Data Security

Is the Children's Community Health Record (CHR) HIPAA compliant?

All individually identifiable health information related to the care and treatment of any patient is protected under the regulations established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy Rule) and should only be used by medical personnel involved in a patient's care. The CHR electronic health record system (EHR) is encrypted and accessible only to authorized individuals through a secure login name and password. Any use of patient records by any persons for any reason other than those directly related to a patient's treatment is a potential violation of HIPAA privacy regulations and is prosecutable as per these established legal guidelines.

Can other physicians see my patient's information?

Yes, any physician with authorized access to the patient's clinical data can see patient information. When a patient encounter takes place, chart updates are automatically entered into the EHR, viewable by authorized users. An exception to this rule is those health records for which additional security restrictions have been applied (e.g. HIV; psychiatric care). In these cases additional authorization is required.

Can other physicians see my practice schedule?

No. Scheduling and financial information for each community practice is completely partitioned by practice, restricting practice management information, (e.g. schedules, claims and billing information), to a particular practice. Only clinically-relevant patient information is available in the shared clinical database between authorized users.

Where is my patient data stored?

Children's maintains a dedicated system of redundant servers in its Data Center. Children's information technology staff is responsible for system updates, data integrity and daily redundant remote data backup.

If Children's cannot see the financials (physician office billing/scheduling/registration) how can an effective backup be done?

Backups include all clinical and financial data and are run as an independent system function without human intervention. While Children's technical team provides support such as updates, backups, etc., these support functions do not require accessing physician practice information.

Can anyone access patient records in an electronic health record environment?

Access to data on Epic is limited to authorized users who verify their identity through use of a unique username and password. The security level of each authorized user is defined by job title based on the information access level required for that role. There are additional security restrictions available on a case-by-case basis for specific patient records within the system (e.g. HIV; psychiatric care). Epic has audit trails with a reporting system that allows Children's to maintain patient record security and monitor authorized access required for patient care. Patient privacy and limiting access strictly to appropriate staff necessary for the care process is a top priority for us.

Will my staff get access?

Yes. All staff will use a unique username and password with levels of access appropriate to their role and scope of practice.

Is a physician forced to see information that doesn't pertain to him, such as history of all other physicians who have treated this patient?
The benefit of an integrated record is information accessibility to all providers across the continuum of care. Epic's organization allows users to filter information appropriate to each provider (e.g. by specialty, care setting, etc.) when reviewing the record. The record is segmented much like a file cabinet with file folders. The folders are available for review as needed and if the provider security allows. In addition, in the interest of patient safety and provider-to-provider communication, providers share a common database for patient information such as history, medication list, and problem list. While the data itself is shared and available to users with appropriate security, the view and entry of such data can be configured in a provider-friendly manner.

How do I get outside records into the electronic chart?
Outside results, referral letters and limited progress notes that are not in a digital format may be scanned into the CHR system and displayed as an image for future reference. Data from scanned documents may not be utilized for reporting or trending historical information.

What will happen to my existing data on my current system? Will all current records be scanned and transferred to the integrated electronic health record?
The management of current patient data will be a decision for each individual practice. One recommendation is "just in time" abstracting of data. When a patient is scheduled, pertinent data is entered into the system the day before the visit. Demographic data, allergies, problem list, current medications, surgical history, and immunizations are the basic data set that providers generally request.

Can the records be changed once they are in system?
Yes, but updates or changes to patient records are tracked via clinician sign in, date, and time of change. The original information can be labeled as 'entered in error'. In Epic, physicians can add or edit notes whenever needed, as all entries are date and time stamped.

How long is data kept by the CHR?
Epic has the capacity to maintain and store integrated health records indefinitely. It is up to the practice to determine the period of time it maintains patient records.

How will the system handle inaccurate data entry?
There will be guided decisions and documentation within the system, but these will not eliminate all data entry errors. Errors in data entry will be noted in the system and correct data will be added as appropriate.

Offices often have policies on how long to keep records prior to transfer to EHR. Do you return to records to the patient or shred them?
Specific policies on the length of time to maintain a patient record are dictated by the requirements of each clinician's individual professional liability insurance policy and the Georgia Statutes of Limitations for various claims. Practices will need to consult an attorney to establish the appropriate record retention policy for their practice. The U.S. Department of Health and Human Services and the Office for Civil Rights created a FAQ document on the proper disposal of protected health information. The document can be downloaded from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf

Children's will maintain reasonable safeguards against destruction, loss or alteration of patient protected health information (PHI) and will maintain virus protection software as well as disaster recovery and a business continuity plan.

Epic is considered a Priority-I application within Children's Disaster Recovery Plan. Should a catastrophic event occur that would cause the Epic operating environment or a significant portion of it to be unavailable or inoperable, Children's will implement Disaster Recovery Operations (DR), which will recreate an operable EHR system environment for community practices.

Practices are responsible for planning and implementation of their individual business continuity plan and DR plan that covers their current internal technical infrastructure. Children's will work with practices to develop these strategies and processes within the scope of the CHR implementation.

What levels/types of security will be in place?

There are comprehensive policies and procedures in place to maintain system security and to monitor access to confidential patient information. There is an electronic chart audit process that checks for inappropriate chart access and generates reports for each medical practice. Incorporated within the EHR system is the ability to "lock down" sensitive or personal information viewable by a single provider entry. Children's sponsors a Physician Advisory Committee that oversees and regularly reviews all the aforementioned policies and procedures as they relate to data security and chart access.

What are my practices responsibilities around privacy and security of data?

Practices will be required to develop and implement written security policies and procedures as required under the HIPAA Security Rule with respect to electronic protected health information (PHI) they handle. In addition, practices will enter into a HIPAA Privacy and Security Compliance Agreement which explains responsibilities for providing training to their staff around security and privacy, reporting breaches of confidential information, and indemnifying Children's for claims or damages resulting from the practice's breach of patient PHI.