Children's Hospital Requirements for Remote Access

Our Commitment

- Children's Hospital is committed to protecting the privacy of patient health information and securing access from unauthorized users.
- As part of our commitment, Children's Hospital has developed this training for all individuals with remote access to hospital information systems.

Responsibility to Protect

WHY?

Advancing technologies have resulted in greater accessibility to electronic patient health information (EPHI).

This in turn requires Children's Hospital to continually improve our systems to ensure privacy and security of patient information.

Spot Light on EPHI

- Nationally, healthcare is becoming:
  - More automated, which increases the need to share patient information in an electronic format
  - More mobile as staff begin to utilize portable devices, both within the hospital and remotely for care purposes
- As usage increases, regulatory and accrediting organizations are developing security standards for healthcare organizations.

All Remote Access Users

WHO?

- **Hospital Employees**
  - All hospital employees who have remote access. For example, employees with remote access and home-based employees.
  - All hospital employees who utilize portable devices (ie. including lap tops, smart phones, and PDAs) to access EPHI remotely.
- **Non-Hospital Employees**
  - Individuals and entities provided remote access to EPHI, including vendors, physicians, residents, business partners, and business associates.

All Users Must Be Responsible

HOW?

All users must:

- Access only EPHI to which they are entitled
- Report any known or suspected misuse of access to the IT Service Desk
- Report any lost or stolen portable media device to the IT Service Desk
- Not share passwords
- Contact the IT Department Service Desk at 353-7300 immediately if you no longer need remote access.

Offsite Portable ***Device*** Users

HOW?

- Children's laptops have system settings that protect the security of the device.
- All returned laptops will be examined for system settings tampering. Disciplinary action can be taken if the system settings have been changed.
- Do not leave portable devices in unattended vehicles or public thoroughfares.
- Do not download EPHI to portable devices.
- Prior to returning portable devices, you should search and delete files intentionally or unintentionally saved to the devices.

Remote *Access* Users

HOW?

- Do not download Children's Hospital's EPHI onto your remote system or device.
- Children's Hospital employees must use SAFE IT when transmitting EPHI through e-mail.
- Only print records containing EPHI if you are authorized to do so. Properly shred and dispose of printed EPHI per HIPAA guidelines.
- IF EPHI is displayed on your computer monitor, do not leave your computer unattended. Others should not be able to view the EPHI in your absence.

In Review

Why… to insure privacy and security of electronic patient health information.

Who… hospital employees with remote access or remote devices accessing EPHI; and non-hospital employees with remote access.

How…

- Only access authorized data
- Report misuse, loss or lack of need for remote access or devices
- Do not tamper with portable device system settings
- Appropriately transmit, download, and print EPHI.

If you have any questions:

E-mail to Kevin Shimamoto, Chief Information Officer