



## Patient Health Information Manual Boston Children's Hospital

# Provider Portal Access Policy

## Purpose

This policy governs use of the Boston Children's Hospital ("BCH") Provider Portal (the "Provider Portal") and is intended to protect the confidentiality and security of information viewed through the Portal.

## Scope

This policy applies to anyone who has access to the Provider Portal. Failure to comply with this policy can lead to sanctions including termination of Provider Portal privileges.

## Policy

### 1. Use and Disclosure of Protected Health Information

- Provider Portal access is permitted only for individuals who (1) require access to BCH patient health information in support of treatment, including, as permitted by the Privacy Rule and this Policy, payment or health care operations in connection with such treatment, for a patient common to BCH and the person (or his/her authorized designee) accessing information through the Provider Portal ("shared patient"); and (2) are Covered Entities in the meaning of HIPAA, or who are part of the workforce of a Covered Entity.
- If information is accessed through the Provider Portal for payment or health care operations purposes, only the minimum scope and amount of information needed to accomplish the purpose may be accessed. *In addition, the Provider Portal is not to be used for any activity that is not directly related to continuity of care for an individual shared patient, i.e., the Provider Portal may not be used for utilization review and/or utilization management purposes, generalized educational purposes, research, or the like, whether or not that activity is included in HIPAA definitions or guidance as a payment or healthcare operations activity.*
- Information accessed through the BCH Provider Portal remains BCH information and does not automatically become medical record information of the person or entity accessing the portal. If such information is used for decision-making in patient care, it may be incorporated into the portal user's medical record for the patient, with appropriate attribution. No information from the BCH Provider Portal that has not been so incorporated should be disclosed to any person or entity, other than the patient, parent or guardian, by any Provider Portal user. Other requests for medical record information from BCH should be directed to the Health Information Management Department at BCH at the address below:

Health Information Management Department  
Boston Children's Hospital  
300 Longwood Ave.  
Boston, MA 02115  
Fax: 617-730-0327

## 2. Acceptable Use of the Provider Portal

- ANYONE who uses BCH computer resources, including the Provider Portal, must comply with this Policy to ensure continued security of BCH computer resources and information.
- BCH provides computer and network resources, including the Provider Portal, for legitimate business use in the course of assigned duties. Use of the Provider Portal an access to information through it is a privilege and granted at the sole discretion of BCH. It is the responsibility of each user to use the Provider Portal in a professional, ethical and lawful manner, consistent with BCH policy.
- Information stored on or transmitted over BCH Computer and Network Resources is the sole and exclusive property of BCH, and remains so even when stored on non-BCH equipment and media. Any user's right to or expectation of privacy does not extend to use of BCH Computer and Network Resources. **BCH has the right to monitor access to and use of its Computer Resources, including the Provider Portal, without notice.**
- Each Provider Portal user is responsible for all activities done with his or her computer account. Information security or privacy violations may lead to termination of Provider Portal privileges.
- Users 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 Provider Portal privileges.
  - **Safeguard your password.** A personal password is required to access BCH'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.
  - **Secure your Workstation.** Use a locking screen saver or log out if you leave your workstation unattended.
  - **Accessing confidential information.** Access the confidential information available through the Provider Portal only if such access is necessary to perform your job and is authorized by your supervisor, Chief, or other authority responsible for granting such access within your organization.
  - **Distributing Confidential Information.** Do not disclose or distribute information from the Provider Portal (unless such information has been incorporated into a Provider Portal user's medical record as described above).
  - **Modifying or breaching the system.** Modifying system facilities, utilities, security settings and/or configurations, or changing restrictions associated with your account is prohibited.
  - **Maintaining Security Software.** You should access the Provider Portal only through computers equipped with security software including software that protects against viruses, spyware, and other forms of malicious software. If you suspect your computer is infected with a virus, spyware, or other malicious software report it immediately to your information security officer or, if you do not have one, to the BCH [\*\*\*ISD Help Desk \(617-355-HELP\)\*\*\*](tel:617-355-HELP).

- **Safeguard Printed Information.** Limit printed information (including PHI and PII, as defined below) to the minimum necessary required to complete your job responsibility. Printouts containing such information must:
  - Not be left in areas where it may be visible by unauthorized personnel
  - Be kept in secured and locked file cabinets
  - Be disposed of properly via shredding or otherwise placed in locked bins. Do not place such information in regular wastebaskets.
- **Guard against privacy violations while using Internet-based Social Networking.** Any “social networking” use or sharing of PHI, PII or other confidential or proprietary information obtained as a result of access to the Provider Portal is prohibited. This includes sharing or posting information (including images) or engaging in conduct that is an invasion of privacy of another, including patients, families, etc.
- **Report any information privacy or security violation or other circumstances that may compromise the security and integrity of PHI or PII involving BCH patients to the BCH Compliance Hotline (1-888-801-2805).**

## Definitions

<b>PHI/ePHI (Protected Health Information)</b>	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.
<b>PII (Personal Identifiable Information)</b>	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.

## Document Attributes

<b>Title</b>	Provider Portal Access		
<b>Author</b>	Pixie Paradiso, Associate General Counsel	<b>Date of Origin</b>	12/2010
<b>Reviewed/ Revised by</b>	Marvin Harper, MD Chief Medical Information Officer  Steve Eddington, RHIA, Director, Health Information Management  Paul Scheib, Director IT Operations Chief Information Security Officer  Richard Lynch Director, Physician Relations and Outreach  Pixie Paradiso Associate General Counsel	<b>Dates Reviewed/ Revised</b>	6/2011, 9/2019
<b>Copyright</b>	©Boston Children’s Hospital, 2011	<b>Last Modified</b>	09/10/2019
<b>Approved</b>	<b>Signature on File</b> Daniel Nigrin, MD, MS Senior Vice President for Information Services, Chief Information Officer		