Administrative Policy

NATIONWIDE CHILDREN'S
When your child needs a hospital, everything matters.℠

Number: XIV-6	Page 1 of 7	Originated: 9/2013 Reviewed: 6/2020 Revised: 8/2020

Contents

Purpose

This agreement applies to all users granted access to information technology resources ("IT Resources") at Nationwide Children's Hospital, Inc. and its affiliate organizations (collectively referred to as "NCH") including, but not limited to, employees, faculty, students, contractors, research collaborators, and volunteers. All users of NCH information technology resources are responsible for adhering to this agreement and all information security and privacy laws, policies, and other applicable contracts. Examples of such laws, policies, contracts include the Health Insurance Portability and Accountability Act (HIPAA); laws governing libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act; the Computer Fraud and Abuse Act; Securities and Exchange Commission laws and regulations regarding Insider Trading, and all applicable software licenses.

Definition

Confidential information: Confidential Information includes all business records, data, and information maintained by NCH and made accessible to NCH Personnel through employment or

affiliation with NCH which is not already freely available to the public. Confidential Information does not have to be marked as "confidential" to be considered Confidential Information. Examples of Confidential Information includes, but are not limited to, patient information, financial information, business plans, employee information, product information, and research data and results. Also, any information disclosed by a company to NCH Personnel to facilitate a business discussion or relationship is considered Confidential Information unless such information has already been made available to the public by the company.

General

1. I understand and agree that I do not have any right to privacy over any information I access or communications I make while using NCH IT Resources. This includes personal email accounts, social networking sites, chat services, text messages, mobile devices, phones, voicemail accounts, blogs, video streams, file sharing services, websites, or future technologies.
2. When I use, access, transmit, and store Confidential Information of NCH or a third party, I agree to follow HIPAA, all federal and state laws and regulations, and NCH policies relating to privacy of medical records.
3. I understand and agree that I am prohibited from using NCH IT Resources to access or view materials that are obscene, sexual or pornographic in nature, objectionable in nature; create a hostile work environment; or subjects NCH to any reputational risk of harm.
4. I understand that the use of NCH IT Resources is provided for NCH business purposes. I agree that my personal use of NCH IT Resources must be minimal and may not interfere with my job responsibilities and must not interfere with other NCH employee access to NCH IT Resources (e.g., streaming online audio or video with no business justification, which unnecessarily impacts system resource availability).
5. I agree that I will not tamper with, disable, or bypass any security controls in place on IT Resources, including but not limited to security software and login account controls.
6. I understand that NCH patients have rights under HIPAA, and I am responsible for ensuring compliance with HIPAA and assisting patients with the exercise of their HIPAA rights.

Access

1. I understand and agree that in performing my job duties, I will maintain Confidential Information in strict confidence whether such information belongs to NCH or a third party.
2. I understand that I may not access, view, or share patient information or other Confidential Information for any reason other than as required to perform my job responsibilities. This means that I may not access information of patients, relatives (including my own children), friends, neighbors, co-workers, celebrities, and crime

victims without a specific need to do so for my job. If I access, view, or share sensitive information outside of my job responsibilities, it will be a breach of confidentiality, a breach of this Agreement, applicable laws and policies, and may result in corrective action, termination, or legal sanctions.

3. I understand that if I need information for a personal reason, such as a copy of my own or my child's medical record, I will not access this information directly from NCH systems made accessible for work purposes (e.g., Epic). I agree that I will use the appropriate methods to obtain such information for personal reasons (e.g., MyChart, Health Information Management Department).
4. I understand my online identity (e.g., usernames, passwords) is an electronic signature which will be attached to each transaction I enter into an NCH system and my use will be subject to auditing. I will not allow anyone else to access any NCH IT Resources or NCH system using my identity.
5. I will not disclose my password to anyone, including management, administrative assistants, and Information Services. In addition, I will only use my own authenticators (e.g., passwords, RSA token, fingerprint) and will not access any NCH IT Resources or systems which I am not authorized to access even if I have the capability to access the system. I understand NCH IS will never ask me for my password.
6. I will exit, log off, or otherwise lock systems when left unattended (e.g., tap out, Windows + L).
7. I understand my accounts will be disabled as soon as my employment with NCH ends or when I transfer to a different NCH position where access is no longer needed for my job. I agree to alert NCH Information Services at the contact information below if my accounts have not been properly disabled.

Disclosure

1. I will not share, transfer, or disclose Confidential Information unless authorized or required by my job duties, and then only in accordance with NCH policies (e.g., obtaining appropriate authorization and consent) and applicable laws.
2. I will use caution to avoid being overheard when discussing Confidential Information of any nature. This includes being mindful of discussions occurring in "on stage" versus "off stage" areas and when not on NCH property.
3. I will use caution in disclosing Confidential Information and will verify key information prior to disclosures, for example, by double checking phone numbers, fax numbers, email recipients, and patient names on paperwork before routing, distributing, or transmitting information so that the correct information is given to the correct people.
4. I will verify a person's identity prior to releasing any information by phone by asking for the Outpatient Care code or other identifying information that would reasonably confirm

that person's identity. I will only leave general information on a patient/family's voice mail, never diagnoses or other detailed information.

5. I will make sure unsecured Confidential Information is not left unattended where unauthorized people may view it. If I become aware that Confidential Information has been left unsecured, I will immediately retrieve it if possible and report the incident through the appropriate channel (e.g., your manager, CS Stars, other contact information below).

Social Media

1. I understand when using social media for personal use or as part of my job for NCH, I must not disclose Confidential Information.
2. I will use caution with social media sites, taking care to never disclose or post Confidential Information or photographs (e.g., patients, other employees, documents, etc.) in any form even if it is believed to be de-identified. For example, blacking out faces in photographs is still prohibited. Any use of an edited or redacted image of person must be approved by the Privacy Office.
3. I will not connect (e.g., friend, follow, link) with patients and patient families to ensure that appropriate patient-provider boundaries are maintained.
4. I will not establish any web pages, social media identities, private social media groups, blogs, or other accounts which contain Confidential Information, branding, or the Nationwide Children's Hospital or any of its affiliates' names without the advance approval of both the Information Services and Marketing departments.
5. I understand I am responsible for following the policy and all guidelines found within in Administrative Policy V-34, Use of Social Media.

Personally Owned Devices

1. I understand while conducting NCH business, I must use devices provided by NCH unless using an authorized method to access NCH IT Resources from a personally owned device. Some examples of authorized methods include securely accessing email on mobile devices, using virtual desktops access through the Employee Portal, Haiku/Canto, or approved enterprise cloud solutions.
2. I understand that I must not store or download Confidential Information on my personally owned device (e.g., laptop, phone, thumb drive).
3. I understand that any device suspected to contain NCH-owned or other Confidential Information which relates to an information security incident may be confiscated (including personally owned devices). This means my personal cellphone may be taken by NCH for a security investigation.

Services and Software

1. I understand while conducting NCH business or engaged with NCH, I must use the licensed software/services that are supported and/or provided by NCH. I may not download or accept licensing or other agreements for services or software without specific authorization from Information Services. If I require additional software to do my job, I will submit a request to Information Services at https://nationwidechildrens.service-now.com/iss.
2. I understand that only NCH-approved and licensed software may be installed on NCH computers.

Transport of Confidential Information

1. I will only transport paper-based documentation containing Confidential Information if I have a business need to do so and the Confidential Information cannot reasonably be accessed electronically or in another more secure manner.
2. I agree to maintain personal possession of all documents containing Confidential Information, and I will not leave the documents in any vehicle or otherwise unattended at any time.

Specific Requirements for Protected Health Information (PHI)

a. If I am required to transport paper-based documentation containing PHI, I will complete an Application for Transport of PHI via The Learning Center and obtain approval from my manager and the Privacy Officer prior to transporting.
b. I understand I am responsible for following all guidelines in Administrative Policy XI-29: Transport of PHI to Offsite Locations.

Electronic Messaging (e.g., email, texting, MyChart)

1. Before sending/replying/forwarding any email containing Confidential Information, I agree to type **SECURE** in the subject line.
2. I will use encryption methods authorized by the Information Security Risk Department when sending NCH Confidential Information regardless of the messaging technology.
3. I will use caution when engaging with (e.g., replying, forwarding, opening attachments) unexpected, questionable, or suspicious mail.
4. I will not send or auto-forward any Confidential Information to my personal or non-NCH email account.
5. I understand that texting/messaging applications are generally prohibited for sending PHI except as allowed by Administrative Policy V-35, Electronic Messaging for Patient Care Related Communication.
6. I understand I am strictly prohibited from using electronic messaging to place patient care orders internally or to outside healthcare providers/staff.

7. I understand that use of NCH messaging technology is prohibited for purposes such as political appeals, religious appeals, or to transmit ethnic, racial, or sexual jokes, or other content which is illegal, offensive, creates a hostile work environment, or poses a risk of harm to the reputation of NCH or its affiliates.

Disposal/Physical Security

1. I understand monitors and screens displaying Confidential Information must be positioned or protected with screen guards so the Confidential Information cannot be viewed by the public or other employees.
2. I will always discard Confidential Information in the secure Shred-It bins located throughout NCH facilities.
3. I understand papers and removable storage media containing PHI may not be left unattended in publicly accessible areas.
4. I will keep portable devices (e.g., iPod, tablets, phones, cameras, laptops, thumb drives, etc.) physically secured at all times and will not leave the devices in unattended vehicles, bags, or rooms.
5. I understand equipment which processes or stores Confidential Information (e.g., hard drives, USBs, CDs, printers, ultrasound machines, pumps, lab equipment, cameras, iPods) must have the Confidential Information wiped or destroyed according to NIST SP 800-88, "Guidelines for Media Sanitization, Revision 1," even when that equipment is supported by a vendor. I will contact Information Services for assistance in complying with this destruction requirement.

Reporting

1. I understand that it is my responsibility to promptly report to my manager/section chief, the Information Security Office, the Privacy Office, or the Corporate Compliance Office any of the following:
    - any known or suspected violations of patient confidentiality, including unauthorized access, use, or disclosure of Confidential Information;
    - any suspected fraudulent activity or misuse of NCH IT Resources
    - lost/stolen NCH devices or personal devices containing Confidential Information on the device; and
    - any suspected or actual compromise of IT Resources, computer system security settings.

Contact Information

1. If I have any questions related to the items above, I will contact one of the below:
    a. IS Service Desk
        - 614-355-3750
        - https://nationwidechildrens.service-now.com/iss

b. Information Security and Risk Department
   - ISRD@nationwidechildrens.org

c. Privacy Office
   - 614-355-0711
   - PrivacyOffice@nationwidechildrens.org

d. Corporate Compliance Office
   - 614-355-0402
   - CorporateComplianceOffice@nationwidechildrens.org
   - Anonymous Compliance Hotline: 877-267-1935

Deviations

1. Any deviation to this policy must be approved in advance and in writing by the IS Security Officer, the Privacy Officer, Legal Services, or the highest-level administrator overseeing the affected clinical or business area(s).

Relevant Policies

1. I understand and agree to abide by the following policies which further specify how I am expected to behave regarding the topics:
   a. V-26: USE OF RECORDING DEVICES
   b. V-34: USE OF SOCIAL MEDIA
   c. V-35: ELECTRONIC MESSAGING FOR PATIENT CARE RELATED COMM.
   d. XI-28: MEDIA AND EQUIPMENT DESTRUCTION GUIDANCE
   e. XII-19: INSIDER TRADING AND CONFIDENTIAL INFORMATION

Approval and Ownership:

Owned By	Title	Date	Signature
Brian Baacke	Chief Information Security Officer (CISO)	7/28/2020	Signatures on file with ISRD
Reviewed By	**Title**	**Date**	**Signature**
Denise Zabawski	Vice President & CIO	7/29/2020	Signatures on file with ISRD
Approved By	**Title**	**Date**	**Signature**
Rick Miller	President & COO	8/3/2020	Signatures on file with ISRD
Amy Roscoe	Vice President, Research Strategic Planning & Finance	8/3/2020	Signatures on file with ISRD