



2009 ~ 2010

Ethics & Compliance Training

Audio-version – Make Sure Your
Volume is On

Prepared by:
Sutter Health Ethics & Compliance Services
Sutter Health Information Systems Security



- If you are not able to hear the audio content please read along with the **notes tab** to the left side of your computer screen.
- The slides advance automatically. Please **Do Not** select the “next” button.



Topics to be Discussed

- About Ethics and Compliance Services
- Standards for Business Conduct
- Confidential Message Line
- Patient Billing Practices
- Disability Access
- Conflict of Interest
- HIPAA Privacy Regulations
 - Identity Theft “Red Flags Rules”
 - New Privacy Laws
 - Social Networking
- Information Systems Security Policies



The Sutter Health Ethics & Compliance Program: An Evolution



- Local Compliance Officers are in place to administer the local Compliance Program—which means:
 - **Providing training & advice**
 - Example: Physician coding courses, advice on billing/coding questions, physician arrangements, privacy, etc.
 - **Providing ongoing monitoring of issues**
 - Example: Monitoring to make sure new policies are being followed
 - **Implementing programs designed to ensure compliance with laws and regulations**
 - Example: Ensuring compliance with patient access laws
 - **Providing compliance reporting**
 - Example: Using Ethics Point to capture key compliance issues with reports of all significant known issues...
 - **Providing trending of issues**
 - Example: Are issues affiliate specific or regional? Are problems systemic issues?

Standards for Business Conduct



- The *Standards for Business Conduct* is our organization's statement of ethical and compliance principles
 - Helps guide our operations.
- The Standards include many real-life examples of how our ethical principles apply to your work.

Standards for Business Conduct

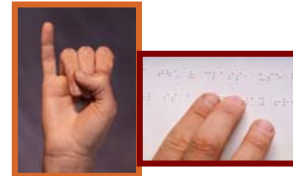


- The Standards also include:
 - How to report issues or concerns
 - Resources available to employees
- Employees must read, understand, sign and abide by the *Standards*. The *Standards* supplement our compliance policies and procedures.
- The *Standards* are available in book form or you can read them on the Ethics and Compliance Services web page. Books are provided:
 - To all new employees
 - To all employees whenever we revise the *Standards*.
- Visit the Ethics and Compliance Services website: <http://mysutter> (click on “Legal and Compliance”)

Standards for Business Conduct

- Sutter Health will provide, at no cost to the patient, language assistance for effective communication to care for patients who are:

- Limited English Proficient (LEP)
- Hearing and visually impaired



- If an interpreter is needed, staff should use either a bilingual staff member who has demonstrated competency as an interpreter or an outside interpreter service.
- ➡ Do not use family members as interpreters except in an emergency or when the patient refuses the offer of an interpreter.

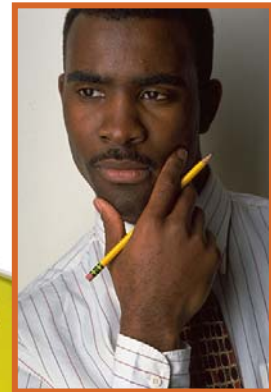


- Children should **NEVER** be used as interpreters.



Reporting Issues and Concerns

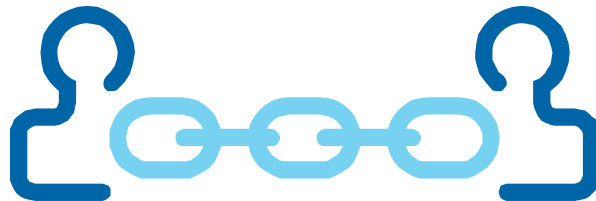
- Every Sutter Health employee has an individual obligation to bring forward questions and concerns about compliance issues.
- What is an issue?
 - A Compliance Issue is any concern reported, **which if proven true**, would:
 - Violate a federal, state or local law or regulation;
 - Violate a Sutter Health policy
 - Violate an Affiliate policy.





Reporting Issues and Concerns

- Resources for reporting include your “Chain of Command” (Supervisor, Manager, Director)
- Other Resources:
 - Human Resources
 - Risk Management
 - HIPAA Privacy Officer
 - HIPAA Security Officer
 - Compliance Officer
 - Call the Confidential Message Line (CML)





Reporting Issues and Concerns

- The CML is intended to **supplement** existing internal communication channels. It is not intended to replace the management team where you work.
- The CML is available when you feel
 - You have exhausted the resources where you work or
 - You feel uncomfortable about bringing an issue to someone in your chain of command.
- Contact the Human Resources Manager at your Affiliate first if the issue relates to:
 - Employment
 - Employee Benefits
 - Other Human Resources Issues



Reporting Issues and Concerns

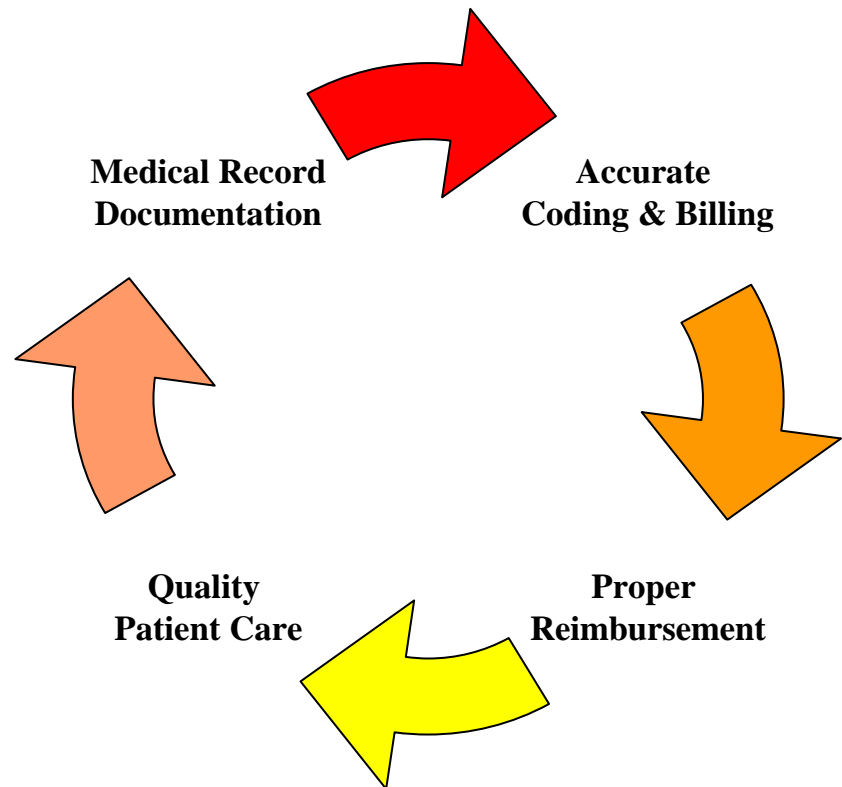
1. Call 1-800-500-1950 (Confidential Message Line)
 - Available 24/7 and get a Live Representative (EthicsPoint)
2. File Reports Online:
 - From home or anywhere else with Internet access: Go to www.ethicspoint.com
 - From work: Go to the Ethics and Compliance Services Intranet site
<http://mysutter/Resources/SystemDepartments/GeneralCounsel/EthicsCompliance/Pages/ConfidentialMessageLine.aspx> click the EthicsPoint icon.





Patient Billing

- Sutter Health has a responsibility to ensure that we bill our services accurately
 - Claims are based on the documentation
- How can we do this?
 - ✗ Ensure that medical record documentation supports the services billed
 - ✗ Accurately code for services rendered following the appropriate coding guidelines
 - ✗ Retain medical records and billing documentation according to policy.





Patient Billing



Coded data from the medical record is used for:

• Internal Uses

- Accurate reimbursement
- Quality management activities
- Productivity
- Budgets
- Case-mix management
- Healthcare planning
- Marketing
- Research activities
- Pay-for-Performance
- Cost reporting
- Auditing & Monitoring

• External Uses

- Coded data is used by the county, state and federal government.
- Future reimbursement determination
- Quality Reporting
 - Leapfrog
 - Healthgrades
- Government Healthcare Planning
 - Flu vaccines
 - Diabetes interventions for children
 - OSHPD

The Federal False Claims Act (FCA)



- FCA began under President Abraham Lincoln during the Civil War in 1863 to prevent defense contractors from defrauding the government. The contractors were selling government property!
- If rules and regulations are not followed, the government has several laws that it can use to investigate and prosecute providers who submit inaccurate bills or other means of waste and abuse of the Medicare and Medicaid program.
 - One of these laws is the Federal False Claims Act.
 - California also has a state false claims act.



The Federal False Claims Act (FCA)

- Any person who knowingly presents or causes to be presented a false or fraudulent claim may be liable under this law.
 - Diagnosis codes or HCPCS codes
 - For outpatient hospital claims each line item is liable
- The government can criminally prosecute an individual or a corporation, or file a civil suit and collect up to three times the amount lost plus fines ranging from \$5,500 to \$11,000 for each false claim.

Both federal and state False Claims Acts protect whistleblowers against retaliation for reporting concerns in good faith.

◆ Retaliation by any person is not acceptable!



The Federal False Claims Act (FCA)



- Billing for services not rendered
- Falsifying treatment plans or medical records to maximize payments
- Failing to report overpayments or credit balances
- Selecting a diagnosis code unrelated to a test for the sole purpose of getting a claim paid.
- Falsifying certificates and billings for services not medically necessary
- Upcoding - The practice of using a billing code that provides a higher payment rate than the billing code that actually reflects the service furnished to the patient
- Unbundling - Fragmenting a service into component parts
- Double-billing - Billing a patient twice for the same service or supply. Also known as “double-dipping”.

Equal Access for Patients with Disabilities



Allowing service animals

Use an Assisted
Listening Device to
amplify sound



Providing magnification for
patients with visual
impairment



Hi-lo tables for easy
access



Equal Access for Patients with Disabilities

- You may need to serve our patients with one of the methods below:
 - schedule a patient for an accessible space,
 - employ accessible equipment,
 - use an alternative communication methods such as pictures, interpreter services or audible formats to assure effective communion,
 - accommodate a patient, visitor or family member who needs it
 - modify procedures to assure that all patients are properly examined, treated and diagnosed.



Health practitioner adapting Mammography procedures to accommodate a person using a wheelchair



Equal Access for Patients with Disabilities

Sutter Health is improving care for patients with disabilities. Steps include:

- ☑ Adopt policies and procedures to ensure disability-accessible care for people with disabilities;
- ☑ Provide annual training on serving patients with disabilities;
- ☑ Resolve disability-access complaint promptly;
- ☑ Acquire and use accessible medical equipment for patient care sites, and
- ☑ Remediate physical accessibility features of its facilities.



Conflict of Interest



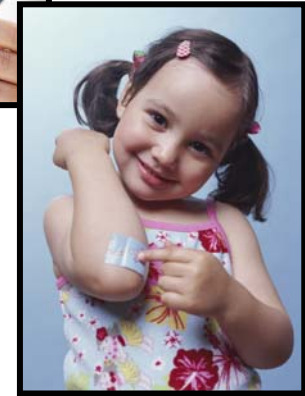
- What is Conflict of Interest?
 - A conflict of interest occurs if an outside interest may influence or appear to influence your ability to exercise objectivity or meet your job responsibilities to Sutter Health.
 - Question to ask yourself: Would an objective observer of your actions possibly wonder if these actions are motivated solely by your responsibilities to Sutter Health?
- Any potential conflicts of interest should immediately be disclosed to the employee's supervisor.



Be sure to check your [Affiliate Conflicts of Interest Policy](#). It may be more strict.



Conflict of Interest



- Receiving an **I-Pod** as a gift or **trips** from a pharmaceutical company that wants to sell its products to Sutter Health.
- Using Sutter facilities to do medical **research** for another organization.
- The director of surgical services is married to the external vendor who supplies their prosthetic **implants**.
- Using Sutter resources, such as business e-mail and **supplies**, to advertise for your own side business.
- Selling a **software** program that the employee developed as part of their job at Sutter Health.

Material gift	Nominal Gift
Any gift, favor, loan, entertainment, or anything else of <u>value greater than one hundred dollars (\$100)</u> per year from any one person or entity.	Any gift, favor, loan, entertainment, or anything else of <u>value equal to or less than one hundred dollars (\$100)</u> per year from any one person or entity.



Conflict of Interest

- Policies embody good business practices that help us avoid improper conduct or conduct that *appears* improper.
- These policies also help us ensure we comply with federal and state legal requirements, such as:
 - The Federal Anti-Kickback Statute
 - Federal Laws Governing Tax-Exempt Organizations
 - California Laws Governing Non-Profit Companies

Bottom line: We are held to a higher standard!





Conflict of Interest Question

- “We are trying to choose which new equipment we should buy for my department and one of the vendors has offered gifts to members of the committee. What should we do?”
 - You should never accept a gift that is intended to influence, or in exchange for, the award of a contract or relating to the selection of a provider of goods or services.
 - Is it really “free”?
 - Sutter policies for vendor may be violated.

**This example is based on the language in the Sutter Health Administrative Conflict of Interest Policy. Please see your affiliate policy as it may be more stringent.*



Conflict of Interest

“I understand that a medical device supplier has flown a manager to a resort area to attend a conference.”

Do you think this is an acceptable practice?

Yes

No



Identity Theft “Red Flag Rules”

- ▶ The Federal Trade Commission published regulations called the “Identity Theft Red Flag Rules”.
- ▶ The red flag rules are focused on detecting, preventing and mitigating harm from identity theft.
 - ▶ Effective November 1, 2009.
- ▶ Sutter Health affiliates have Identity Theft Prevention programs that have been adopted by their Board of Directors.



Identity Theft “Red Flag Rules”



- ▶ Identity theft is stealing the identity of others by using their
 - credit card,
 - drivers license,
 - insurance cards,
 - social security or other personal identification numbers.
- ▶ The identity thief uses the information to open new accounts or access existing accounts.
- ▶ A “red flag” is a pattern, practice or specific activity that could indicate identity theft.

Identity Theft “Red Flag Rules”

Examples of red flags include:

- ▶ Presentation of suspicious documents
 - Driver’s license, insurance cards etc.
 - Photos that don’t resemble the patient
 - Signatures or medical information that does not match information on file
- ▶ Questions from a patient about a bill for services they did not receive, a collection notice, or a negative credit report.
- ▶ Presentation of an invalid or duplicate SSN or an address or phone number that does not exist.



Identity Theft “Red Flag Rules”



- ▶ You can prevent identity theft by:
 - Verifying the identity of patients and customers
 - Protecting the confidentiality of all patient, employee and business information.
 - Disposing of all documents containing confidential information according to your affiliate’s policies and procedures (e.g. shredding).
 - Contacting your Information Systems department before transferring or disposing of computer equipment containing confidential information.
 - Becoming familiar with the Sutter Health Identity Theft Program document available on the Sutter Health Risk Services MySutter web site.



Reporting Privacy Breaches California Law



- If there is a privacy breach, California law requires licensed health facilities to notify the **patient** and the California Department of Public Health (CDPH) within five (5) days of detection. *Health and Safety Code section 1280.15*
- A privacy breach under this law is defined as the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use.

Reporting Privacy Breaches California Law

- Facilities covered by these regulations include:
 - General acute care & psychiatric hospitals
 - Skilled nursing facilities
 - Home health/hospice agencies
 - Licensed ambulatory surgery centers
 - Licensed clinics – This is usually hospital-based outpatient clinics, NOT the Medical Foundations.
- CDPH will investigate privacy breaches and may assess penalties up to \$25,000 per patient (maximum of \$250,000 per event).





Reporting Privacy Breaches California Law

- In addition, the State can assess penalties against **individuals** for these breaches. This means that the State can:
 - *Investigate* individuals, including physicians, nurses, support staff etc.
 - Require individuals to pay *fin*es
 - Recommend that an individual's *licensing board* investigate or discipline an individual

Reporting Privacy Breaches

Federal Law - HIPAA

- HIPAA rules require **all SH affiliates** to report breaches of unsecured Protected Health Information (PHI) which result in significant financial, reputational, or other harm to a patient. *CFR § 164*
- Significant harm is determined by a documented risk assessment.
- PHI is considered unsecured if it is not made unusable, unreadable, or indecipherable to unauthorized individuals by:
 - Encryption of electronic PHI
 - Destruction of paper and electronic media





Reporting Privacy Breaches Federal Law - HIPAA

- Breaches involving more than 500 patients must also be reported to the patient and to the Federal Department of Health and Human Services. (DHHS).
 - If the 500 patients are from a single state the breach must also be reported to the media.
- DHHS may assess penalties from \$100 to \$50,000 per violation.
- Criminal penalties (fines and imprisonment) may also be levied against providers and **individuals**.



Examples of Privacy Breaches

- Examples of privacy breaches that may be reportable include:
 - Misdirecting faxes containing PHI outside the Sutter health care system.
 - Inappropriately accessing records of family members, friends, or co-workers.
 - Providing discharge instructions or other paperwork to the wrong patient or provider.
 - Using social networking sites to discuss specific patients and their health conditions.
 - Inappropriately sharing information gained while performing professional duties with others who have **no need to know**.

Your Responsibilities



- Be knowledgeable about and follow SH/affiliate policies and procedures related to the use and disclosure of PHI.
- Access, use, and disclose PHI only when it is needed to perform your job duties.
- **Immediately** report any suspected privacy violations to your department manager, your affiliate Privacy Officer, Compliance Officer or others in your Chain of Command.

General Information Security Management



- Winter was approaching and Sally found a really great screensaver with a dancing snowman. She was able to download it onto her work computer. “It’s just a screensaver, nothing will happen,” thought Sally.
- A few days later she noticed that she could not open certain software that she needed to do her job. Little did she know that the screensaver contained a virus.
- Use only SH authorized and properly licensed software and hardware.
 - Downloading things such as screensavers can contain viruses



General Information Security Management

- All electronic data stored or processed on your affiliates information system is property of Sutter Health and activity may be monitored
- Your Sutter Health affiliate reserves the right to inspect and search any and all Sutter Health property, with or without the employee's presence.
 - Inspection can be done at any time, without prior notice.
- You will be asked to sign a confidentiality agreement annually.

Electronic Access to Sutter Health's Network



- Your access is based on your individual role & responsibilities.
- You are responsible for limiting your access to information needed to perform your job duties.
 - For example, if you are a patient biller you would not necessarily need access to the payroll system.
 - Ask your manager if you are not sure.



Passwords



- Passwords are confidential – Do not share your password with others.
 - Do not keep your password written where others can see it or access it.
 - Change your password from time to time. Pick a “strong” password that is hard to guess.
 - Use letters, numbers, and characters
- No one, including your Supervisor/Manager, should ask for your password.
- You have a unique user account and will be held accountable for its use.
 - If you believe that your password has been compromised, contact your Supervisor/Manager and/or Help Desk immediately.



Why We Need Workstation Security

- Security measures allow us to protect our workstations and our confidential information from:
 - Physical loss, theft, damage or unauthorized access
 - Displaying confidential information to unauthorized personnel
 - The introduction of malicious software (i.e. viruses) into the system.
- Do not modify SH IS Resources that have been provided to you
 - no unauthorized installation of software or hardware is allowed!
- Keep personal use of workstations to a minimum
 - Personal use must not interfere with work and must not violate other policies





Internet and E-Mail Usage


- Public networks, such as the Internet, are **not secure**. When sending confidential patient or business information it is your responsibility to use a secure encrypted transfer method.
 - E-mail and Internet access is provided to support Sutter Health business purposes.
 - **Certified Mail** is Sutter Health's standard secure mail solution. Contact your **Help Desk**, if you need a Certified Mail account.
- Do not auto-forward your email outside of the Sutter Health network to your home email or another account.



Internet and E-Mail Usage



- E-Mail or Instant Messages that are disruptive or contain inappropriate, sexually explicit or otherwise offensive or controversial material are prohibited.
- Sutter Health IS resources should not be used to:
 - Conduct or manage personal businesses;
 - Using the copy machine or other office supplies
 - Engage in political lobbying; or
 - Engage in fundraising activities or solicitation for or on behalf of any third party, unless it is for a pre-approved purpose.
 - Pre-approved activities may include internal or external community events (e.g. the United Way, March of Dimes, Make a Wish, Annual Employee Giving Campaign, or other Annual Events).



Reporting an Incident

- A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with operations in an information system.
- If you suspect a security incident, please report it to your Affiliate Information Systems Security Officer or your Compliance Officer immediately. You may also contact the confidential message line.
- Plan to provide basic information:
 - Your name and phone number
 - Date and time of when the incident occurred
 - Was Protected Health Information (PHI) involved?
 - Facts or observation that led to report the suspected incident
 - Any other unusual information and/or circumstances surrounding the event



Sutter Health Information Systems Security Policies



Why?

These policies help us:

- To protect patient information
- To protect our vital system resources
- To comply with the state and federal laws

It's the right thing to do!

