

IS&T Access Request Security Agreement



PLEASE PRINT CLEARLY:

LAST NAME

FIRST NAME

MIDDLE INITIAL
(if no middle init, use "X")

Last 3 digits of Soc. Sec. #

1. Information Security

Access to Kaleida Health's information systems are subject to the Kaleida Health Corporate Information System Access Request Security Policy (Policy # IS.2). It is the policy of Kaleida Health to protect its information assets and to allow the use, access, and disclosure of such information only in accordance with its interests and applicable laws and regulations. It is Kaleida Health's legal and ethical obligation to protect the confidentiality of patient information. The purpose of this document is to establish the user's responsibility for safeguarding its computer hardware, software, and information assets in whatever form, such as but not limited to printed, audio, video, electronic, and oral communications. Information assets may be defined as any information within Kaleida Health's purview, including information which it may not own but which is governed by laws and regulations to which it can be held accountable. The use of any information must comply with Kaleida Health Policies and must comply with all federal and state or local laws and regulations including, but not limited to, HIPAA Security and Privacy regulations.

Access to any of Kaleida Health's systems is granted on a need-to-know basis. To accomplish this a user may be issued specific and confidential computer system ID's and/or passwords. These access identification codes may not be shared, disclosed or utilized by any other individual, inside or outside of Kaleida Health, including staff or people claiming to be staff of the Information System and Technology Division.

All printed information, as well as data storage media, including, but not limited to, microfiche, optical and magnetic storage media, is considered the property of Kaleida Health and is considered confidential matter. As such, this information shall not be shared, distributed, or stored in a careless manner.

The use of a computer or computer services without the permission of, or in excess of the permission of the owner or lessor, is prohibited by the Penal Law of the State of New York. The use of the Kaleida Health's network and/or computer systems for non-business purposes, or for personal gain, is prohibited. Users are required to preserve the security and confidentiality of any information assessable through the computer or network. Users are required to use all necessary and appropriate safeguards to prevent unauthorized use or disclosure of information they have access to. Users are permitted only to utilize or access information necessary for performance of their job. Use of technology can and will be monitored, thus limiting the potential for abuse. Users and department heads are responsible for notifying IST Security Services in the event of any change in user's responsibilities or the termination of user's services.

Intellectual Property Infringement

Copyright, trademark and patent infringement is strictly prohibited. The federal Copyright Act extends to much of what is transmitted over computer networks, such as text, pictures, music and software. Since copyright infringement is a strict liability crime, intent to infringe is not required.

Kaleida Health has purchased the right to use software on personal computers that is protected by federal copyright laws. At no time may this software be copied for use on a personal computer other than the one for which it was originally intended. Additionally, parts of MS-Office Professional and other "suites" can not be split across multiple PC's.

Only software purchased or authorized by Kaleida Health may be used on its computers. Software brought in from outside or downloaded from the Internet, may not be used without approval from the Information Systems and Technology Division, due to licensing issues, the potential exposure to computer viruses and the potential impact on the computer network. Kaleida Health has the right to monitor for compliance at any time and without prior notification.

Electronic Signature

Electronic Signatures are allowed for individuals with appropriate security levels in specific systems and/or application modules. For legal and medical reasons, the user of these systems must adhere to the security criteria setup to support and maintain the authentication of the electronic signature. The user must agree in writing to the fact that the "Electronic Signature" may be used instead of the traditional hand signature and must not be shared with anyone else.

2. Electronic Mail

The usage of Electronic Mail system is subject to the terms and conditions in the Corporate Information System E-Mail Policy and Procedures (Policy # IS.4) The Electronic mail system is the property of Kaleida Health and as such may be subject to disclosure for both business and legal purposes. Access to Kaleida Health's e-mail system is granted solely for the clinical and business purposes. All messages composed, sent or received on this system are and remain the property of the organization. Kaleida Health prohibits it to be used in any manner that would be disruptive to the operation or offensive to others. Any employee who receives sexually explicit or personally offensive materials electronically should report this to his or her supervisor and the Information Systems and Technology Division immediately. The use of electronic mail for transmission of information disparaging to others, for promotion of political causes or for personal gain is prohibited. Kaleida Health has the ability and right to monitor electronic mail at any time and without prior notification.

3. Internet Usage

Internet usage is subject to the terms and conditions in the Corporate Information System Internet Access Policy and Procedures (Policy # IS.5) The Internet is an international network of networks that connects businesses, government agencies, universities and individuals. It is considered a public network that poses additional risks to confidential information if proper precautions are not taken. For example, patient information transmitted via e-mail may be intercepted and disclosed without the knowledge of either the sender or receiver. For this reason it is recommended that all confidential information sent over the Internet be encrypted. As such the Internet can be an important professional tool.

Internet communications that are not authorized to represent the organization's opinions should convey this fact within the body of the communication. Such language should convey the fact the user's opinions are not to be attributed to the organization.

While recognizing that the Internet contains hundreds of thousands of sites with potentially useful information, it's also obvious that it contains thousands of sites containing material, which is offensive, obscene or illegal. Visiting, viewing or downloading material from any Web site containing pornographic, sexist, racist, illegal material or material which is offensive in any way is strictly prohibited. Kaleida Health has the ability and right to monitor Internet traffic at any time and without prior notification.

Breaches of information security, intellectual property, Internet usage, electronic mail and electronic signatures including the sharing of access codes, identifications, or passwords, or wrongful access to the Kaleida Health network or systems connected to that network, are viewed as serious violations. Users violating this policy will be subject to disciplinary action, which may include but is not limited to termination of access to the system and termination of employment. Violators are also subject to civil or criminal liability.

I have read, understand, and agree with the terms and conditions as stated in this document.

PRINT NAME

DATE

USER SIGNATURE