Your Role in Protecting Patient Privacy 2018
This training will focus on what responsibilities you have in order to ensure that both you and our organization are in compliance with state and federal privacy regulations. The following topics will be covered:

**HIPAA PRIVACY**

- Protected Health Information
- Minimum Necessary
- Patient Rights
- Notice of Privacy Practices
- Appropriate Access to Patient Information
- Reporting Privacy Concerns / Potential Breach Reporting
We Are Committed to Privacy & Security Compliance

- Our goals with this training module are to
  - Assist you with meeting compliance obligations;
  - Help you understand key elements of privacy and security compliance to protect patient privacy and honor our promise to patients, families and regulators to keep medical records and patient information confidential.

- Upon completing this module you will understand:
  - How to help protect the privacy of patient information;
  - Common risks to privacy and security;
  - How to describe safeguards used to protect patient information and information assets;
  - Your compliance obligation to prevent privacy breaches and report suspected breaches when they occur.
The Privacy Rule

Protects information known as PROTECTED HEALTH INFORMATION (PHI) that exists in written, oral, and electronic formats.
Examples of Protected Health Information (PHI)

- Individually identifiable health information (name, address, date of birth, age, phone number, account number, drivers license number, social security number, etc.);

- Medical records, diagnosis, x-rays, photos, prescriptions, lab work and test results;

- Billing records, claim data and EOB-Explanation of Benefits;

- Electronic records, paper records and oral communications.
When Can PHI Be Disclosed Without Patient/ Parent Authorization

Examples includes disclosures for:

• **Treatment** of the patient, including appointment reminders;

• **Payment** (in order to get paid for the treatment we provide);

• **Health Care Operations** (Auditing and Monitoring, Compliance Review, Medical Staff peer review activities, teaching, quality improvement initiatives.

As well as:

• Mandatory infectious disease reporting;

• Mandatory child abuse reporting;

• Mandated discharge reporting to the state;

• To HHS in compliance with the Privacy Rule.
The Privacy Rule

• Limits the way in which workforce members may access, use and disclose patient information.

• You must have a work related reason to access, use and disclose patient information.

• Requires that all workforce members use only the minimum amount of patient information necessary to do their job. This is what HIPAA defines as the “Minimum Necessary Standard”.

Patient Rights Under The Privacy Rule

- The Privacy Rule provides patients with certain rights, commonly referred to as Patient Privacy Rights.

- These rights are communicated to our patients in the Joint Notice of Privacy Practices.
Summary of Patient Rights Under The Privacy Rule

• Right to request a copy of their medical information;
• Right to request an amendment to their medical information that they believe is erroneous or incomplete;
• Right to request a list of certain disclosures of their medical information;
• Right to request restrictions on how we use and disclose medical information for treatment, payment and healthcare operations;
• Right to request confidential communications;
• Right to request a paper copy of the Notice of Privacy Practices;
• Right to opt out of the facility directory and be a “confidential patient.”
The patient directory lists the patient’s name, room number and phone number.

Patients are given the opportunity to “opt out” of the directory.

Opting out of being listed in the directory helps to better protect privacy for patients who choose to do so.

In addition to confidential patient flags, we also use Break the Glass to protect confidential patients or patients with sensitive diagnoses such as:

- Chadwick Center - Victims of violent crimes or abuse
- CAPS - Behavioral Health patients
- Children of employees
- Employee records
- High profile cases
Think Twice Before Breaking the Glass

• The name fits: don’t break the glass... unless it’s absolutely necessary.

• Break-the-Glass (BTG) is an Epic feature that allows users to gain access to a restricted patient record. The act of gaining access to a restricted record is called breaking the glass.

• BTG forces users to think twice about the patient information they are about to access. It displays a security screen that requires users to enter the reason why they need to access a record that has been marked sensitive.

• The goal of BTG is to prevent users from accidentally looking at or clicking into a record that they did not actually intend to access, and to deter users from accessing records for curiosity viewing.

• An audit trail stores details of the event when a user chooses to Break-the-Glass. Each time a workforce member accesses a record protected by BTG, it is recorded and sent to the privacy office for review and action, when necessary.
Mr. Zhou was a cardiothoracic surgeon from China working as a researcher at UCLA. He was sentenced to prison for unauthorized access to medical records. He pleaded guilty to 4 misdemeanor counts of illegally accessing and reading confidential medical records. Judge sentenced him to four months in federal prison, followed by a year of supervised release. He was also fined $2,000. This was a noteworthy case as it was the first to result in severe sanctions against an individual even when the information was not further leaked, sold or used improperly. The case was part of a larger settlement with UCLA in which they agreed to pay a $865,000 fine.
If you don’t have a legitimate business reason to access the patient’s record, back out - - Don’t go any further.

If you do need to access the record, follow these steps to document your business need for accessing the record with BTG protections:

1. When a user tries to open a restricted patient’s chart, they will receive the Break-the-Glass warning.
2. Press the magnifying glass to see a list of reasons from the Category List.
3. Most users select “Direct Patient Care”.
4. Users selecting “Clinical Research” as their reason for breaking-the-glass will be prompted to enter the 4-digit RCHSD study number. Users selecting “Other” will need to enter a detailed free text explanation. Further explanation is not required for the remaining categories, but a user may enter free text here to explain or provide more detail.
5. User enters their Epic Password and clicks “Accept”. They will receive access to the patient’s record.
Let’s Learn From Other’s Mistakes

• Read On to Learn More About:
  – Additional privacy violations in the news
  – Government’s response to privacy violations/enforcement actions
  – Our response (what we are doing to keep these types of events from happening here)
A physician practice violated HIPAA while using Internet-based calendar and email services. Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona, has agreed to pay HHS a $100,000 settlement. Staff posted clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible. Phoenix Cardiac Surgery violated HIPAA by emailing patient information from an Internet-based email account to workforce members’ Internet-based email accounts.

“This case is significant because it highlights a multi-year, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules. This settlement highlights the need for all providers, regardless of their size, to understand the implications of the technology they use in their practices, to implement policies and procedures for HIPAA compliance, and to obtain business associate agreements where needed”.
CPM 11-65, Appropriate Use of RCHSD Email, is summarized as follows:

- Policy applies to all users including, but not limited to, employees, medical staff, contractors, students, and volunteers.

- We require the use of encrypted email for all communications that include PHI, confidential, proprietary and/or privileged information sent outside of RCHSD.

- RCHSD email must be used to conduct RCHSD business. Personal email addresses may not be used when conducting RCHSD business regardless of whether the email contains patient PHI or other sensitive information.

- Users are also reminded that scheduling for work purposes should be done through the user’s RCHSD Outlook account, as opposed to a user’s personal calendar (e.g., Google Calendar). Staff members shall not support calendaring outside of RCHSD Outlook.

- Users must not transmit confidential or proprietary information to unauthorized recipients, including but not limited to their personal email or future employer email addresses. Proprietary information is information that belongs to our organization.
The Million-Dollar Subway Ride

MASSACHUSETTS GENERAL HOSPITAL

A patient complained to the Office for Civil Rights (OCR) that their PHI was lost along with the information of 192 other patients. An employee took billing encounter forms and daily office schedules home to work on them over the weekend. Documents included patient names, dates of birth, MRN, insurer name and policy number and diagnoses. The employee left the documents on a subway train while commuting to work and the documents were never recovered. Mass General was found negligent in providing appropriate safeguards to protect the PHI when removed from their premises and they impermissibly disclosed PHI. A large fine was imposed and they were also asked to complete a three year corrective action plan designed to improve compliance.

The hospital will pay out $1 million, stemming from the loss of patient records on a Red Line train two years ago. A hospital employee who had taken work home mislaid the papers. They were never found.
Cancer Care Group, a 13 physician oncology practice in Indiana, was fined $750,000 for a stolen laptop with ePHI stored on it that was taken from an employee’s car. The stolen bag contained the employee’s computer and unencrypted media back up which contained names, addresses, dates of birth, social security numbers, insurance information and clinical information of 55,000 current and former Cancer Care patients.

The settlement imposed on this small organization demonstrates the seriousness with which OCR views HIPAA non-compliance.
Preventing Unauthorized Disclosure

- Keep printed patient information secure at all times.
- Never leave laptops or devices that contain PHI unattended in open areas such as cars, restaurants or waiting rooms.
- Never leave printers unattended when printing sensitive information.
- Never leave your computer monitor open towards public view when patient information is being accessed.
- Report suspicious activities to the Service Desk.
- Report suspected HIPAA violations through the Safety Reporting System (SRS).
Use of Social Media

- Do not share on social media any patient information acquired through your time spent at work, even if the information is public;

- Posting patient information to social media sites such as Facebook, Tumblr, Twitter, Instagram or a Blog without authorization is a violation of the patient’s right to privacy and confidentiality;

- Even if you think you’ve de-identified the information, it still might be identifiable to others. Even if the name of the patient is not used -- any detailed description of the patient that could reasonably identify the patient could be considered a privacy violation.
Criminal HIPAA Conviction for Respiratory Therapist

A former respiratory therapist has been convicted on criminal HIPAA violations by a federal jury in Ohio. The jury agreed with prosecutors that the protected health information of patients was wrongly obtained and that PHI was used to seek and obtain intravenous prescription drugs.

The individual was employed as a respiratory therapist at the ProMedica Bay Park Hospital in Oregon, Ohio. Over a period of 10 months, she improperly accessed the medical records of 596 patients. The Respiratory Therapist was permitted access to patient records in order to conduct her work duties; however, she was only permitted access to the records of patients she was treating. The employee abused her access rights and viewed the PHI of other patients without authorization, according to the prosecution.

Nurse Faces Jail Time for HIPAA Violations

This HIPAA violation case example shows how important it is to train staff before there’s a problem. An employee at a midsize clinic was peripherally involved in a lawsuit when a car accident victim sued her husband. When the plaintiff became a patient at the clinic, the employee peeked at the patient’s file and gave private info to her husband. The husband called the plaintiff and demanded that the lawsuit be dropped. The plaintiff quickly called the clinic and the Attorney General's office to complain. The employee faces a $250,000 fine and up to 10 years in prison if convicted.
What are the Penalties for Violating Patient Privacy and Why Such a Hard Line Approach?

Rady Children’s has a zero tolerance policy for violating patient confidentiality by inappropriately accessing patient information. *Intentional unauthorized access of medical records may result in termination.* Even access to an employee’s own child’s information may result in corrective action. These types of access will also need to be evaluated to determine if the incident is a reportable breach.

State and Federal laws are very clear about protecting patient privacy. *There are serious consequences to hospitals and individuals for violating patient privacy.* Regulators are increasing investigations and sanctions on facilities and individuals for privacy breaches.

In addition to Federal HIPAA laws, the California Department of Public Health (CDPH) has a Medical Breach Enforcement Division which investigates breaches and conducts site visits for unauthorized access breaches reported to the CDPH. *We are also required to provide CDPH with the contact information of the person involved in an incident involving inappropriate access to patient information as they will be reaching out to the individual as part of their investigation.*

*CDPH has indicated that they may hold individuals personally responsible for these types of incidents (through fines, enforcement, notification to certification boards, etc.).*

Not only do we want to minimize our risk as an organization, we also have a duty and responsibility to our patients and families to diligently protect their health information.
So How Can You Use Patient Information?

• **ONLY TO DO YOUR JOB!**

• You may access patient information only if it is necessary for you to do your job and care for the patient, and only the information you need for that purpose. Remember: this is part of the “Minimum Necessary Standard.”

• You may give information to other employees, physicians and other healthcare providers who are involved in the patient’s care.

• You may not access or view patient information for personal use or curiosity.

• At all times, protect patient information as if it were your own.

• Violations of RCHSD policy will result in corrective action up to and including termination.
Be Aware of What Hat You Are Wearing When Accessing Patient Information

*The workforce member hat:*
Workforce members cannot access, inspect or make copies of their own record or the records of their spouse, child, domestic partner, significant other or any other relative’s record without following the proper procedures;

*The parent/guardian hat:*
All requests for access, inspection or copies of your own record or your child’s record must be submitted in writing on an Authorization for Disclosure of Health Information Form to the Health Information Management Department.

Information may also be accessed through My Chart. Do not access this information in Epic or other clinical information systems. If you need MyChart access to your/your child’s record, contact the treating provider.
**Is it All Right for Me to....?**

*Search for or look up my name, my child’s name, another relative’s name, or a co-worker/co-worker’s family in the Epic patient look up (search) screen?* I’m just checking to see if the name shows up in our system, and I’m not going any further into the medical record.

No. Searching for a patient name in the patient lookup screen brings up the patient’s demographic information in the electronic medical record (EMR). Elements of a patient’s demographic information can be considered protected health information under law. This access is also tracked by our audit systems, even if you don’t select or view anything further. Searching in this manner is against our policies and will result in corrective action. Any access to patient information in an EMR will also need to be reviewed as a possible privacy breach.

*Use Epic or any computer system with patient information to look up my own information such as test results, billing information, or past medical records?*

No. You will need to go through the same steps as any other patient to obtain information – access your information via MyChart, contact your provider directly, or contact the Health Information Management Department and sign necessary release authorizations, etc.

*Look up information about my children in Epic or other computer systems?* I need to verify some upcoming appointments, and I could just look them up.

No. There is a big difference between being an employee and being a parent. When you are wearing the parent hat, you can sign-up for MyChart, or contact your child’s provider directly, just like any other parent. All other requests for information need to go through MyChart or Health Information Management and will require a signed authorization.

*Access information about my friend or relative whose child is in the hospital via Epic?*

No. If you do not have a legitimate work reason to access a patient record, you may not look up or access patient information.

*Ask a co-worker to look up patient information in Epic for my personal use?*

No. This would put your co-worker in a difficult position as this is a violation. You will need to follow the same procedures as any other patient or parent/guardian.
Monitoring and Auditing: Things We Actively Audit

• Break-The-Glass (BTG) audits;

• Same name match audits (tracks workforce member access to a record of a patient who has the same last name);

• Random audits – system randomly selects an employee; review performed to determine whether access was required in order for the person to do their job;

• Focused audits on a particular patient or employee conducted as a result of a concern call.

All computer systems have audit trails showing who has been in a patient’s record, what information the person accessed, whether information was printed, and how long the person was in that system. This information is audited and reviewed on a continual basis.
Failure to Comply with Policies

• Individuals are required to comply with all privacy and security policies.

• An individual found in violation of these policies will receive corrective action based on the nature of the violation, frequency, and the severity of their action.

• Accessing patient information that is not needed for you to do your job will likely result in termination.
Your Role in Privacy and Security Compliance

• **Understand** the reasons for confidentiality and agree to abide by our confidentiality policies and procedures;
• **Keep patient information confidential** at all times including electronic, written and verbal information;
• **Report** suspected or known violations of confidentiality and security such as:
  - Unauthorized or suspicious visitors;
  - Logged-on but unattended workstations;
  - Uncontrolled access to areas that house equipment and/or PHI;
  - Passwords on Post-it™ notes;
  - Staff accessing records without a need to know.
Privacy Breaches: How Do They Happen?

- Faxing documents with PHI to the wrong individual/location;
- Wrong patient label placed on a document and handed to the wrong patient/family;
- Not checking patient identifiers then handing documents to the wrong patient/family;
- Transposing a number when typing in a medical record number to look up an address; documents get sent to incorrect patient/family;
- Searching for a patient and not validating date of birth; another patient with the same name is selected in error;
- Selecting the wrong Primary Care Provider (PCP) for a patient; documents then go to the wrong provider.
What Can You Do to Protect Patient Information?

• Be mindful of your surroundings when discussing patient information;

• Recognize that a child of an employee receiving medical treatment at one of our facilities is entitled to the same rights of privacy and confidentiality;

• Double check documents before handing to patients/family members;

• Don’t leave patient information on the printer or a fax machine unattended, and keep the equipment in a secure area away from traffic;

• Verify the fax number for the recipient. Always use a fax cover sheet with our confidentiality statement;

• Turn computer monitors away from public view.
Despite our Best Efforts, Breaches Do Happen and There are Breach Reporting Provisions

• Under the HITECH Act federal breach reporting requirements, we are required to notify patients (and in certain cases the media) and HHS of breaches of unsecured health information.

• Providers must conduct an analysis to determine whether they have a reporting obligation.
Your Role: It’s Important to Report Potential HIPAA Violations

• So they can be investigated, managed and documented;
• To determine cause and help prevent them from happening again in the future;
• So damages can be kept to a minimum;
• To minimize your personal risk;
• To help us meet strict deadlines for reporting to the patient/patient family, as well as to the state and/or federal government.
If there is a reportable breach, the HITECH Act requires the following notification:

- **Notice to individuals** whose information was breached within 60 days of discovery of the breach;
- **Notice to media** if more than 500 residents of a state or jurisdiction are involved (e.g., patient information that was present on a stolen laptop);
- **Notice to HHS** if 500 or more patients are involved, as well as an annual report to HHS of all breaches that occurred during the preceding year.
Notice Requirements - State

- California law is more stringent than federal law.

- We must notify the patient and California Department of Public Health (CDPH) within **15 business days** of confirming a breach (for CDPH licensed areas).
Reporting a HIPAA/Privacy or Security Concern

If you become aware of a potential breach of patient information, immediately follow these steps:

• Enter a Report in the Safety Reporting System;

• Notify your department manager or supervisor.
The Safety Reporting System is located on the Hospital Intranet under Frequenty Accessed Links.

Reminder: Please use SRS to report PRIVACY/HIPAA/INFO SECURITY concerns. The “Report of Health Information Disclosure Form” should not be used for this.
Reporting Breaches or Other Security Concerns

Use the Safety Reporting System

Call the Chief Compliance & Privacy Officer or the Privacy Manager!

Call the Chief Information Security Officer!

Reporting is Everyone’s Responsibility…do you know the Safety Penguin?
A Recap of What We Learned Today:
What You Can Do to Assure You Do Not Violate Privacy Laws

- Comply with the Confidentiality Agreement you sign, as well as the Code of Conduct;
- Do not take patient information home with you. If you work in the field, always keep patient information secure. Use a lockbox to transport PHI from one location to another;
- Do not leave patient information or other sensitive information in your car or trunk (even if locked), as cars can get broken into or stolen;
- Keep your badge secure at all times. Do not leave your badge in unattended or unlocked vehicles;
- Only share patient information in authorized situations;
- Contact Health Information Management if you need medical records for personal use (your records, your child’s, your relative, etc.) – do not access it directly in Epic!
If You Have Concerns

There are a number of resources available to you. Please do not hesitate to call if you have questions, suggestions or concerns:

• Contact Christina Galbo, Chief Compliance & Privacy Officer at (858) 966-8541 or cgalbo@rchsd.org.

• Contact Melody Herbert, Privacy Compliance Manager at (858) 966-1700 ext. 2483 or mherbert@rchsd.org.

• Contact the IT Security Department at (858) 966-8746 or ITSecuritygroup@rchsd.org

• Call the confidential Compliance Hotline at (877) 862- 4228.
Reporting a Concern to the Compliance Hotline

- There may be times when your concerns cannot be properly addressed through the normal chain of command;

- Hotline is available seven days a week including all holidays;

- Your confidentiality and anonymity are guaranteed to the extent permitted by law;

- Your call will not be recorded or traced;

- All allegations will be thoroughly investigated and verified before any action is taken.
Do You Have a Concern?

Make the right call

Compliance Hotline
1-877-862-4228

24 HOUR TELEPHONE HOTLINE
- Staffed by trained personnel
- Independent from RCHHC
- Important that sufficient detail is shared

This hotline should be used to report concerns about potential violations and to receive follow-up information in confidence.
Non-Retaliation

• You will not be retaliated against for voicing a legitimate concern internally, or to an outside entity.

• If you feel you are a victim of retaliation, please report your concerns to the Compliance Department immediately to initiate an investigation.
We are proud of our strong commitment to the highest ethical standards.

We are focused on complying with the law and acting with integrity at all times.

The RCHHC Compliance Program reinforces the responsibility each of us has to speak up if we see something that doesn’t seem right.

*Always do the right thing!*