CARRA Data Warehouse Terms of Use
(version 2019-June-01)

The Childhood Arthritis and Rheumatology Research Alliance also d/b/a CARRA, Inc. ("**CARRA**"), a tax exempt 501(c)(3) corporation, is a North American organization of pediatric rheumatologists who is committed to advancing the health and quality of life of children living with rheumatic disease, and who has joined together to answer critical clinical research questions. The mission of the alliance is to prevent, treat and cure rheumatic diseases in children and adolescents through fostering, facilitating, and conducting high quality research.

Duke University ("**Duke**") and The Children's Hospital Corporation d/b/a Boston Children's Hospital ("**BCH**") are collaborating with CARRA under separate agreements to continue the Childhood Arthritis and Research Alliance Network Registry, first established in 2010 to develop and implement an investigator-sponsored infrastructure to enable observational, disease-related data capture for the major pediatric rheumatic diseases across now over 60 academic medical sites and centers (the "**CARRA Registry**"). Through funding from public and private sources, BCH has designed and developed the informatics for the CARRA Registry data warehouse ("**CARRA Data Warehouse**"), an informatics infrastructure that enables CARRA Registry investigators, other users appointed by and authorized at CARRA Registry sites, and other authorized researchers and users ("**Authorized Users**") to collect and access the data that has been obtained from research subjects at participating CARRA Registry sites ("**CARRA Research Data**") as well as data obtained from other studies ("**Extramural Research Data**"), together the "**Research Data**". Access to the CARRA Data Warehouse is through BCH's Virtual Private Network remote access or other BCH secure platforms ("**VPN**"). Data collection activities employ various platforms for electronic data capture system utilized by BCH ("**EDC**") such as REDCap (Vanderbilt University, Nashville, TN), and others provided by Duke such as Rave (Medidata Solutions, New York, NY).

Scope of Terms:

These Terms of Use, as may be modified from time to time ("**Terms**"), constitute legally binding terms and apply to Your use of the CARRA Data Warehouse. By providing data to, or accessing and/or using the CARRA Data Warehouse, You (i) agree to be bound by these Terms and all applicable laws, rules and regulations, including but not limited to the Health Insurance Portability and Accountability Act of 1996, as amended ("**HIPAA**"), as defined in 45 Code of Federal Regulations (CFR) §164.514(e)(2) ("**Applicable Law**"); (ii) certify that You are a permitted Authorized User and that you have otherwise been given the proper authorization to access the CARRA Data Warehouse; and (iii) agree that You shall use the CARRA Data Warehouse solely for the purpose of accessing Research Data as contemplated by the CARRA Registry Site Data Use and Transfer Agreement ("**CARRA Registry Site DUA**"), the Registry Site Agreement ("**Site Agreement**"), and/or the CARRA Data Warehouse Extramural Data Use and Transfer Agreement ("**CARRA Extramural DUA**") or as otherwise specified by other applicable agreement for CARRA Data Warehouse access executed between You and Duke, CARRA and/or BCH (together the "**Related Agreements**").

You also certify that you have read and agree to the guidelines for data access and publication as outlined in the CARRA Data and Biospecimen Release and Terms of Use Conditions and the CARRA Publication and Presentation Policy guidelines posted on the CARRA Policies webpage (https://carragroup.org/members/policies-and-templates) by which Research Data may be shared and disclosed ("**CARRA Guidelines**") and accept that they may be amended from time to time without prior notice.

BCH reserves the right to modify these Terms at any time, and from time to time, and each such modification shall be effective upon posting on the CARRA Policies webpage (https://carragroup.org/members/policies-and-templates). All material modifications will apply prospectively only. Your continued use of the CARRA Data

Warehouse following any such modification constitutes Your agreement to be bound by and Your acceptance of these Terms as so modified. It is therefore important that You review these Terms with each use of the CARRA Data Warehouse. If You do not agree to be bound by these Terms and to abide by all Applicable Law, You must discontinue use of the CARRA Data Warehouse website immediately.

1. In order to access the CARRA Data Warehouse and BCH VPN, You agree to the following:

a) Access. BCH grants You use and access to CARRA Data Warehouse through VPN based solely on Your representations herein. You certify that all such representations are complete and accurate.

b) Remote Access Policy. When accessing the CARRA Data Warehouse through VPN, You agree to adhere to all BCH security policies and guidelines for computer use and may be held accountable for any security breach to the supported system or other BCH computer resources caused by Your use of and access to the CARRA Data Warehouse. You agree to abide by the "Boston Children's Hospital, The information Services Policy and Procedure Manual: Acceptable Use of Computer and Network Resources, Remote Access Policy" subsection ("**Remote Access Policy**"), available within the CARRA Data Warehouse policies section of the CARRA Policies webpage (https://carragroup.org/members/policies-and-templates).

c) For purposes of these Terms, You understand that (i) Research Data itself does not comprise BCH's data, including BCH Protected Health Information; and (ii) rights to the Research Data collected, stored, and transmitted from the CARRA Data Warehouse are subject to the "CARRA Data/Sample Sharing Policy" on the CARRA Policies webpage (https://carragroup.org/members/policies-and-templates) and any other requirements set forth in any applicable Related Agreements (iii) Research Data stored on and transmitted from the CARRA Data Warehouse will not affect Duke's status as the "Covered Entity" (as the phrase is defined in HIPAA) responsible for protecting disclosure of the Research Data; and (iv) each CARRA Registry site shall retain rights to use its own Research Data for internal educational, clinical, and research purposes.

d) CARRA Data Warehouse Safeguards. You agree to take appropriate safeguards to prevent use of or access to the CARRA Data Warehouse and the VPN by anyone who is not an Authorized User and has not been granted access to CARRA Data Warehouse and/or VPN access by BCH.

i. Should access or use other than by permitted Authorized Users be required by government request, requirement, order or law, You shall immediately inform BCH and Duke as set forth in Section 1.d.ii and Section 1.d.iii, respectively.
ii. BCH Reporting: You understand and agree that any other information You may obtain via access to VPN, excluding Research Data and related information, comprises BCH's information. If You obtain unauthorized information, it must be destroyed immediately and You must promptly notify BCH by contacting the BCH Compliance officer at timothy.hogan@childrens.harvard.edu; 857-218-4680.
iii. Duke Reporting: lf You obtain unauthorized access to the CARRA Data Warehouse or the Research Data, You must immediately destroy all unauthorized hard copies and electronic copies of Research Data, other data or any other unauthorized information and immediately notify Duke at DCRI-Carra_Registry@dm.duke.edu with "Unauthorized Access" included in the subject line.

2. In accessing the Research Data, You agree to the following:

a) Use of Research Data. You agree that You shall use Research Data accessed from the CARRA Data Warehouse only as allowable and set forth in the Related Agreements or other data use agreement, as applicable, subject to any subsequently amended and mutually agreed purposes.

b) Other Use or Disclosure. You agree that You will not disclose, or allow access to Research Data to anyone other than Authorized Users except as required by law. For the subset of Research Data which pertains exclusively to CARRA Registry site's own subjects ("**Subjects**"), that site retains all rights to use its own Subject's Research Data.

c) Research Data Safeguards. You agree to take appropriate safeguards to prevent use of, access to or disclosure of Research Data to anyone other than as provided by Related Agreements and CARRA Guidelines. If Research Data is accessed or used by anyone other than a permitted Authorized User or if disclosure of Research Data is required by government request, requirement, order or law, You shall immediately inform Duke and BCH as set forth in Section 1.d.ii and Section 1.d.iii, respectively.

d) Contact/Identification. Except for Subjects at Your Site for which the Site already possesses coded identifiers under the Site's IRB authorization, and for all other Users not affiliated with a Site, You shall refrain from (1) any manipulation of Research Data that enables You or others to identify subjects whose information is included in Research Data and (2) any use or attempted use of Research Data to enable contact with any individual who is a subject of Research Data or his/her relatives, employers or household members.

e) Publication. Publications by You regarding Research Data shall be governed by the terms outlined in the CARRA Guidelines, subject to any further limitations imposed by Your Site's IRB. In all publications resulting directly from use or analysis of Research Data, You must cite funding support from CARRA and provide appropriate acknowledgement under CARRA Guidelines where so specified, or if not so specified then as per the most recently released version of "Uniform Requirements for Manuscripts Submitted to Biomedical Journals" guidelines produced by the International Committee of Medical Journal Editors.

3. Other:

a) Liability. Except to the extent permitted by law, You assume all liability from and against any and all claims, losses, liabilities, costs and other expenses to the extent resulting from Your use of the CARRA Data Warehouse and Research Data.

b) Disclaimer. THE CARRA DATA WAREHOUSE AND ALL MATERIALS AND CONTENT AVAILABLE THROUGH THE SERVICE ARE PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. CARRA, BCH, AND DUKE DISCLAIM ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, RELATING TO THE CARRA DATA WAREHOUSE AND ALL MATERIALS AND CONTENT AVAILABLE THROUGH THE CARRA DATA WAREHOUSE, INCLUDING: (A) ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, QUIET ENJOYMENT, OR NON-INFRINGEMENT; AND (B) ANY WARRANTY ARISING OUT OF COURSE OF DEALING, USAGE, OR TRADE. CARRA, BCH, AND DUKE DO NOT WARRANT THAT THE CARRA DATA WAREHOUSE OR ANY PORTION OF THE CARRA DATA WAREHOUSE, OR ANY MATERIALS OR CONTENT OFFERED THROUGH THE CARRA DATA WAREHOUSE, WILL BE UNINTERRUPTED, SECURE, OR FREE OF ERRORS, VIRUSES, OR OTHER HARMFUL COMPONENTS, AND CARRA, BCH, AND DUKE DO NOT WARRANT THAT ANY OF THOSE ISSUES WILL BE CORRECTED. WITHOUT LIMITING THE FOREGOING, CARRA, BCH, AND DUKE DO NOT WARRANT THE ACCURACY OR USEFULNESS OF ANY RESEARCH DATA.

NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM THE CARRA DATA WAREHOUSE OR CARRA, BCH, OR DUKE, OR ANY MATERIALS OR CONTENT AVAILABLE THROUGH THE CARRA DATA WAREHOUSE WILL CREATE ANY WARRANTY THAT IS NOT EXPRESSLY STATED IN THESE TERMS. YOU UNDERSTAND AND AGREE THAT YOU USE ANY PORTION OF THE CARRA DATA WAREHOUSE AT YOUR OWN DISCRETION AND RISK, AND THAT CARRA, BCH, AND DUKE ARE NOT RESPONSIBLE FOR ANY DAMAGE TO YOUR PROPERTY (INCLUDING YOUR COMPUTER SYSTEM USED IN CONNECTION WITH THE CARRA DATA WAREHOUSE) OR ANY LOSS OF DATA.

THE LIMITATIONS, EXCLUSIONS AND DISCLAIMERS IN THIS SECTION APPLY TO THE FULLEST EXTENT PERMITTED BY LAW.

Acceptable Use of Computer and Network Resources

This document is referenced as, and replaces, the *Guidelines for Ethical Use of Computers and Computer Information*.

Purpose

This document describes requirements and obligations for your use of Boston Children's Hospital (Boston Children's) Computer and Network Resources (as defined below) to (i) ensure that confidential and proprietary information stored on the Computer and Network Resources is adequately secured and protected; and (ii) comply with applicable laws and regulations.

Policy

Scope

- This policy applies to:
  - ANYONE who uses Boston Children's Computer Resources and related services or accesses the information stored there (collectively, "the Users").
  - ANY hardware and software systems that store, communicate, or can access Boston Children's electronic information (collectively, the "Computer and Network Resources").

Access and Use

- Boston Children's provides Computer and Network Resources, including email and use of the Internet, for legitimate business use in the course of your assigned duties. Use of these resources and access to the information on them is a privilege granted to you at the sole discretion of Boston Children's. It is your responsibility to use these Computer Resources in a professional, ethical, and lawful manner, consistent with Boston Children's policies.
- Information stored on or transmitted over Boston Children's Computer and Network Resources (including email) is the sole and exclusive property of Boston Children's, and remains so even when stored on non-Boston Children's equipment and media (such as your personal laptop and/or mobile device). Your rights to privacy do not extend to your use of Boston Children's Computer and Network Resources, including email and the Internet or to any information stored on or transmitted over the Computer and Network Resources. Boston Children's has the right to monitor your access to and use of its Computer Resources, including the content of your computer files and email accounts, without notice to you.
- Your rights to access any data on Boston Children's Computer and Network Resources end when you terminate your employment or association with Boston Children's.

Non-compliance with the Policy

- Noncompliance with this Policy, the ***Information Security Policies and Procedures***, the ***Patient Health Information Manual,*** and the ***Human Resources Personnel Policy Manual*** may subject you to disciplinary action, up to and including: termination of employment, termination of medical staff privileges, termination of computer privileges, or other sanctions as Boston Children's deems appropriate under the circumstances. You may also be subject to substantial civil and criminal penalties under the law.

Acknowledgment of the Policy

- At any of the following times, or at Boston Children's discretion, you may be required to acknowledge having read this policy and having agreed to comply with it:
  - Acceptance of employment
  - Acceptance of a consultant or temporary position
  - Appointment or reappointment to the medical staff
  - Initial access to computer resources
  - Additional access to restricted applications

Definitions

PHI/ePHI (Protected Health Information)	Includes any individually identifiable patient health information. Identifiable refers not only to data that is explicitly linked to a particular individual, but also includes health information with data items that reasonably could be expected to allow individual identification. ePHI refers to PHI stored electronically.
PII (Personal Identifiable Information)	Personal Identifiable Information (PII) includes, but is not limited to, social security numbers, credit or debit card numbers, personal information such as financial account numbers, driver's license or state issued identification card numbers and demographic information such as home addresses.
Confidential Information	Includes PHI and PII and any Boston Children's information that is confidential under any Boston Children's policy, law, regulation or agreement, or that is restricted to authorized personnel only, such as Research, Human Resources, programming code, Contracts, Legal, and Financial data. Specific examples include, but are not limited to: • Employment information, occupational health records, medical information, • compensation data and employee personnel records. • Hospital business information, such as financial and payer information, strategic • planning, fundraising and reporting information and internal memoranda. • Research information, including data, agreements, and information describing or • relating to inventions or discoveries. • Information concerning outside companies with which Boston Children's does business, including data the Hospital is contractually

	obligated to keep confidential.
Information Security Policy and Procedure	Found in the Boston Children's eLibrary, these documents define in detail the technical measures taken by the Information Services Department (ISD) to secure computer resources and data, and the Users' responsibilities for preventing the loss, modification and/or misuse of patient and Boston Children's information.

Additional Information Security terms are defined in the ***ISD Glossary.***

Requirements and Obligations

Authorization to access the Computer and Network Resources

Proper authorization is necessary before access to Boston Children's Computer and Network Resources will be granted. A User must be authorized by his/her manager and have been issued an employee ID. See ISD eHelp>***Computer Accounts*** for instructions on requesting, modifying and terminating computer access.

Reporting terminations

If termination of employment or association with Boston Children's is voluntary, your Manager will notify Human Resources no later than your last day of work. Computer accounts are disabled no later than the next business day following your last day of work.

If termination of employment or association with Boston Children's is involuntary, your manager or Human Resources must notify the ISD Help Desk immediately to request that account access be disabled as soon as possible.

Reporting transfers

Upon transfer to a new department or change in job responsibilities, you and your manager must ensure that you have the correct levels of system access to perform your new job duties.

Recovering equipment

When a User ends employment or association with Boston Children's, all Boston Children's provided equipment must be returned. This includes laptops, smartphones, tablets and any other equipment assigned to the User by Boston Children's. Prior to reassigning the equipment, all data will be erased by ISD in an appropriate manner.

No user should try to dispose of Boston Children's provided equipment, even if he or she believes that the equipment is at its "end of life." All equipment must be returned to ISD for proper disposal. ISD will make all "end of life" determinations. Contact the ISD ***Help Desk*** for more information

Protecting the Integrity of Computer and Network Resources

You are responsible for all activities done with your computer account. Information security violations may lead to discipline or discharge as described in the Personnel Manual: ***Discipline Policy and Standards of Conduct.***

You are required to take all reasonable precautions to protect the integrity, access, confidentiality and availability of Computer and Network Resources and information including but not limited to:

- **Protect the integrity of computer accounts**. Do not share your account with anyone and do not let anyone use your account for any reason. Do not attempt to access or use other users' accounts, even if they give their permission. Improper use of another person's computer account is subject to disciplinary action up to and including termination of your employment or appointment.
- **Safeguard your password**. A personal password is required to access Boston Children's Computer and Network Resources. Keep your password confidential; *do not*, under any circumstances, disclose passwords to anyone. Refuse any request to "borrow" your password. Report any such requests to the ***ISD Help Desk*** at ext 5-4357 as well as to your supervisor or Chief. The ISD Help Desk will never ask for your password and you should never disclose it anyone claiming to be from ISD or the ISD Help Desk.
- **Secure your Workstation**. Use a locking screen saver or log out if you leave your workstation unattended.
- **Accessing confidential information.** Access confidential information (including ePHI and PII) stored on Boston Children's computer and network resources only if such access is necessary to perform your job and is authorized by your supervisor or Chief. You and your manager are responsible for ensuring that you have the proper level of access. If you feel you have been given excessive access to information not necessary for doing your job, contact the Help Desk to have the access removed.
- **Distributing Confidential Information.** When disclosing confidential information (including ePHI and PII) within or outside of Boston Children's, do so only to recipients who are authorized to receive it. See the ***Use and Disclosure of Patient Health Information Policy*** for instructions on releasing PHI, and the ***Media Relations Policies*** for instructions on dealing with media.
- **Document Retention.** Boston Children's has established standards for retaining and destroying documents created by administrative and operating units. These standards cover in detail the retention, organization, and destruction of documents and are published in the Compliance Manual: ***Document Retention and Destruction*** section. You must follow these standards at all times. Consult with the Office of General Counsel if you have questions concerning whether any form of document should be maintained or destroyed, whether special circumstances require retaining it beyond indicated time frames, or any other question or concern you may have.
- **Using the system for personal reasons.** Except for incidental email and Internet use noted below, access Boston Children's Computer and Network Resources only to conduct hospital business.
- **Modifying or breaching the system.** Modifying system facilities, utilities, security settings and/or configurations, or changing restrictions associated with your accounts is prohibited unless authorized by Boston Children's.
- **Modifying, repairing, and relocating computer resources.** Repair, alter, modify, or move any Hospital-owned computer hardware or software only as authorized by ISD. Boston Children's must authorize the removal of any computer equipment for use at home or other non-Boston Children's locations. Contact the ***ISD Help Desk*** at ext 5-4357 if you need to maintain, modify, or move any Hospital-owned hardware.
- **Maintaining Security Software.** All Boston Children's PCs and laptops are equipped with security software including software that protects against viruses,

spyware, and other forms of malicious software. Laptops and other mobile devices are also equipped with encryption software. Disabling or in any way interfering with the proper execution of installed security software is prohibited. If you suspect your computer is infected with a virus, spyware, or other malicious software report it immediately to the ***ISD Help Desk.***

Acceptable Use of Technology Resources

Email, Internet, and Electronic Communication Use

Access to Boston Children's email system, the Internet, and other electronic communication tools such as Instant Messaging, is provided to help you perform your hospital duties. Though meant to be used strictly for business purposes, some incidental personal use is expected and it is allowed when:

- it does not consume more than a trivial amount of resources,
- does not interfere with productivity,
- does not interfere with any business activity, and
- is not otherwise prohibited by this policy.

Email and Electronic Communication Use

All email created or received on Boston Children's email system is Boston Children's property. Boston Children's has the right to access, review, copy, and/or delete all such messages at any time and for any purpose, without notice to you. Boston Children's also has the right to disclose them to third parties. This applies to personal and business emails.

Do not use email in any manner that violates legal requirements, ethical standards, or Boston Children's policies. This includes transmitting defamatory, obscene, pornographic, offensive, insulting, discriminatory or harassing material or messages.

Use distribution lists carefully as they may contain addresses for people who should not receive the email you are sending. Be careful when replying to emails that were sent to a distribution list.

Sending junk mail, spam, chain letters, and solicitations is prohibited. All email communications must comply with the Solicitation, Distribution and Posting policy.

Some of the messages sent, received or stored on Boston Children's electronic media constitute confidential, privileged communications between Boston Children's and either its in-house or outside attorneys. Upon receipt of a message either from or to counsel, do not forward it or its contents to others without authorization from the Office of General Counsel.

Keep inclusion of confidential information (including ePHI and PII) and other proprietary information in email and Instant Messaging to a minimum when sending on Boston Children's internal systems. If it is necessary to include such information on emails sent out of Boston Children's internal email system, it must be done in a secure manner. This is easily done by including **#secure#** in the subject line of the email. See Information Security Policy and Procedures*:* ***Email Policy*** for specific instructions on using secure email and more guidelines on acceptable Email use.

Internet Use

Internet use must conform to all applicable laws including, but not limited to, those that protect copyrights and intellectual property, and Boston Children's policy. Boston Children's has the ability and the right to access and review your Internet use and may do so for any

purpose it deems appropriate. Boston Children's may disclose this information to any party (inside or outside Boston Children's) it deems appropriate.

- Viewing, "surfing" and/or bookmarking any Internet sites that are not appropriate to Boston Children's environment is prohibited. These include offensive, discriminatory, obscene, pornographic, hate, gambling, and hacker sites.
- Downloading non-business-related files from the Internet is prohibited. These include MP3 or other music files, screensavers, movies and video, and other digital images or files, even if the copying and use of such files is legal. These files often contain spyware and other malicious code that could compromise the integrity of Boston Children's computing environment.

Social Media Use

Boston Children's recognizes that the use of online social media sites (Facebook, e.g.) has become an integral part of the personal and work lives of many of our staff. When used responsibly, thoughtfully and professionally, social media platforms are beneficial tools that further the hospital's mission, allow us to engage our patients and their families, and share the hospital's work with a wider audience.

However, use of social media also poses unique challenges and risks that we all need to be aware of. Among them are maintaining the privacy of patients' personal health information, ensuring that social networking activities do not interfere with patient care and work responsibilities, and respecting professional boundary issues between Children's staff and patients.

When using on-line social networking for work-related purposes, you must:

- Respect professional boundaries with patients, families and staff.
- Avoid accepting invitations to "friend" patients and families, especially on sites that are not hosted by Children's.
- Be careful not to disclose Protected Health Information. The ***rules of HIPAA*** apply online exactly as they do in personal interactions. Even seemingly anonymous posts may be considered PHI if they contain as little information as the data a patient was seen at the hospital.
- Be careful not to disclose confidential or sensitive information about patients, families, colleagues or hospital operations.
- Ensure that your social networking activities do not distract from patient care or work responsibilities.
- Follow all Children's policies, including the ***Acceptable Use of Computer and Network Resources policy***, ***Confidentiality of Patient Information***, as well as personnel policies addressing inappropriate conduct, including ***Sexual Harassment and Discrimination***.
- Obtain approval from ***Public Affairs***, your department's leadership and anyone else whose approval is required before setting up a social networking site that will be used for hospital purposes.

You must also ensure that the time spent on-line does not distract from patient care or other work obligations; and otherwise comply with all policies, laws and regulations related to computer use, on-line communications and Boston Children's operations.

All users who access social network sites are required to strictly follow the guidelines set forth in the ***Online Social Networking Policy***. There is also a list of ***Frequently Asked Questions*** that addresses some of the questions and concerns about this Policy.

Use of Mobile Computing Devices

Mobile computing devices are portable devices capable of retrieving and storing data, text messages and email including, but not limited to,

- iPads and other tablets
- Smart phones (iPhone, Android, e.g.)

Boston Children's or personally owned mobile devices that access the Boston Children's Exchange system for email, calendar or contacts are required to create a secure PIN or password and lock the device after 15 minutes of inactivity, requiring the PIN or password to be re-entered. Where technically possible the device must also be encrypted.

Although recommended, accessing email only through Online Web Access (OWA) does not require the above protections.

A personally owned mobile device that is used to access confidential information, including accessing Boston Children's email or receiving text pages, must also be protected.

Should a device that also functions as a telephone (iPhone, Blackberry, e.g.) be lost or stolen you **must not have the phone service turned off** until ISD has completed a wipe of the data.

Should a personally owned mobile device be re-purposed (by giving to a family member or turning in to Verizon, e.g., for an upgrade) all Boston Children's data must be removed first.

Please see the ***Mobile Device and Laptop Security*** policy for detailed instructions on protecting Boston Children's and personally owned mobile devices.

Laptops

Unencrypted laptops cannot be used to store hospital information and cannot be directly connected to the hospital network. ISD installs encryption software on all Boston Children's provided laptops. Non-Boston Children's laptops allowed to access Boston Children's network and computer systems must have adequate, up–to-date encryption software. If necessary, Boston Children's will provide such software.

Staff using laptops will be required to install a hospital-provided Network Access Control software agent that will check to see if the laptop is encrypted and running antivirus software. This software will report the information back so it can be centrally tracked. Laptops without his agent or that do not meet the encryption and security standards will be technically denied access to the Boston Children's network

Please see the ***Mobile Device and Laptop Security*** policy for detailed instructions on protecting Boston Children's and personally owned mobile devices.

Portable Data Storage Devices

Storing EPHI, PII, and confidential information on an unencrypted personally owned portable data storage device including, but not limited to, USB's (also known as a flash drive or memory stick), portable hard drives and iPods and iTouch devices is prohibited.

If business needs require storing EPHI, PII, and confidential information on a USB device a Boston Children's managed encrypted Ironkey USB device must be purchased. For details about encrypted USBs and ordering instructions see:
http://web2.tch.harvard.edu/ehelp/mainpageS2853P92.html

It is better to err on the side of caution when saving presentations containing charts or graphs that might contain embedded confidential information that could be compromised if the device is lost or stolen.

Remote Access

Users given remote access to Boston Children's Computer and Network Resources are granted privileges, permissions, or access rights no greater than those given for access at work.

Observe the following when remotely accessing Boston Children's Computer and Network Resources:

- Attend active remote sessions at all times.
- To reduce the possibility of security breaches always enter passwords manually; do not allow any program to remember your password.
- Do not store passwords on your computer (e.g. in a Word file).
- Storage of Confidential Information (including ePHI and PII) on non-Boston Children's workstations (including home computers and unencrypted personal laptops) is prohibited. Personal network drives are provided for storing Confidential Information. See the Information Security Policy and Procedure: ***Safeguarding Electronic Data*** for additional information

In addition, Users working on non-Boston Children's equipment must:

- Secure, install, and maintain, at their own expense, licensed security software (software that protects against viruses, spyware, and other forms of malicious software) on that equipment.
- Keep their equipment up to date on its Operating System (Windows XP, etc.) and software (Microsoft Word, Internet Explorer, e.g.) security patches

Except when using Online Web Access (OWA) to read email, accessing Boston Children's systems from public access equipment such as hotel kiosks or trade show computers is prohibited.

Disposal of Printed Information

Dispose of all printouts of Confidential Information (including ePHI and PII) in designated, locked bins. Do not place such information in regular waste baskets as this may allow unauthorized personnel to view it.

Limit printing of Confidential Information (including ePHI and PII) at home or at remote locations to the minimum necessary required to complete the immediate task. Printouts containing such information or other proprietary information must:

- Not be left in areas where it may be visible to unauthorized personnel.
- Be kept in secure and locked file cabinets when stored at remote locations or at home.
- Be disposed of properly via shredding or otherwise placing in locked, facility-based confidential trash bins. If these are unavailable, printed materials must be brought back to Boston Children's for proper disposal.

Copying/Use of Authorized Licensed Software

Install and use only properly licensed software on Boston Children's computers located on and off Boston Children's premises. You must comply with software vendors' license agreements for software purchased and/or licensed for Boston Children's business use. Do not use licensed software in a manner that would breach Boston Children's contractual obligations. Unless a

license agreement states otherwise, duplication of software is illegal. Without prior written authorization from the Chief Information Officer or his/her designee, you may not:

- Copy software licensed to Boston Children's for use on your home computers
- Provide copies of software licensed to Boston Children's to any third party, including independent contractors or consultants
- Modify, revise, reverse engineer, or update any licensed vendor software.

Direct questions about licensed software or authorizations required hereunder to ISD (***Help Desk***) and/or your supervisor or Chief.

Authorization for Non-Standard Software

Computers provided by ISD are specifically configured for optimal performance and security and to meet regulatory requirements. Any deviation from these configurations without the approval of ISD is prohibited. You may seek ISD Authorization for non-standard software you wish to install by submitting a Security Policy Exception Form. The form and instructions for submission can be found on the ***eHelp*** page of Children's Today.

There are many types of software that can compromise the security of our Computer and Network resources, such as peer-to-peer file sharing software, software that stores documents at third party websites, and even software from trusted companies such as Google and Yahoo. ISD conforms to industry standards and best practices when determining the risks imposed by running such software. For a comprehensive list of Unauthorized Software please visit the ***Unauthorized Software*** section of ***eHelp***.

Please observe the following guidelines regarding the use of such software:

- Use is prohibited on Boston Children's managed computers unless an exception (I.e., specific authorization to you] has been granted by ISD.
- If installed on computers that are not managed by ISD (Research computers, e.g.) the software must, at a minimum, not be used while connected to Boston Children's. In cases where software is identified as "high risk," ISD will ask that you remove it prior to connecting to Boston Children's network.
- If installed on home computers that are used to access Boston Children's Computer and Network resources they must not be used while connected to Boston Children's. It is recommended that you run only the programs necessary to do your work when connecting to Boston Children's from home.

ISD maintains and monitors software that detects the use of non-standard software and may, at its discretion or at the request of the Legal or Human Resources departments, ask users to remove any software that does not have a direct business purpose, or that adversely impacts the security of our Computer and Network resources or the data stored there.

Prohibited Use of Technology Resources

In addition to your responsibility to use Boston Children's Computer and Network Resources in a professional, ethical, and lawful manner, some activities are specifically prohibited. These include, but are not limited to:

- Engaging in non-Boston Children's related commercial activities
- Using computer resources, including printers, software, and information, for private gain. For example, you may not generate banners, invitations, pictures, graphics, etc. for personal use.
- Disseminating or displaying sexually explicit, offensive, derogatory, discriminatory, harassing, stalking or otherwise inappropriate content via email, Instant message (IM), telephone, pager, or any form of electronic media.

- Using photographs or likenesses of Boston Children's employees, patients, logos, or hospital premises without explicit and appropriate consent.
- Using Boston Children's training material and other proprietary information in anything other than its intended manner.
- Engaging in any activity that is illegal under local, state, federal or international law.
- Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property laws or regulations.
- Unauthorized use/distribution of copyrighted material including, but not limited to, digital media (music, movies, photographs, e.g.), Internet content, or other copyrighted sources.

Monitoring of Use

As noted above, Boston Children's has the right to monitor your access to and use of its Computer and Network Resources and the content of your computer files, including email, without notice to you. Boston Children's may exercise this right to safeguard the integrity of Boston Children's Computer and Network Resources, preserve the confidentiality of information stored on the Computer and Network Resources, and ensure compliance with Boston Children's policies and/or regulatory requirements, such as HIPAA, and other business or legal reasons. Boston Children's may from time to time request and require that you agree to adhere to certain additional terms and conditions as a condition of your continued use of the Computer and Network Resources.

Direct requests for additional information about Boston Children's monitoring activities, circumstances, and/or procedures may be made to the Chief Information Security Officer (CISO).

Reporting

Report any information security violations or other circumstances that may compromise the security and integrity of Boston Children's Computer and Network Resources and the information stored on or transmitted over them as soon as possible (but no later than the day the incident occurs) to ISD (by contacting the ***Help Desk***) and your supervisor or chief.

Boston Children's will investigate, respond to and mitigate data and equipment losses. You are obligated to cooperate with these efforts and to provide timely responses to requests by the team performing the investigation, response and mitigation.

Related Content

Policy and Procedure

All Security and Privacy Policies including but not limited to:

- ***Compliance Manual***
- ***Information Security Manual***
- ***Patient Health Information Manual***
- ***Human Resources Manual***

Document Attributes

Title	Acceptable Use of Computer and Network Resources		
Author	David St. Clair IT Audit and Compliance Manager	**Date of Origin**	01/18/2000 (Guidelines for Ethical Use…)
Reviewed/ Revised by	David St. Clair, Ellen Rothstein (Legal), Mary Beckman, Compliance Director Last revision by Paul Scheib, CISO	**Dates Reviewed/ Revised**	08/04/09, 6/19/2012, 10/22/2012, 11/06/2012, 7/17/2014 1/20/2015, 7/25/2017
Copyright	© Boston Children's Hospital, 2018	**Last Modified**	7/25/2017
Approved	**Signature on file** Paul Scheib Chief Information Security Officer, Director of Information Services Operations **Signature on file** Daniel Nigrin, MD, MS Chief Information Officer Senior VP for Information Services		

Revision Notes

Document actions taken when reviewed or revised.

Date	Review/Revision Action	Reviewer
06/18/09	Revised to reflect current practice; renamed from *Guidelines for Ethical Use of Computers and Computer Information* to *Acceptable Use of Computer and Network Resources*.	David St. Clair
08/04/09	Final formatting and links	Shelley Norton
3/2/10	Added new section: Authorization for Non-Standard Software.	David St. Clair
7/25/17	Reviewed for general accuracy	Paul Scheib

Policy Replacement

This policy replaces the following document: *Guidelines for Ethical Use of Computers and Computer Information* (Archived 08/09).

Safeguarding Data

Purpose

This policy addresses the importance and defines best practices pertaining to the safeguarding of personal digital data. Personal digital data is Children's Hospital related information created or modified by individual hospital employees and/or associated personnel (e.g. documents, images etc.). Every year a subset of hospital employees lose critical and sometimes irreplaceable computer files because they fail to properly backup or store those files.

Children's Hospital has substantial safeguards in place to protect employee data. The hospital data center includes fault tolerant server computers housed in an environmentally controlled space and can operate without external power with the aid of stand by batteries and a self contained generator. Every day all digital information stored on datacenter computers is duplicated and stored at a remote site. Extraordinary measures are in place to protect employee data but those measures are only relevant if the hospital community, when working with digital information, employs best practices.

Definitions

The following key terms are used in this document: ***Confidential Information*** (confidential information includes but is not limited to: Employment, Hospital business, Patient, Research, and Third Party information) ***Electronic Protected Health Information (ePHI)***; ***Computer Equipment***; ***Confidentiality***; ***Personal Digital Data***.

Key term definitions are located in the Glossary section of this manual.

Policy

All important and confidential data shall be stored on private or shared network drives. Patient data can be stored on network-shared drives if it is known who else has access to that specific share location and if those who have access have a need to see the patient data. Copies of data can be stored on mobile devices if the device complies with the ***PDA and Laptop Security***.

To ensure the integrity of ePHI, mechanisms should be put in place to prevent the unauthorized changing of data. Servers and workstations should use error correcting memory. Network protocols that are used to transmit data should use checksums to detect errors. Applications that modify ePHI should store checksums of the data and also log any changes that are made to the data and by whom.

All data that is transmitted over a computer network that is not controlled by the Hospital must be encrypted according to the Acceptable Encryption Policy.

Procedure

Private Network Drive (P: drive)

- All hospital employees with a computer account are provided with a private (P:) drive.
- The P: drive is a place to store information not meant to be shared with other hospital employees.
- Employees can access their P: drive by logging into any hospital maintained PC. Click on **My Computer** icon for list of available mapped drives
- The private drive is also available off site if the employee has remote access.
- Employees can store up to 150 MB of data on their P: drive.
- Additional storage can be acquired by completing out a Quota Increase Request Form that can be obtained from the Help Desk.
- The safekeeping of data on the P: drive is a costly service so only hospital related information should be stored there.
- Please refer to the ***Guidelines for Ethical Use of Computers and Computer Information*** for requirements and obligations regarding the use of Children's Hospital's computer resources ("Computer Equipment") and the information stored on and accessible through those Computer Resources.

Shared Network Drive (S: or J: drive)

- All hospital employees with a computer account are provided with a shared (S:) or (J:) drive.
- The S: or J: drive is a place to store information intended to be shared with designated hospital employees and/or departments.
- Employees should never store patient data on the shared drive unless they know exactly who else has access to that specific share location. Never store patient data should in the root of the shared drive or a public folder such as PMCommon, DMCommon, or PSCommon. Employees must have clear knowledge of who can access the files stored within a shared drive. Any questions regarding folder or file access should be directed to the Help Desk.
- Employees can access their S: or J: drive by logging into any hospital maintained PC.
- New shared folders can be created at the request of an employee. Requests for new shared folders should be directed to the Help Desk and include a list of employees permitted to access the folder, as well as, the content to be stored there.
- The shared drive is also available off site if the employee has remote access.
- The safekeeping of data on the S: or J: drive is a costly service so only hospital related information should be stored there.

- Refer to the ***Guidelines for Ethical Use of Computers and Computer Information*** for requirements and obligations regarding the use of Children's Hospital's computer resources ("Computer Equipment") and the information stored on and accessible through those Computer Resources.

Peripheral Storage Device (special circumstances)

- The Help Desk can assist employees to copy data to recordable CDROM media.
- Personal computers or laptops with a peripheral storage device such as a CDROM or ZIP can backup data to these devices. External media with electronic hospital and/or patient information is considered **electronic protected health information (ePHI)** and must be safeguarded accordingly.
- Refer to ***Portable Electronic Media Safeguards and Disposal*** policy for procedure surrounding the proper management of tape and optical media.

Related Content

Additional Resources

- ***Guidelines for Ethical Use of Computers and Computer Information***
- Personnel Policy ***3.08 Confidentiality of Patient, Personnel, and Hospital Information***

  PDA and Laptop Security
- ***Disposition of Used Computer Equipment***

Associated Regulations

Associated Regulation #	Regulation Name
45 CFR Parts 160, 162, and 164	Health Insurance Reform: Security Standards (HIPAA Security Rule)

Document Attributes

Title	Safeguarding Data		
Author	**Jim Shattuck,** Shari Bedar, Beth Bitner, Ryan Callahan, Yvonne Danjuma, Cheryl Gikas, Scott Lenzi, Kevin Murray, Paul Scheib, Gary Smith, Richard Souza		
Copyright	©Children's Hospital Boston, 2004	**Revised**	1/23/04

Approved	**Signature on file** Paul Scheib Chief Information Security Officer, Director of Information Services Operations **Signature on file** Daniel Nigrin, M.D., M.S. Chief Information Officer Senior VP for Information Services

Revision Notes

Document actions taken when reviewed or revised.

Date	Review/Revision Action	Reviewer
1/2004	New policy to comply with HIPAA Security Rule and Privacy Rule requirements for safeguarding protected health information	