation or breach of the Business Associate's obligations under its contract or HIPAA, the Workforce member must report the matter as required by the Allscripts Privacy and Security Incident Response Policy.

B. Allscripts shall take reasonable steps to cure the breach or to end the violation, as described below.

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

The following actions will be taken when there is a potential violation of a BAA by Allscripts when acting as a Business Associate or by an Allscripts Business Associate:

A. Upon discovery of a potential violation of a BAA, including suspected or confirmed unauthorized access, use or disclosure of PHI, the individual who discovered the potential violation (Workforce member, vendor, etc.) reports as required by the Allscripts Privacy and Security Incident Management Policy.

B. CPSC investigates to determine the scope of the suspected or confirmed unauthorized access, use or disclosure and whether additional action is necessary.

C. If the CPSC determines that the unauthorized access, use or disclosure was material, CPSC works with the applicable business unit to cure the violation and perform any required notifications.

D. If an Allscripts Business Associate fails to cure a violation or continues to violate the requirements of the BAA, the 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 appropriately protect PHI.

5 De-Identification of Protected Health Information

A. In some circumstances, 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 in accordance with the Allscripts PHI Use and De-identification Policy.

6 Permitted Uses and Disclosures of Protected Health Information

A. Workforce members may use or disclose PHI 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 incident to such use or disclosure.

B. Subject to the Minimum Necessary requirement described in this Policy, Workforce members may use and disclose 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.

7 Disclosure of Protected Health Information as Required by Law

7.1 Requirements

Allscripts is permitted to make disclosures of PHI without an authorization pursuant to the applicable requirements of 45 C.F.R. §164.512 including, but not limited to:

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

Workforce members shall direct these requests to the CPSC or Chief Litigation Counsel, who determines whether or not the PHI may be released without an authorization.

7.2 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, Workforce members shall:

A. Follow Section 10.0 of this Policy, Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings, if the request is made by a non-governmental official.

B. Follow Section 11.0 of this document, Disclosure of Protected Health Information for Law Enforcement Purposes, if the request is made by a governmental official or a person acting on behalf of a governmental official.

8 Disclosure of Protected Health Information for Certain Public Health Activities

A. Generally, Workforce members may use or disclose PHI only in accordance with Section 6.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information.

B. 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.

C. Such requests shall be reviewed and approved by Allscripts Privacy Counsel before any PHI is shared.

9 Disclosure of Protected Health Information for Certain Health Oversight Activities

A. As a general rule, Workforce members may not disseminate PHI other than as provided in Section 6.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information, without authorization from the Covered Entity client or the patient. In addition, 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.

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

9.1 Compliance with Legal and Professional Standards

A. Workforce members shall report conduct that may be unlawful or otherwise violates professional standards to the Chief Compliance Counsel or Compliance Speak Freely Line.

B. If a 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 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.

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

In the event a Workforce member receives 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 Chief Litigation Counsel or Allscripts Privacy Counsel. Note: Requests must be in writing.

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

11 Disclosure of Protected Health Information for Law Enforcement Purposes

11.1 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 Chief Litigation Counsel, CPSC, or General Counsel to evaluate and respond to the request.

11.2 Law Enforcement Delay

If a law enforcement official notifies Allscripts that an action otherwise required under HIPAA would impede a criminal investigation or cause damage to national security, Chief Litigation Counsel, CPSC or General Counsel shall:

1. Delay such action for the time period specified by the law enforcement official; or
2. If the statement is made verbally, Chief Litigation Counsel, CPSC or General Counsel 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 verbal statement, unless a written statement as described above is submitted during that time.

11.3 When Protected Health Information can be Disclosed by Workforce Members

Workforce members may disclose PHI for a law enforcement purpose to a law enforcement official in the following circumstances after approval by Chief Litigation Counsel, CPSC or General Counsel:

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 8.0 of this Policy, Disclosure of Protected Health Information for Certain Public Health Activities or domestic violence governed by Section 13.0 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 5.0 of this Policy, De-Identification of Protected Health Information.

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

Workforce members may not disseminate PHI except as provided in Section 6.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information. If 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 Chief Litigation Counsel, CPSC or General Counsel, who determines whether to disclose PHI in response to the request.

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

In the event Workforce members receive a request for disclosure of PHI for one of the reasons below, such Workforce members shall direct the request to the Chief Litigation Counsel, CPSC or General Counsel, who determines whether to disclose PHI in response to the request.

- Abuse, neglect, or domestic violence;
- Serious threat to the health or safety of the public;
- 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);
- A crime other than abuse, neglect, or domestic violence;
- Criminal conduct is suspected in the death of an individual; and,
- A crime has taken place on Allscripts premises.

14 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 or Employment Counsel, reviews and responds to the request.

Workforce members may only 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 authorized by Human Resources.

15 Use of Limited Data Sets

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

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 Allscripts Privacy Counsel, in a written agreement signed by both the Covered Entity client and Allscripts.

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

Patients requesting restrictions on Uses and Disclosures of their PHI are informed that such requests must be made directly to their providers. Written requests from patients for restrictions on Uses and Disclosure of their PHI shall be promptly forwarded to the patient's healthcare provider. The provider is responsible for reviewing and responding to the patient's request.

17 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. Allscripts Privacy 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 24.0 of this Policy, Right to Access Records, rather than the procedure outlined below.

17.1 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 Privacy Counsel.

17.2 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.

17.3 Documentation Requirements

The Business Unit that receives the request shall retain the original authorization from the patient or patient's representative.

17.4 Historical Patient Information

Notwithstanding the foregoing, if approved by Allscripts Privacy Counsel 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 16.0 of this Policy, Right to Request Additional Restrictions on Use or Disclosure of Protected Health Information.

18 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. The following are potential exceptions to this general rule. Questions or requests for exceptions shall be directed to Allscripts Privacy Counsel.

- Communications made to an individual by a Covered Entity/provider during a face-to-face interaction
- To provide promotional gifts of only a nominal value to the individual
- Communications made to describe a healthcare-related product or service (or payment for the product/service) that is provided by the Covered Entity
- Communications made for the treatment of the individual
- Communications made for case management, care coordination, or to recommend alternative treatments/therapies, providers, or settings.

18.1 Payment in Exchange for Marketing

A. Under certain circumstances, Allscripts is permitted to make a marketing communication without first obtaining a patient authorization. Allscripts does not need a patient authorization if the requirements of this section 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.

B. If the communication meets an exception under this Section, Allscripts Compliance Counsel 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, Allscripts Compliance Counsel 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.

18.2 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 a valid authorization has been obtained.

18.3 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 Allscripts Compliance Counsel.

19 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.

19.1 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 Privacy Counsel determines whether an exception set forth in the section below applies and whether an authorization from the Covered Entity client and the patient is required. If Privacy Counsel 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 17 of this Policy, Uses and Disclosures of Protected Health Information for which an Authorization is Required, before providing the PHI to the third party.

19.2 Exceptions Not Requiring an Authorization

Allscripts may directly or indirectly receive remuneration in exchange for an individual's PHI without first obtaining the patient's authorization 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 24.0 of this Policy, Right to Access Records.

20 Minimum Necessary Protected Health Information for Routine Disclosure

20.1 Minimum Necessary Requirements

A. Except as described in the next Section, 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 6.0 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, 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. Workforce members also may rely on the statements of Allscripts' own Business Associates or certain professionals within its Workforce (such as IT security professionals, attorneys, or internal auditors) that the information requested to provide professional services to Allscripts is the minimum necessary for such purposes.

C. Workforce members may disclose the following PHI in each of the contexts described herein:
   1. 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," 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.

20.2 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.

20.3 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.

20.4 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.

21 Non-Routine Disclosures of Protected Health Information

In making a determination as to whether a non-routine disclosure of PHI should be made, Allscripts Privacy Counsel 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 28.1 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.

In making this determination, Allscripts Privacy Counsel 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 certain professionals within its workforce that the information requested to provide professional services to Allscripts represents the minimum necessary for such purposes.

22 Minimum Necessary Access to Protected Health Information by Job Description

A. 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.

23 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).

24 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. All requests from patients for access to records held by Allscripts shall be forwarded directly to the Covered Entity client to respond or the patient shall be advised to contact their healthcare provider.

24.1 Granting Access to Protected Health Information

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 reasonable fee for providing the Covered Entity client with a copy of the PHI.
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.

24.2 Denial of Access to Protected Health Information

The Covered Entity client determines whether a request for access from a patient will be denied. The Covered Entity client is responsible for notifying the patient if his/her request is denied. 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.

25 Accounting of Disclosures

Upon request, Workforce members, in consultation with the CPSC, shall 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 is not required to 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.

25.1 Logging of Disclosures

A log of required disclosures shall be maintained. These may include disclosures made pursuant to the following sections of this Policy:

1. Section 4.0 Disclosure and Review of Privacy Violations Committed by Allscripts or an Allscripts Business Associate
2. Section 7.0 Disclosure of Protected Health Information as Required by Law
3. Section 8.0 Disclosure of Protected Health Information for Certain Public Health Activities
4. Section 9.0 Disclosure of Protected Health Information for Certain Health Oversight Activities
5. Section 10.0 Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings
6. Section 11.0 Disclosure of Protected Health Information for Law Enforcement Purposes
7. Section 13.0 Disclosure of Protected Health Information in Situations Presenting a Serious Threat to Health or Safety
8. Section 14.0 Disclosure of Protected Health Information as Necessary to Comply with Workers' Compensation Laws

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.

25.2 Timing of Requests

A. The request recipient 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 recipient 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 recipient, 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 recipient uses only one such extension of time for action on a request for an accounting.

25.3 Process

The following describes the actions taken when Workforce members receive a 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. The recipient works with the Covered Entity client and other appropriate Workforce members to accommodate the request for an accounting in accordance with this Policy/procedure and the BAA with the Covered Entity client.

3. *Exception*: Allscripts temporarily suspends a Covered Entity client's right to receive an accounting of disclosures for the time specified by a health oversight agency or law enforcement 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 specifies the time for which such a suspension is required. If a verbal statement is received from an agency or official, 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 verbal statement, unless a written statement is submitted during that time.

25.4 Content of the Accounting

A. If Allscripts makes multiple disclosures during the period covered by the accounting, Allscripts 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:

      a. Disclosures required by law;
      b. Disclosures for certain public health activities;
      c. Disclosures for certain health oversight activities;
      d. Disclosures made pursuant to judicial or administrative proceedings;
      e. Disclosures for law enforcement purposes;
      f. Disclosures for military or national security purposes;
      g. Disclosures deemed necessary to comply with laws governing workers' compensation; and,
      h. 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.

25.5 Charges and Fees

Allscripts may impose a reasonable fee for each request for an accounting by a Covered Entity client.

26 Right to Request Amendment of Protected Health Information

If Allscripts maintains the Designated Record Set (DRS) for a Covered Entity client, Allscripts shall amend information collected and maintained about Covered Entity clients' patients in the DRS for as long as the PHI is maintained by Allscripts. Allscripts requires Covered Entity clients seeking amendment of PHI to make a request to amend in writing and to provide reasoning to support the request. Workforce members shall, without delay, direct patients requests for amendment to either contact their healthcare provider directly or refer such requests to the Covered Entity client.

26.1 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, Compliance Counsel, or his/her delegate, directs 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, Compliance Counsel, or his/her delegate directs appropriate Workforce members to inform the Covered Entity client of the completed amendment in a timely manner.

26.2 Another's Granting of an Amendment

If a third-party request that Allscripts make an amendment of a DRS held by Allscripts, the request will be forwarded to the applicable Covered Entity client. If the Covered Entity client decides to amend its DRS, follow process in 26.1 of this Policy.

26.3 Denying an Amendment Request

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

27 Right to Request Alternative Communications

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.

28 Verification of Identity or Authority

28.1 Identity and Authority of a Public Official

28.1.1 In-Person Contact

When a public official requests PHI in person on a visit to/inspection of 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.

28.1.2 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. Workforce members who receive such a written statement shall forward it to the Chief Litigation Counsel, CPSC or General Counsel without delay.

28.2 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 10.0, Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings (if no State action is involved) or Section 11.0, Disclosure of Protected Health Information for Law Enforcement Purposes (if State action is involved).

28.3 Disclosures under Technical HIPAA Policy Exceptions

A request for a disclosure under the following technical HIPAA exceptions is processed in accordance with the relevant sections of this Policy or referred to Allscripts Privacy Counsel for approval prior to the disclosure:

1. Disclosures required by law;
2. Disclosures for public health activities;
3. Disclosures for health oversight activities;
4. Disclosures to law enforcement officials;
5. Disclosures for 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);
7. Disclosures to comply with workers' compensation programs;
8. Disclosures to report victims of abuse, neglect or domestic violence;
9. Disclosures about decedents;
10. Disclosures to facilitate organ and tissue procurement; or,
11. Disclosures to correctional institutions about inmates or other individuals.

29 Internal Enforcement of Privacy and Security Requirements

The following describes the actions taken when a possible violation of this Policy or the Allscripts Code of Conduct has occurred:

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, the CPSC, in consultation with CSO, Chief Compliance Counsel, business

manager, and/or Human Resources, considers 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 in accordance with the Allscripts Progressive Disciplinary Action for Compliance Violations Policy.
   Sanctions may include, but are not limited to, the following:
   a. Informal counseling
   b. Verbal warning
   c. Written warning
   d. Suspension
   e. Termination
5. CPSC directs 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 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 may be filed with the Allscripts Chief Compliance Counsel via the Speak Freely Ethics & Compliance hotline from the US and Canada at 866-206-1906 or from any location using the webform at https://ethcomp.com/Allscripts
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 an unauthorized disclosure has been confirmed, 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. 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.

31 Training on HIPAA-Related Standard Operating Procedures

A. 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 PHI. The CPSC, in collaboration with Human Resources, directs all

Workforce members to receive such training within 30 days of joining Allscripts workforce. Allscripts management shall 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.

32 Maintenance of HIPAA-Required Documentation

Allscripts shall maintain records as required by HIPAA for six (6) years. Refer to Allscripts Records Management Policy and Retention Schedule for further retention requirements.

33 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 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.

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 in 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 Allscripts 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.