PRIVACY AND CONFIDENTIALITY FOR PATIENTS

POLICY: Patient privacy is the expectation that health information will only be accessed, used, and shared as needed for care, payment, and health care operations. At Children’s, protecting patient privacy is everyone’s responsibility. This responsibility is part of Children’s commitment to family-centered care with the highest possible ethical standards. This commitment is supported by Washington State and federal laws.

Therefore, Children’s has adopted the following privacy principles:

- We honor the trust placed in us to maintain the privacy of patient health information.
- We respect and support the privacy rights of patients and their families.
- We are accountable for understanding and following our privacy policies and procedures.
- We access and use only the patient and family information that we need to know to do our jobs.
- We share patient and family information on a need-to-know basis.
- We always provide the information needed to deliver high quality care.

At Children’s, everyone is responsible for protecting patient privacy including all staff (employees, temporary staff, and consultants), physicians and community providers, residents and students, and volunteers.

PROCEDURE:

1. Protected Health Information
   A. Protecting patient privacy means safeguarding a patient’s health information, referred to as Protected Health Information (“PHI”). PHI is any health information that can identify a patient.
   B. PHI is not just in the medical record, but also, for example, on hospital bills. It can also be information provided orally.

2. Required Privacy Training
   A. New employees will become familiar with the importance of patient privacy through new employee orientation sessions.
   B. All staff should complete patient privacy training within 90 days of being hired. Staff completion of training will be monitored through the annual evaluation process.
   C. Privacy training is available through booklets and an online course. For more information, see the Privacy Program website on CHILD.
3. **Department Directors and Managers are Responsible for:**
   
   A. Providing staff with access to policies and procedures relating to privacy and confidentiality.
   
   B. Securing PHI and other confidential information from unauthorized access.
   
   C. Ensuring that all employees and contract staff within their department or program sign the appropriate [Children’s Confidentiality Agreement](http://child.chmc.org/p&p/administrative/privacy and confidentiality for patients.doc(v)).
   
   D. Escalating privacy concerns, as appropriate, to Children’s Privacy Official.

4. **Guidelines for Protecting Patient Privacy**
   
   A. Conduct conversations with or about patients as privately as possible (avoid hallway, elevator, and cafeteria conversations).
   
   B. Provide information on a need-to-know basis.
   
   C. Report privacy concerns to your supervisor or contact the Privacy Official at mail stop 4P-2, through email at [Privacy.Questions@seattlechildrens.org](mailto:Privacy.Questions@seattlechildrens.org), or through the Privacy Help Line at (206) 987-1200.
   
   D. Take precautions when traveling off site with PHI by securing and disposing of it appropriately.
   
   E. Seek out only the information you need to know to do your job.
   
   F. Know how to help patient and families with their privacy rights. Refer to the Privacy Program website on CHILD for information resources.

5. **Guidelines for Preventing Privacy Breaches**
   
   A. Don’t share your computer passwords.
   
   B. Don’t forget to log off when you finish using a computer.
   
   C. Don’t leave PHI in public areas.
   
   D. Don’t discard PHI in waste baskets. Use an appropriate recycling or secure disposal bin (for non-paper items).
   
   E. Don’t browse computer systems or scan paper records for patient information you don’t need to know.
   
   F. Don’t answer detailed questions about a patient from non-family members without approval from the patient or family.
6. Guidelines for PHI in Public Hearing

<table>
<thead>
<tr>
<th>PHI Sources - Public Hearing</th>
<th>Guidelines</th>
</tr>
</thead>
</table>
| Patient Interactions (Interviews, Telephone Calls, etc.) | • Lower your voice as appropriate.  
• Use private areas as available.  
• Curtail elevator and cafeteria conversations.  
• Include private areas in future space planning. |
| Overhead Paging | • Routine pages using child’s full name is prohibited.  
• Telecom will use first name and last initial.  
• Exception for urgent clinical or safety concern. |
| Clinical Discussion of Patient Information | • Use available private areas as far as possible. |
| Audio Taping by Staff | • Obtain permission from patient and family. |

7. Guidelines for PHI in Public View

<table>
<thead>
<tr>
<th>PHI Sources - Public View</th>
<th>Guidelines</th>
</tr>
</thead>
</table>
| Patient Room Tags | • Use first initial and last name, or when necessary, obtain permission from patient or family to use both names.  
• Include no diagnosis information. |
| Parent Message Boards (on units) | • Use room number (and bed as necessary).  
• Include no diagnosis information. |
| White Boards (including electronic) | • Use first initial and last name (or obtain permission to display both names).  
• Include no diagnosis information.  
• Re-position boards to reduce “public” access. |
| Patient Physical Privacy | • Shield patient from “public” view as practical.  
• Install curtains, cubicles, drapes, partitions, and locks as is practical and appropriate. |
| Inpatient Record Binder (Notebook, Chart Book) | • Use first initial and last name on binder tag.  
• Include no diagnosis on the outside cover. |
| Computer Terminals | • Use PC screen saver.  
• Install privacy screen on monitor.  
• Re-position monitor to reduce “public” access.  
• Log out of shared computers. |
| Videotaping & Photography by Staff | • Obtain permission from patient, family, and other staff. (Consent for Care and Treatment grants permission for diagnosis purposes.) |
| Disposing of Patient Information | • Place paper in secure recycling bins.  
• Place non-paper in secure disposal bins.  
• Do not use garbage cans for confidential information. |
8. **Related Privacy Policies**

   A. Authorization to Release or Obtain Patient Health Information.
   B. Use and Disclosure of Health Care Information.
   C. Notice of Privacy Practices.
   D. Patient Complaint or Grievance.
   E. Faxing of Patient Health Information.
   F. Recycling and Secure Disposal of Confidential Health and Business Information.
   G. Patient Rights and Responsibilities.
   H. Request to Restrict Use or Disclosure of Protected Health Information.
   I. Accounting for Disclosures of Protected Health Information.
   J. Requesting Confidential Communication.
   K. Media and Communications.
   L. Use of the Information Network.

9. **Breach of Privacy or Confidentiality**

   A breach of patient privacy may be grounds for corrective action up to, and including, termination.

10. **Guidelines for Working through Privacy Questions:**

    A. Think about Children’s privacy principles.
    B. Apply your common sense.
    C. Consider how you would want you or your family’s information to be treated.
    D. Talk to your supervisor.