



CONFIDENTIALITY AND SECURITY AGREEMENT

In consideration of my assignment at Allscripts Healthcare, LLC, d/b/a Allscripts ("Allscripts") I understand and accept the following responsibilities:

A. Confidential Information

In the course of my assignment at Allscripts, I may handle or have access to Confidential Information. Such Confidential Information may include personal information of Allscripts' employees or customers that is required to be kept confidential to protect the privacy of the individuals to whom the information relates. Confidential Information also includes, without limitation, any data, computer software, invention, design, idea, concept, specification, formula, device, equipment, marketing or other strategic plans, internal processes, documents or materials, pricing policies, customer lists, and any other information which, in any way whatsoever, is a trade secret or confidential or proprietary in nature and which belongs to Allscripts or its partners, affiliates, and vendors, or is in the possession of Allscripts or any client or customer of Allscripts.

During my course of assignment and thereafter, I will hold all Confidential Information in trust and confidence, and I will not use, disclose, communicate or convey, or allow to be used, disclosed, communicated or conveyed, directly or indirectly, any such information, except as may be necessary in the performance of my duties. I understand that unauthorized disclosure could be highly damaging to Allscripts, its clients, employees, affiliates, or vendors. As such, I agree to:

- Treat all Confidential Information in a secret and confidential manner and comply with all applicable procedures established by Allscripts with respect to maintaining the secrecy and confidentiality of Confidential Information; and
- Use Confidential Information only as necessary and proper in the performance of my duties at Allscripts; and
- Provide such reasonable assistance as may be required by Allscripts, in the effort to maintain the secrecy and confidentiality of Confidential Information.
- I will not allow any unauthorized person or persons to inspect or have access to any document that is of a confidential nature, regardless of media format, and I will report any unauthorized access to my supervisor/manager as soon as I become aware that such an incident has occurred.
- I will not remove any records containing confidential information from Allscripts unless authorized to do so by my supervisor/manager and I will return such records to Allscripts upon termination of employment or as requested by my supervisor/college administrator.

B. Information Security

I understand that it is my responsibility to abide by and follow Allscripts' Information Security policy (Attached hereto as Exhibit A), which applies equally to employees, contractors, temporaries, as well as employees of third parties authorized to perform services at Allscripts.

C. Work Product

“Work Product” means any idea, invention, discovery, development, design, technique, improvement, plan, work of authorship, computer software, data, information, enhancement, or other work product, whether tangible or intangible, which is (i) in whole or in part conceived, made, developed, reduced to practice, prepared, or otherwise created by me, whether within or outside Individual’s normal hours of assignment, while on assignment with Allscripts and (ii) related to, concerned with, or arising out of the business or activities of Allscripts.

During the course of my assignment at Allscripts and at all times thereafter, I agree to the following:

- I will promptly and fully disclose all Work Product to my immediate supervisor at Allscripts.
- All Work Product shall be conclusively deemed to be conceived, made, developed, reduced to practice, prepared, or otherwise created within the scope of my assignment and shall, as between Allscripts and me, be the sole property of Allscripts; and I hereby irrevocably assigns to Allscripts all right, title, and interest of whatever nature that I may have in and to Work Product.
- I shall, at the expense of and on behalf of Allscripts, do all acts and things requested by Allscripts for Allscripts to obtain, establish, preserve, and protect Allscripts’ rights and interests in Work Product, including, but not limited to, preparing and signing such applications, papers, assignments, instruments, and other documents as Allscripts may deem necessary for it, or its nominee, to obtain and maintain patents, copyrights, trade secrets, trademarks, and service marks, within the United States of America and/or elsewhere.

D. Non-Solicitation

While on assignment with Allscripts and for a period of six (6) months following the end of such assignment, I will not, without Allscripts’ prior written consent, directly or indirectly: (i) solicit or cause to solicit any client or prospective client of Allscripts to purchase products competitive with Allscripts or (ii) solicit or cause to solicit other employees, agents, contractors, or subcontractors of Allscripts to leave the employment of Allscripts.

E. Independent Contractor

I understand that I am not an employee of Allscripts and am acting, during my assignment with Allscripts, as an independent contractor. I agree that I have no right or authority to assume, create, or incur any liability or any obligation of any kind, expressed or implied, against, or in the name of, or on behalf of Allscripts. This Agreement will not create any rights in any third party.

F. Delivery of Materials Upon Assignment Termination

Immediately upon the end of my assignment with Allscripts, I will deliver to Allscripts all correspondence, drawings, business plans, marketing plans, manuals, notes, notebooks, reports, flow-charts, computer software, proposals, papers, documents, and any other tangible information regardless of form or medium, in my possession or control, which relate to, are connected with, my assignment at Allscripts including, but not limited to, all Confidential Information and all Work Product.

G. Miscellaneous

I acknowledge that money damages may not adequately compensate Allscripts for the violation of any covenant contained in this Agreement, and that such violation may cause or threaten irreparable harm to Allscripts. I therefore agree that, upon a proper showing that such violation has occurred or is threatened, a court order enjoining such violation is a proper remedy in addition to any other remedies or damages

available to Allscripts. The rights, remedies, and protections afforded to Allscripts and any successors or assigns of Allscripts shall be in addition to and not in limitation of any rights, remedies, and protections provided at law or in equity.

This Agreement is for the benefit of and may be enforced by Allscripts, and Allscripts' successors and assigns. To the extent my assignment is transferred from Allscripts to an affiliated Allscripts company, this Agreement will automatically be transferred to such affiliate without the necessity for any amendment of this Agreement.

I acknowledge and agree that I may not assign or otherwise transfer any right, duty, or obligation under this Agreement without the prior written consent of Allscripts.

I acknowledge and agree that any failure to enforce any provision of this Agreement by Allscripts shall not constitute a waiver of such provision in any way or prevent Allscripts at any time from advantage of any remedies as it may have for any breach of such provision.

I acknowledge and agree that this Agreement shall be governed by the laws of North Carolina and that if any provision of this Agreement is judicially determined to be invalid or unenforceable as written, then such provision shall, if possible, be modified and reformed to the degree necessary to render it valid and enforceable. Further, any such invalidity or un-enforceability of any provision shall have no effect on the remainder of this Agreement which shall remain in full force and effect.

I HEREBY ACKNOWLEDGE THAT I HAVE READ THE ABOVE AGREEMENT IN ITS ENTIRETY, HAVE HAD THE OPPORTUNITY TO ASK QUESTIONS ABOUT THIS AGREEMENT AND UNDERSTAND AND AGREE TO EACH PROVISION OF THIS AGREEMENT. FURTHER, I UNDERSTAND NO AMENDMENT TO THIS AGREEMENT WILL BE EFFECTIVE UNLESS IT IS IN WRITING AND SIGNED BY BOTH ALLSCRIPTS AND ME.

SIGNED this _____ day of _____ 20_____.

Signature

Witness

Print Name

Print Name

Vendor Name

Note to Allscripts hiring manager – please scan and send signed agreement to ContractorSetupSupport@allscripts.com at the same time you submit any Contractor on-boarding forms.

EXHIBIT A

Acceptable Use Policy

1.0 Overview

Allscripts is committed to protecting our employees, partners and clients from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Allscripts. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every Allscripts employee, affiliate, contractor, and temporary employee who deals with information and/or information systems (“End User”). It is the responsibility of every End User to know these guidelines, and to conduct his/her activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Allscripts. These rules are in place to protect the End User and the company. Inappropriate use exposes Allscripts to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Allscripts, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Allscripts.

4.0 Policy

4.1 General Use and Ownership

1. While Allscripts network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Allscripts. Because of the need to protect Allscripts’ network, management cannot guarantee the confidentiality of information stored on any network device belonging to Allscripts.
2. End Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, End Users should be guided by departmental policies on personal use, and if there is any uncertainty, End Users should consult their supervisor or manager.
3. Information Security (“InfoSec”) recommends that any information that End Users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Allscripts Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Allscripts Awareness Initiative.

4. For security and network maintenance purposes, authorized individuals within Allscripts may monitor equipment, systems and network traffic at any time, per Allscripts Audit Policy.
5. Allscripts reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. End Users should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. End Users are responsible for the security of their passwords and accounts. System level passwords shall be changed quarterly; user level passwords should be changed every 60 days.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with InfoSec Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by End Users from an Allscripts email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Allscripts Healthcare Systems, unless posting is in the course of business duties.
7. All hosts used by the End User that are connected to the Allscripts Internet/Intranet/Extranet, whether owned by the End User or Allscripts, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy.
8. End Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. End User may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an End User of Allscripts authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Allscripts-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Allscripts.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Allscripts or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an Allscripts computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Allscripts account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the End User is not an intended recipient or logging into a server or account that the End User is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the End User's host, unless this activity is a part of the End User's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the End User's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, Allscripts Healthcare Systems employees to parties outside Allscripts Healthcare Systems.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Allscripts networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Allscripts or connected via Allscripts network.
7. Use of blogs, wikis, and message boards are not considered corporate communications and should not contain comments regarding Allscripts Healthcare Systems, Allscripts employees, clients, partners, or competitors.

5.0 Enforcement

Any End User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

| Term | Definition |
|-------------|-------------------|
|-------------|-------------------|

| | |
|-------------|--|
| <i>Spam</i> | Unauthorized and/or unsolicited electronic mass mailings |
|-------------|--|

| | |
|-------------|---|
| <i>Blog</i> | Information that is instantly published to a Web site |
|-------------|---|

| | |
|-------------|---|
| <i>Wiki</i> | A website that allows users to add/edit content |
|-------------|---|