Allscripts Enterprise

INFORMATION PRIVACY & SECURITY POLICIES: PRIVACY POLICY

Revision:	v6.0
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
7-Aug-14	2.0	Revision of entire policy to encompass international business requirements.	Ross/Wright/Carter
27-Oct-15	3.0	Technical and editorial modifications to the policy.	Ross/Wright/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	P&S Team

Approval Log

Date	Version	Approval Authority
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

1.0 Purpose and Scope

The Allscripts Privacy Policy defines the requirements for the Allscripts Workforce to ensure the protection of confidential, sensitive, and proprietary information, including Protected Health Information ("PHI"), Personally Identifiable Information ("PII"), Personal Information ("PI"), Personal Data ("PD"), Personal Health Information, and/or other sensitive information (collectively, "Sensitive Information") at Allscripts and as required under applicable laws, as defined in Appendix A.

It is the policy of Allscripts to comply with all applicable laws and 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.

All members of the Workforce shall be required to comply with this Policy and it is applicable to all Allscripts' global operations. Individuals who violate these requirements are subject to disciplinary action, up to and including termination or dismissal.

2.0 Exceptions

Exceptions to this Privacy Policy may be granted by the Chief Privacy & Security Counsel ("CPSC") or his/her designee.

3.0 Privacy Principles

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

3.1 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.

3.2 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 CPSC shall advise the Business Units as to appropriate means of obtaining consent or authorization.

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

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

3.5 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.

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

3.7 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 CPSC shall provide guidance to Business Units regarding individual rights to access and/or amend Sensitive Information upon request by the Business Unit.

3.8 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.

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

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

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

4.0 Privacy Policy Requirements

4.1 Policy Availability

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

4.2 Review Cycle

4.2.1 The CPSC shall review the privacy requirements for the organization. The CPSC shall be responsible for conducting an annual review of this Privacy Policy and all related corporate policies, standards, and procedures. The CPSC may grant an exception for an annual review of this Privacy Policy. A review shall also occur each time there is a significant and material change in laws or regulations regarding the privacy of Sensitive Information. The CPSC shall submit material changes or modifications for approval to the Chief Compliance Counsel, the CSO, and Legal team for review prior to presentation for final review and approval by the Privacy and Security Executive Council (PSEC).

4.2.2 Requests for changes or modifications to this Privacy Policy may be submitted by a member of the Workforce in writing to the CPSC. The CPSC and the Chief Compliance Counsel shall determine whether the requested change or modification should be included in the Privacy Policy.

4.3 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.

5.0 Privacy Requirements

5.1 Executive Commitment

Allscripts' executive leadership agrees that maintaining the privacy and security of Allscripts, the Workforce, client PHI, PII, PD, PI, Personal Health Information, 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.

5.2 Workforce Responsibilities

Each member of the Allscripts workforce is responsible for the security of Sensitive Information in his or her workspace. Workforce members take reasonable and appropriate precautions to safeguard access to Sensitive Information including, without limiting the generality of the

following, compliance with security measures required by the Security Policy and other guidance issued by the Chief Privacy & Security Counsel and Chief Security Officer.

Each Workforce member shall be responsible for:

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

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

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

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

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

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

5.2.7 Reporting any violations of this Privacy Policy, related policies or procedures or the law or regulations to the CPSC, CSO, Chief Compliance Officer, Human Resources representative, Allscripts management, the Speak Freely Help Line (866.353.6238) and/or Redball reporting process.

5.3 Managers' Responsibilities

In addition to responsibilities as a member of the Workforce, each Allscripts manager shall be also be responsible for:

5.3.1 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;

5.3.2 Ensuring all members of the Workforce who report directly or indirectly to such manager have completed the required privacy training;

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

5.3.4 Requesting guidance from Human Resources or the CPSC on implementing this Privacy Policy as a manager if needed.

5.4 Business Units and Functional Areas

In addition to responsibilities as a member of the Workforce, each Business Unit or functional area leader shall also be responsible for:

5.4.1 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 CPSC, and providing those requirements or requests to the legal team and the CPSC prior to contract execution;

5.4.2 Identifying where Sensitive Information is located, and providing such information to the CPSC and/or CSO;

5.4.3. 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;

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

5.5 Chief Privacy and Security Counsel

The Chief Privacy and Security Counsel shall be responsible for:

5.5.1 Developing, implementing and maintaining this Privacy Policy and related policies and procedures;

5.5.2 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;

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

5.5.4 In collaboration with Human Resources, 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 this Privacy Policy, related policies and procedures, and the privacy and security laws and regulations of applicable jurisdictions;

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

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

5.5.7 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;

5.5.8 Ensuring that Allscripts complies with applicable privacy laws, regulations, and contractual privacy requirements;

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

5.6 Human Resources

Human Resources shall be responsible for:

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

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

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

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

6.0 Permitted Uses and Disclosures of Sensitive Information

All members of the Workforce shall safeguard 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.

6.1 Consent and Authorization to Use Sensitive Information

6.1.1 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.

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

6.1.2.1 the requirements of the consent or authorization provided by the subject or owner of the Sensitive Information;
6.1.2.2 the requirements of this Privacy Policy, or other applicable policies and procedures;
6.1.2.4 relevant contractual requirements; and
6.1.2.5 as required by law.

6.1.3 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.

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

6.2 De-Identified Sensitive Information

6.2.1 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 in accordance with the consent or authorization.

6.2.2 Requests to de-identify Sensitive Information must be submitted, in writing, to the CPSC or her/his designee 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.

6.3 Disclosures Required by Law

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

7.0 Privacy Risk Assessment

Allscripts shall assess Privacy Risk annually pursuant to Allscripts' Risk Management Policy.

8.0 Reporting and Handling of Privacy Complaints and Incidents

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

9.0 Disposal of Sensitive Information

All electronic media and paper copies containing Sensitive Information shall be retained in accordance with Allscripts Records Management Policy and Retention Schedule, and properly disposed of once the intended use has been completed in accordance with the Allscripts Information Classification and Handling Policy. 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.

10.0 Human Resources Privacy Requirements

10.1 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.

10.2 Allscripts operates a self-funded employee health plan for United States employees. 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.

10.3 Allscripts shall provide a privacy notice to all U.S. employees who participate in the self-funded health plan and shall provide authorization and release forms to employees for the use and disclosure of Sensitive Information, including PHI.

10.4 For countries other than the United States, Allscripts Human Resources will protect any health-related Sensitive Information obtained as a result of providing health-related benefits to employees in accordance with this Privacy Policy, applicable laws, regulations, and contractual requirements.

11.0 Definitions

11.1 **"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.

11.2 **"CPSC"** means the Chief Privacy and Security Counsel who is also the Chief Privacy Officer.

11.3 **"CSO**" means the Chief Security Officer.

11.4 **"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.

11.5 **"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.

11.6 **"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).

11.7 **"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.

11.8 **"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.

11.9 **"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).

11.10 **"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.

11.11 **"Workforce"** 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.

Appendix A – Applicable Regulatory Standards

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

- Health Insurance Portability and Accountability Act of 1996 (US)
- Health Information Technology for Economic and Clinical Health 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 (Canada)
- Personal Health Information Protection Act (Ontario, Canada)
- Personal Information Protection Act (Alberta, Canada)
- Health Information Act (Alberta, Canada)
- Personal Information Protection Act (British Columbia, Canada)
- E-Health (Personal Health Information Access and Protection of Privacy) Act, (British Columbia)
- Personal Information International Disclosure Protection Act, SNS 2006 c.3 (Nova Scotia)
- Freedom of Information and Protection of Privacy Act (Manitoba)
- Personal Health Information Act (Manitoba)
- Personal Health Information Protection Act (Ontario)
- Health and Information Protection Act (Saskatchewan)
- European Union Data Protection Directive (EU)
- General Data Protection Regulation (EU)
- Organization of Economic Cooperation 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)
- Data Protection Act of 2003 (Bahamas)
- Privacy Data Protection Regulations (Data Security), 5777-2017 (Israel)
- Law No. 20 of 2014 (Regarding Electronic Transactions) (Kuwait)
- Data Protection Act, 2012 (Act 843) (Ghana)