

---

INFORMATION PRIVACY & SECURITY POLICIES:  
PRIVACY POLICY

---



---

**REVISION 3.0 October 27, 2015**

---

Reproduction and distribution of this document without the express written permission of Allscripts Healthcare Solutions, Inc. is strictly prohibited. The methodology and models presented herein are proprietary and copyrighted by Allscripts Healthcare Solutions, Inc. and/or its affiliates.

## Summary of Changes

Date	Version	Summary of Changes	Author
August 7, 2014	2.0	Revision of entire policy to encompass international business requirements.	Wright/Ross/Carter
<b>October 27, 2015</b>	3.0	Technical and editorial modifications to the policy.	Wright/Ross/Carter

## Approval Log

Date	Version	Authority
April 2012	1.0	PSEC
August 7, 2014	2.0	PSEC
<b>October 27, 2015</b>	3.0	PSEC

## Table of Contents

Table of Contents .....	2
1.0 Purpose and Scope.....	4
1.1 Applicability .....	4
2.0 Exceptions .....	4
3.0 Policy Framework .....	4
3.1 Policy Document .....	4
3.2 Regulatory Standards Mapped to this Policy .....	4
4.0 Risk Assessment and Treatment .....	6
4.1 Assessing Privacy Risk.....	6
4.2 Treating Privacy Risks .....	6
4.3 Related Policies, Procedures or Other Documents.....	7
5.0 Privacy Policy.....	7
5.1 Policy Availability .....	7
5.2 Review Cycle .....	7
5.3 Policy Retention .....	7
6.0 Organization of Privacy.....	8
6.1 Executive Commitment .....	8
6.2 Workforce Responsibilities .....	8
6.3 Managers’ Responsibilities.....	8
6.4 Business Units and Functional Areas .....	9
6.5 Chief Privacy & Security Counsel.....	9
6.6 Human Resources .....	10
7.0 Permitted Uses and Disclosures of Sensitive Information .....	11
7.1 Consent and Authorization .....	11
7.2 De-identifying Sensitive Information.....	11
7.3 Disclosures Required by Law .....	11
8.0 Training .....	12
9.0 Reporting and Handling of Complaints and Incidents.....	12
10.0 Disposal of Sensitive information .....	12
11.0 Human Resources Privacy Requirements.....	12
12.0 Definitions .....	12

## 1.0 Purpose and Scope

1.0.1 The purpose of this Privacy Policy (“Privacy Policy”) is to outline the key high-level privacy policies that are applicable to the confidentiality of confidential and proprietary information, Protected Health Information (“PHI”), Personally Identifiable Information (“PII”), Personal Information (“PI”), Personal Data (“PD”) and/or other sensitive information (collectively, “Sensitive Information”) at Allscripts Healthcare Solutions (“Allscripts”) and as required under Health Insurance Portability and Accountability Act (“HIPAA”) and Health Information Technology for Economic and Clinical Health Act (“HITECH”), as well as applicable international law.

1.0.2 It is the policy of Allscripts to comply with all regulatory requirements for the use, access and disclosure of Sensitive Information, to ensure the confidentiality and protection of Sensitive Information, and to prevent and mitigate any privacy incidents by limiting or reducing their potential impact.

1.0.3 Allscripts’ executive management supports this Privacy Policy and requires that all members of the Workforce (as defined in Section 12.11) comply with and follow these requirements and related procedures with respect to Sensitive Information.

1.0.4 This Privacy Policy shall become effective upon publication.

### 1.1 Applicability

All members of the Workforce shall be required to comply with this Policy. This Privacy Policy is applicable to all Allscripts’ global operations.

## 2.0 Exceptions

Exceptions to this Privacy Policy may be granted by the Chief Privacy & Security Counsel (“CPC”) (defined in Section 12.2) or his/her designee.

## 3.0 Policy Framework

### 3.1 Policy Document

Allscripts has implemented the following fair information privacy principles that support individual rights and set guidelines for the protection of Sensitive Information:

3.1.1 Notice. Allscripts shall provide notice regarding its privacy policies and procedures and include the purposes for which Sensitive Information is accessed, collected, used, retained, and disclosed. Notice may occur in a variety of formats including publication on Allscripts’ internal and external websites and specified in internal and external contracts and agreements.

3.1.2 Choice and Consent. Where practical or required by law or contract,



Allscripts shall provide individuals with opportunity to consent to or authorize Allscripts' access, collection, use, retention, and disclosure of Sensitive Information. Consent or authorization may be explicit or implicit depending upon the specific circumstances, and the CPC shall advise the Business Units (as defined in Section 12.1) as to appropriate means of obtaining consent or authorization.

3.1.3 Limited Collection. Sensitive Information shall only be collected for the purposes identified in the notice.

3.1.4 Limited Use and Disclosure. Sensitive Information shall only be used and/or disclosed to third parties for the purposes identified in the notice.

3.1.5 Limited Retention. Sensitive Information may be retained only as long as necessary, including, but not limited to, as may be required by law or contract, to fulfill a valid business purpose.

3.1.6 Accuracy. Allscripts shall maintain the accuracy and integrity of the Sensitive Information under its care.

3.1.7 Right to Inspect/Correction. Individuals may request access to their Sensitive Information and request amendment to that Sensitive Information if such information is believed to be inaccurate. Allscripts shall review and respond to requests for access and amendment in a timely manner. The CPC shall provide guidance to Business Units regarding individual rights to access and/or amend Sensitive Information upon request by the Business Unit.

3.1.8 Disposal. Allscripts shall dispose and destroy Sensitive Information, at the end of the applicable retention period, in a manner that prevents the likelihood of restoration of the Sensitive Information or in a manner required by law or contract.

3.1.9 Training. Workforce members shall be provided training on this Privacy Policy.

3.1.10 Breach Notification. Actual or suspected breaches of Sensitive Information shall be immediately reported in accordance with the Privacy and Security Incident Reporting Policy.

3.1.11 Accountability. Violations of this Privacy Policy may result in discipline up to and including termination, in compliance with Human Resources policies.

3.1.12 This Privacy Policy is reviewed and approved by Allscripts' Chief Compliance Counsel, the CSO, Legal, and the Privacy and Security Executive Council (PSEC).

### 3.2 Regulatory Standards Mapped to this Policy

Laws and regulations relevant to this Policy include, but are not limited to, the following:

- Health Insurance Portability and Accountability Act (“HIPAA”) of 1996 (US)
- Health Information Technology for Economic and Clinical Health (“HITECH”) Act of 2009 (US)
- Federal Trade Commission Act (US)
- Children’s Online Privacy Protection Act of 1998 (US)
- Privacy Act (Australia)
- Privacy Act of 1983 (Canada)
- Personal Information Protection and Electronic Documents Act (“PIPEDA”) (Canada)
- European Union Data Protection Directive (EU)
- Organization of Economic Co-operation and Development Guidelines
- Asia-Pacific Economic Cooperation Privacy Framework
- Personal Data Protection Act (Singapore)
- Information Technology Act of 2008 (India)
- Protection of Privacy Law of 1981 (Israel)

## 4.0 Risk Assessment and Treatment

### 4.1 Assessing Privacy Risk

An integral part of this Privacy Policy includes the assessment of risk. Risk Assessments shall include the identification, quantification and prioritization of risks as follows:

4.1.1 Identify. Assess what negative events, consequences or threats could occur if a vulnerability or weakness is exploited. Risks shall be identified at enterprise-wide, departmental, and operational levels.

4.1.2 Quantify. Identified risks shall be quantified to determine the *probability* and *consequence* of occurrence. Quantified risks enable the organization to make appropriate decisions with regards to the treatment of risks.

4.1.3 Prioritize. The quantified risks shall be prioritized based on criteria as defined by the CPC for privacy risks. The Chief Compliance Counsel shall evaluate the prioritization of risks to ensure they are in alignment with Allscripts’ business objectives.

4.1.4 Privacy Risk Assessments shall be conducted on a defined periodic basis, at least annually.

### 4.2 Responding to Privacy Risks

4.2.1 Once risks have been identified, validated, quantified, and prioritized, an action plan will be created to address the risk. This plan will be reviewed and approved by the Chief Compliance Counsel and implemented and

monitored by the CPC and his or her delegates.

4.2.2 Risk response measures shall include the evaluation of the tangible and intangible impacts of the identified risk(s) against the tangible and intangible costs of the risk(s) treatment.

4.2.3 Measurement of the performance of implemented risk responses shall be performed utilizing metrics as defined by the CPC and the Chief Compliance Counsel.

### **4.3 Related Policies, Procedures or Other Documents**

- Information Security Management Policy
- HIPAA Privacy Policy

## **5.0 Privacy Policy**

### **5.1 Policy Availability**

This Privacy Policy shall be made available to the Workforce through Allscripts management, the Intranet, formal training programs, and other appropriate mechanisms.

### **5.2 Review Cycle**

5.2.1 The CPC shall review the privacy requirements for the organization. The CPC shall be responsible for conducting an annual review of this Privacy Policy and all related corporate policies, standards, and procedures. A review shall also occur each time there is a significant and material change in laws or regulations regarding the privacy of Sensitive Information.

5.2.2 Requests for changes or modifications to this Privacy Policy may be submitted by a member of the Workforce in writing to the CPC.

5.2.3 The CPC and the Chief Compliance Counsel shall determine whether or not the requested change or modification should be included in the Privacy Policy.

5.2.4 The CPC shall submit material changes or modifications for approval to the Allscripts legal team for review prior to presentation to the PSEC.

### **5.3 Policy Retention**

This Privacy Policy, as well as any procedures supporting this Privacy Policy, and all previous versions shall be maintained for a minimum of six (6) years after the latest effective date, even if superseded, or longer if required by a legal, regulatory, or contractual requirement.

**6.1 Executive Commitment**

Allscripts' executive leadership agrees that maintaining the privacy and security of Allscripts, the Workforce, client PHI, and other Sensitive Information is essential to Allscripts' business and reputation and to operating in a responsible, compliant manner. Accordingly, the Executive Leadership affirmatively approves and supports this Privacy Policy, including the designation of a Privacy Officer.

**6.2 Workforce Responsibilities**

Each Workforce member shall be responsible for:

6.2.1 Reading and understanding the contents of this Privacy Policy and its related policies and procedures;

6.2.2 Ensuring that his or her actions comply with the requirements of this Privacy Policy and its related policies and procedures;

6.2.3 Completing any role-based training on the requirements in this Privacy Policy and its related policies and procedures;

6.2.4 Collaborating with all levels of the Allscripts organization to ensure that an effective privacy program is implemented and maintained;

6.2.5 Seeking assistance if uncertain how to comply with the requirements of this Privacy Policy and its related policies and procedures;

6.2.6 Demonstrating to his or her understanding of and compliance with this Privacy Policy and its related policies and procedures through the annual training and certification or through any other means used by Allscripts for such certification;

6.2.7 Complying with the Security Policy and related policies and procedures and implementing and maintaining the Security Program; and

6.2.8 Reporting any violations of this Privacy Policy, related policies or procedures or the law or regulations to the CPC, CSO, Chief Compliance Officer, Human Resources representative, Allscripts management, and/or the Compliance Reporting Line or Incident Reporting Line.

**6.3 Managers' Responsibilities**

Each Allscripts manager shall be also be responsible for:

6.3.1 Ensuring that all members of the Workforce reporting directly or indirectly to such manager have read, understand, been trained on, and comply





with, this Privacy Policy and its related policies and procedures;

6.3.2 Completing required privacy training and ensuring any and all members of the Workforce who report directly or indirectly to such manager have completed the required privacy training;

6.3.3 Ensuring that this Privacy Policy and its related policies and procedures are fully implemented in his or her functional area of responsibility; and

6.3.4 Inquiring of Privacy Counsel and/or Human Resources for guidance on implementing this Privacy Policy as a manager.

6.3.5 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, without limiting the generality of the foregoing, compliance with security measures required by the Security Policy and other guidance issued by the Chief Privacy & Security Counsel and Chief Security Officer

#### **6.4 Business Units and Functional Areas**

Each Business Unit or functional area shall be additionally responsible for:

6.4.1 Identifying any privacy-related contractual requirements mandated or requested by external clients or third party vendors, and not previously approved by the legal team and the CPC, and providing those requirements or requests to the legal team and the CPC prior to contract execution;

6.4.2 Maintaining a list of all Workforce members who have access to Sensitive Information and approving access by Workforce members to any Sensitive Information in a manner consistent with such Workforce members' duties and responsibilities; and

6.4.3 Documenting and maintaining procedures to implement this Privacy Policy within its own Business Unit.

#### **6.5 Chief Privacy and Security Counsel**

The Chief Privacy and Security Counsel shall be responsible for:

6.5.1 Developing, implementing and maintaining this Privacy Policy and related policies and procedures within Allscripts;

6.5.2 Coordinating with the CSO in the development and maintenance of security policies and programs to ensure that appropriate physical, administrative and technical safeguards are in place to protect the privacy and security of Sensitive Information;

6.5.3 Upon request, reviewing, guiding, and approving Standard Operating Procedures (SOPs) for Business Units and functions, relating to Sensitive Information; and,

6.5.4 Designing and ensuring the provision of adequate training to all Workforce members, including to every new hire as a part of the on-boarding process, on applicable privacy and security requirements under HIPAA, HITECH, PIPEDA, EU Data Protection Act, and other applicable international laws;

6.5.5 Receiving and reviewing complaints related to this Privacy Policy and related procedures or the requirements for the handling of Sensitive Information under any applicable U.S. or international law, including documenting the complaint and disposition thereof;

6.5.6 Coordinating with Human Resources to recommend appropriate discipline for violations of this Privacy Policy;

6.5.7 Reviewing and responding to requests from law enforcement and regulatory agencies for access to Sensitive Information, in coordination with others to the extent permitted and as appropriate; and

6.5.8 Ensuring that Allscripts complies with applicable privacy laws, regulations, and contractual privacy requirements.

## **6.6 Human Resources**

Human Resources shall be responsible for:

6.6.1 Together with the CPC, designing, documenting, and enforcing a disciplinary policy for non-compliance with or violation of this Privacy Policy and related policies and procedures;

6.6.2 Ensuring that Workforce members reporting violations of this Privacy Policy, related policies or procedures or the law are protected from retaliation;

6.6.3 Collaborating with hiring managers to ensure privacy and security obligations are specified in Allscripts job and roles descriptions; and

6.6.4 Communicating job status changes including termination of Workforce members to IT Operations so that access to systems with Sensitive Information is appropriately modified.

## **7.0 Permitted Uses and Disclosures of Sensitive Information**

### **7.1 Consent and Authorization to Use Sensitive Information**

7.1.1 All members of the Workforce shall safeguard, maintain the confidentiality of and protect any Sensitive Information in accordance with the requirements of this Privacy Policy, other applicable policies and procedures, relevant contractual requirements, and as required by law.

7.1.2 Limited Collection. Workforce members shall only collect, request, or access the minimum amount of Sensitive Information necessary to serve a valid business purpose and in accordance with the requirements of this Privacy Policy, other applicable policies and procedures, relevant contractual requirements, and as required by law.

7.1.3 Limited Use. Allscripts Workforce members shall only access, use, and disclose Sensitive Information in accordance with:

7.1.3.1 the requirements of the consent or authorization provided by the subject or owner of the Sensitive Information;

7.1.3.2 the requirements of this Privacy Policy, or other applicable policies and procedures;

7.1.3.4 relevant contractual requirements; and

7.1.3.5 as required by law.

7.1.4 All access, use and disclosure of Sensitive information shall be limited to the minimum amount of Sensitive Information necessary to accomplish a valid business purpose.

7.1.5 All requests to limit or cease using Sensitive Information shall be directed to the CPC for review.

### **7.2 De-Identified Sensitive Information**

7.2.1 In certain cases, Allscripts may receive consent or authorization to de-identify Sensitive Information. In these cases, once the Sensitive Information has been de-identified, workforce members may use and disclose the de-identified Sensitive Information.

7.2.2 Requests to de-identify Sensitive Information must be submitted, in writing, to the CPC who will evaluate the scope and purpose of the request and the means of de-identification to ensure a low likelihood of re-identification of Sensitive Information and that applicable legal, contractual, and industry-standard requirements are met.

### **7.3 Disclosures Required by Law**

Allscripts may use or disclose Sensitive Information as required by law.

The CPC, in collaboration with Human Resources, shall develop a training program to train all members of the Workforce on this Privacy Policy and related policies and procedures. Such training program shall include the maintenance of a record of all Workforce members who complete required trainings.

## **9.0 Reporting and Handling of Complaints and Incidents**

For the purposes of this Privacy Policy, all privacy complaints and incidents shall follow Privacy and Security Incident Reporting Policy.

## **10.0 Disposal of Sensitive Information**

All electronic media and paper copies containing Sensitive Information shall be properly disposed of once the intended use has been completed. All media or copies containing PHI from a client is either to be returned to the client, or destroyed, in accordance with the contractual agreement with the client.

## **11.0 Human Resources Privacy Requirements**

11.1 Human Resources is responsible for ensuring that Workforce members' Sensitive Information is appropriately identified and protected in accordance with this Privacy Policy, applicable laws, regulations, and contractual requirements.

11.2 Allscripts operates a self-funded employee health plan. It has contracted with one or more third party administrators to administer this benefit plan. The employee health plan is a covered entity under HIPAA, and shall comply with the requirements of the Allscripts HIPAA Privacy Policy.

11.3 Allscripts shall provide a privacy notice to all employees who participate in the employee welfare benefit plan and shall provide authorization and release forms to employees for the use and disclosure of Sensitive Health Information, including PHI.

## **12.0 Definitions**

12.1 **“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.

12.2 **“CPC”** means the Chief Privacy and Security Counsel who is also the Chief Privacy Officer.

12.3 **“CSO”** means the Chief Security Officer.

12.4 **“Information”** is considered databases, data files, contracts, agreements, system documentation, research information, user manuals, training



material, standard operating procedures, business continuity plans, disaster recovery plans, third-party data, audit trails, and archived information.

12.5 **“Privacy Guidelines”** are documents that support this Privacy Policy but are not directive in nature. Guidelines are designed to provide members of the Workforce a recommended path to achieve compliance with Allscripts’ policy.

12.6 **“Privacy Policy”** refers to this formal statement by Allscripts’ executive management outlining the overall intention and direction of the safeguarding and protection of PHI and other Sensitive Information for Allscripts, including, but not limited to, affiliates of Allscripts. It is not intended to be detailed, but rather to serve as a capstone principle supported by subordinate documents (including, but not limited to, the Privacy Procedures and Privacy Standards).

12.7 **“Privacy Procedures”** directly support this 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 all Workforce members who are bound within this Privacy Policy’s scope to be in compliance.

12.8 **“Privacy Standards”** support this Privacy Policy by providing specific boundaries. Privacy Standards are focused and serve to establish a set of mandatory decision criteria for systems and processes. Privacy Standards are intended for a limited audience and are mandatory by definition. Privacy Standards do not normally require executive management approval and therefore are more fluid and may adapt to technology changes.

12.9 **“Sensitive Information”** is a subset of **Information which** contains data elements that may be regulated, controlled, or otherwise designated as not public and therefore must be protected, such as PHI. This includes privileged, personal, confidential or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it. “Sensitive Information” includes, but is not limited to, Protected Health Information, Personal Information, Personal Data, and Personally Identifiable Information (as those terms are defined in applicable law).

12.10 **“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 for our clients.

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