Live Training Sign-In Sheet

Date Training Performed:

Titles of Slide Decks Used During Training: Code of Conduct, General Compliance, Privacy Training for Students

Person/s Presenting Training:

Name	School/Program	Last 4 digits of SSN	E-mail Address	Department	Job Title	Supervisor's Name

DETAR HEALTHCARE SYSTEM EMERGENCY CODES

Code RED	Code BLUE	Code GREY	Code TRIAGE	Code BLACK	Code SILVER	Code GREEN	Code ORANGE	CODE PINK
What does it Signify?	What does it Signify?	What does it Signify?	What does it Signify?	What does it Signify?	What does it Signify?	What does it Signify?	What does it Signify?	What does it Signify?
FIRE	CARDIAC OR RESPIRATORY ARREST	SECURITY/ POTENTIAL VIOLENCE	INTERNAL OR EXTERNAL DISASTER	TORNADO	BOMB THREAT	Patient elopement	Hazardous Material Spill	INFANT ABDUCTION
Who should call the code?	Who should call the code?	Who should call the code?	Who should call the code?	Who should call the code?	Who should call the code?	Who should call the code?	Who should call the code?	Who should call the code?
Staff member who discovers fire or smoke should call 4144 to report or designate someone to do so.	Staff member who discovers the arrest.	Staff member encountering the disruptive behavior or weapon will call the code or designate someone to do so.	Administrator or House Supervisor Until his arrival.	The Safety Officer or designee will call the code when information is received that a tornado has been sighted.	A code will NOT BE ANNOUNCED until it is verified there is a danger.	Charge nurse or staff designee	Notify safety manager, John Wallace, ext 6165	Staff discovering an infant or child is missing.
What should staff do?	What should staff do?	What should staff do?	What should staff do?	What should staff do?	What should staff do?	What should staff do?	What should staff do?	What should staff do?
Follow the R-A-C-E GUIDELINES: R – Rescue/ remove from immediate danger. A – Alarm. Pull nearest fire alarm. Dial 4144 and give exact location. C – Contain. Assure all smoke doors are closed. E – Extinguish. Use fire extinguishers to help control the fire. E – or Evacuate if necessary	Clinical staff initiate CPR. Designated staff member dials 4144 to have Code BLUE paged and give location. Non-clinical staff report to nurses station to assist with phones. Nursing staff not involved in code will assist in contacting patient's primary M.D. and relay orders. Will assist in monitoring other patients until code is over.	Staff member will call 4144 to announce Code GREY and give location. Plant Engineering and Security staff will move quietly to the area and determine the need to call police. If Code Grey is due to patient behavior, the attending physician will be notified, in addition.	After Administrator or designee has announced Code TRIAGE, staff will activate the disaster plan that is available in the Environment of Care emergency plans book. Department Director will determine and initiate buddy call list if additional staff is required.	For Tornado Watch: Close all blinds; provide patients with pillows and pull all drapes and curtains. Tornado Warning: Above + Move all patients into hallway, close doors to hallways, move all visitors and other staff to hallways. Stay away from glassed areas in hallways.	Person who receives call should gather as much information as possible and complete the form in the EOC plans manual. Contact CEO and Director Plant Operations stat. Administration will notify police and notify staff to turn off all cell phones and pagers. Administration and local law enforcement will coordinate the search.	Make self available to answer questions	Trained user cleans up spill with appropriate personal protective equipment and decontamination materials. Complete Incident Report	Secure all exits from the unit of disappearance and initiate a search. Everyone be on the alert for suspicious parcels or bags (i.e., duffle bag) being carried that may be large enough to conceal an infant. Hospital lock down – no one leaves until all clear given.

Additionally, at DeTar we have several rapid response teams:

CAT (CLINICAL ASSESSMENT TEAM)--a support team called by staff to mobilize assistance for a clinical consult/intervention

STROKE ALERT-- can be called from anywhere in the hospital to mobilize radiology, respiratory, pharmacy, house supervisor to initiate protocols

CODE 3--called to mobilize the lab, radiology, house supervisor for an incoming medical emergency via EMS to the emergency department

TRAUMA ALERT—called to mobilize resources including lab, radiology, house supervisor, and security to the emergency department for incoming trauma patient(s)

STEMI ALERT—can be called from anywhere in the hospital to mobilize a select group of health care professionals to institute protocols for a new onset myocardial infarction (heart attack) patient

To meet the possibility of an active shooter in the facility, the following has been developed:

Active Shooter "Code Gray--Dr. Cannon"

Upon notification of Code Gray—Dr.Cannon:

1. Have an escape route and plan in mind
2. Evacuate regardless of whether others agree to follow
3. Leave your belongings behind
4. Help others escape if possible
5. Prevent individuals from entering an area where the active shooter maybe
6. Keep your hands visible
7. Follow instructions given by Law Enforcement Officers
8. When safe, dial 911 and give police any information you may have about the shooter and/or the shooter's location

If you are in the area with the shooter:

☐ Hide in a closed room, lock the door if possible and move non-life support equipment and furniture in front of the door to provide protection if shots are fired in your direction

☐ Silence your cell phone and/or pager

☐ Turn off any other sources of noise (radio, TV, etc…)

☐ Hide behind large items

☐ Remain quiet

☐ Dial 911 to alert the police to the shooter's location. If you cannot speak, then leave the line open to allow the dispatcher to listen

DEFEND yourself as a last resort and only when your life is in imminent danger.

Your charge nurse, head nurse, supervisor, and/or manager can assist you in an emergency.

FAILURE(S) OF UTILITIES /COMMUNICATIONS

FAILURE OF	WHAT TO EXPECT	RESPONSBILITY OF
Electrical Power	Emergency generator will produce electrical power….significant areas will remain with power. RED plug outlets to be used.	Make sure life support systems are maintained…ventilate patients if necessary. Provide support to patients/visitors. Use flashlights as needed.
Medical Gases (including Oxygen) and/or leaks and vacuum	Gas alarms, no oxygen, no medical air, no vacuum.	Report gas alarms to Plant Operations ASAP; follow directions. Hand ventilate patients, use portable oxygen (call for additional cylinders from Respiratory Department. Report lack of medical air to Plant Operations. Call for portable suction devices from Purchasing Department.
Water	No Water	Use bottled water for drinking / minimize water use for other procedures. Seek hospital plan of action for further instructions, as how water will be conserved. Observe and report potential areas of concern to Plant Operations and / or Supervisor.
Elevator stopped between floors	Alarm can be sounded and/or use of telephone in the elevator compartment.	Maintain communication with those in the elevator, assuring them that assistance will be made available as soon as possible. Plant Operations will be the department that assists with this problem.
Patient Equipment & Systems, including patient call systems	Equipment fails or fails to perform satisfactorily.	Remove non-working equipment from the work area and provide care to patient as necessary. Equipment must be tagged with fault and sent to BioMed; a variance report need to be generated ASAP and charge nurse/supervisor notified. If call system fails provide simple device like “bells” and/or frequent rounds.
Telephone, fax machines, including hospital beepers & pagers	No Phone service; unable to receive or send FAX messages; unable to reach person/department by beeper-pagers.	Use overhead paging personal phones computers, walkie-talkies, and couriers. Report to Plant operations to initiate repairs.
Computer	Failure of computers for documentation, test requests, reports, E-mail	Report to use of manual methods, refer to IS Department for more instructions, use telephone, FAX, and/or use couriers.

Important Things to Remember

The emergency phone number is **4144.**

For security reasons and patient rights you are asked to wear your institution's name badge at all times.
Evacuation plans and location of fire extinguishers are different as the units vary…**YOU** must learn about these when you are on a unit.

Please call Charlene Adams, RN, Director of Education, 361 788-6135, for any questions or concerns regarding this information or any other matters.

Infection Control

DeTar Healthcare System used the "category" isolation system. Universal precautions are utilized on **ALL** patients. Isolation gowns are disposable. Rooms, 564, 464, a specified room in L&D, day surgery, pediatrics, GYN and ICU with special ventilation room designed for patients with diseases like TB; care givers must wear special masks.

Personal Protective Equipment (safety glasses, goggles, etc) are located on each unit. Gloves and needle disposable boxes are located in every patient room. **DO NOT RECAP NEEDLES** before disposing them in the sharps box.

The **RED** biohazard bags are used for infectious trash: used suction canisters, blood bags and tubes, chest drainage systems, emptied Foley bags, very bloody bandages, peri-pads, diapers, etc. Alcohol preps with a drop of blood do not have to go into the red biohazard bag.
ALL soiled linen is treated as infectious and is placed in **BLUE** plastic bags.
All contaminated items going to Central Sterile for reprocessing must be bagged.

Report needle sticks and blood/body fluid exposure to infection control director, Leslie Hanslik, at 361 788-6318.

C: allied heath emergency information

Community Health Systems

Code of Conduct

CHS Community Health Systems

2016-2017

TABLE OF CONTENTS
COMMUNITY HEALTH SYSTEMS
CODE OF CONDUCT

COMMUNITY HEALTH SYSTEMS[1]
CODE OF CONDUCT

STATEMENT OF BELIEFS

We believe that each community served is different and that the success of each facility depends upon the actions of each colleague, physician, contractor, and agent of that facility. We have adopted the following Statement of Beliefs that summarizes the commitments of the organization's constituents to our patients, colleagues, physicians, and the communities served.

We are dedicated to providing personalized, caring, and efficient service to our patients with total satisfaction as our top priority.

We recognize the value of each colleague in providing high quality, personalized care to our patients.

We encourage colleague involvement in quality improvement to improve processes on an ongoing basis.

We advocate participation in community activities.

We are committed to involving physicians in partnership, both as consumers of service and as providers in ensuring quality care.

We are devoted through services, quality, and innovation to provide continued healthcare leadership in the communities we serve.

Although aspects of the Compliance Program focus on various legal areas, the primary focus of the Compliance Program is to ensure that internal policies and controls, training and education, and auditing and monitoring are in place to help prevent, detect, and deter fraud, abuse, and waste in government health care programs. Accordingly, we are dedicated to compliance with all federal, state, and local laws, rules, and regulations, including privacy and security of patient health information, coding, billing, and documentation guidelines, and financial arrangements.

[1] Community Health Systems, Inc. ("CHSI") is a stock holding company whose shares are traded on the New York Stock Exchange ("NYSE"). Its subsidiary companies and partnerships own or lease and operate their respective hospitals and other assets and businesses. Community Health Systems, Inc. does not have any employees. Throughout this document, we refer to Community Health Systems, Inc. and its consolidated subsidiaries in a simplified manner and on a collective basis, using words like "we," "our," "our organization," "CHS" and the "Company". This drafting style is suggested by the Securities and Exchange Commission, or SEC, and is not meant to indicate that Community Health Systems, Inc. or any other subsidiary of Community Health Systems, Inc. owns, controls, or operates any asset, business, or property. The hospitals, operations, and businesses are owned and operated, and management services provided, by distinct and indirect subsidiaries of Community Health Systems, Inc. CHSPSC, LLC ("CHSPSC"), an indirect subsidiary of CHSI, provides management and consulting services to the local operating entities pursuant to the terms of management agreements with the local entities. CHSI has no employees, and those officers and directors of CHSI who are identified in this document are employed by CHSPSC.

WELCOME

Dear Colleagues,

It is my pleasure to welcome you to Community Health Systems.

When you decided to join our organization, you made an important personal and professional decision. Your decision included a responsibility not only to provide high quality healthcare, but also to personally conduct yourself in such a way that is consistent with the organization's commitment to operate with the highest standards of integrity and behavior.

Every person, business or government entity that comes in contact with a CHS representative expects this level of commitment, and so do we. It's the way we do business.

We have created a Code of Conduct which starts with our Statement of Beliefs and is an integral part of our compliance program. It should be used with policies and procedures, applicable regulations and laws and good common sense. It serves as a solid framework for business decisions and, pursuant to the Affordable Care Act and similar laws, it is mandatory that each of us comply with this Code of Conduct every single day.

As a condition of your association with CHS, it is required that you read the Code of Conduct so that you are aware of these standards.

Thank you very much.

Sincerely,

Wayne T. Smith

INTRODUCTION

The Code of Conduct (the "Code") is designed to provide all persons and businesses associated with Community Health Systems, Inc. and its subsidiaries (collectively "CHS" or the "organization") including directors, officers, colleagues, physicians, contractors, and agents with guidance to perform their daily activities in accordance with the organization's ethical standards and all federal, state, and local laws, rules, and regulations. The Code is an integral component of the organization's Compliance Program and reflects our commitment to achieve our goals within the framework of the law through a high standard of business ethics and compliance. This Code of Conduct has been adopted by the Board of Directors of Community Health Systems, Inc. and by each subsidiary.

The Code encompasses a summary of many topics from Compliance policies and other department policies. The Compliance policies and other department policies and procedures provide more specific guidance relating to the topics presented in the Code. It is the obligation of CHS colleagues to be knowledgeable about and adhere to the policies within these policies, as well as the Code.

The Code is based on federal, state and local regulatory compliance and therefore compliance with all policies incorporated into the Code of Conduct is mandatory. Failure to comply with any of the provisions of this Code of Conduct may result in disciplinary action by your specific facility for colleagues and cancellation of contractual or business relationships with physicians, contractors, and agents. Violations of portions of this Code relating to federal healthcare benefit programs may lead to severe consequences including, but not limited to, civil monetary penalties and/or exclusion from federal healthcare benefit programs for colleagues, physicians, contractors, agents, facilities, or CHS. Questions or concerns regarding interpretation of this Code or any Compliance policy should be addressed to a supervisor, the Facility Compliance Officer (FCO)[2], the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program.

THE ROLE OF MANAGEMENT

Though all CHS colleagues are required to follow the Code of Conduct, all managers, directors, supervisors, board members, and corporate staff are expected to set the example by conducting their business affairs consistent with the highest ethical and legal standards. Managers must ensure their staff has the tools to perform assigned tasks according to applicable laws, rules, regulations, and policies. In addition, the Board of Directors of Community Health Systems, Inc. has established the Executive Compliance Committee (the "Committee"). The Committee is responsible for the adoption, amendment, and ultimate enforcement of the Compliance Program. The standing members of this committee are:

Wayne T. Smith, Chairman and Chief Executive Officer
Tim Hingtgen, President and Chief Operating Officer
W. Larry Cash, President of Financial Services and Chief Financial Officer
Lynn T. Simon, M.D., MBA, President, Clinical Services and Chief Quality Officer
Rachel A. Seifert, Executive Vice President and General Counsel
Martin G. Schweinhart, Executive Vice President of Administration
Mark Buford, Senior Vice President, Internal Audit
Michael Lynd, Vice President, Financial Services
Andi Bosshart, Senior Vice President, Corporate Compliance and Privacy Officer

[2] Facility Compliance Officer ("FCO") collectively refers to Compliance Officers of any CHS affiliated entity including but not limited to hospitals, home health or hospice agencies, ambulatory surgery centers, physician practices, skilled nursing facilities, and inpatient rehabilitation facilities.

Employees of CHSPSC, which provides management and consulting services to CHSI's affiliates, provide advice and recommendations on particular functions or areas of expertise.

The Corporate Compliance and Privacy Officer is Andi Bosshart. Ms. Bosshart is an employee of CHSPSC. The responsibilities of the Corporate Compliance and Privacy Officer include:

- Overseeing and monitoring the implementation of the Compliance Program.
- Reporting on a regular basis to the Executive Compliance Committee on the progress of implementation, and assisting the committee in establishing methods to improve CHS facility efficiency and quality of services, and to reduce the organization's vulnerability to fraud, abuse and waste.
- Periodically revising the program in light of changes in the needs of the organization, and in the law and policies and procedures of government and private payer health plans.
- Developing, coordinating, and participating in a multifaceted education and training program that focuses on the elements of the Compliance Program, meeting federal requirements, and seeks to ensure that all appropriate colleagues and management are knowledgeable of, and in compliance with, pertinent federal and state laws and regulations.
- Seeking to ensure independent contractors and agents who furnish medical and other services to the facilities are aware of the requirements of the Compliance Program.
- Coordinating personnel issues with appropriate managers to assure colleagues, medical staff and independent contractors have not been sanctioned or excluded from participation in any federal health care program.
- Assisting the organization's financial officers in coordinating internal review and monitoring activities, including periodic reviews of facilities.
- Independently investigating and acting on matters related to compliance, including the flexibility to design and coordinate internal investigations (e.g., responding to reports of problems or suspected violations) and any resulting corrective action with all facilities, departments, providers and sub-providers, agents and, if appropriate, independent contractors.
- Developing policies and programs that encourage the reporting of suspected fraud and other improprieties without fear of retaliation.
- Preparing and submitting all periodic reports required under the Compliance Program to the Executive Compliance Committee, the Board Audit and Compliance Committee, and the government under any Corporate Integrity Agreements or compliance reporting requirements for settlement agreements.

THE ROLE OF THE INDIVIDUAL

Every CHS colleague is required to comply with the Code of Conduct. Each individual is expected to perform his/her daily activities with the highest standards of ethics and compliance. Colleagues should notify their FCO, their Facility Privacy Officer ("FPO"), the Corporate Compliance and Privacy Officer or the Confidential Disclosure Program of any known or suspected violations of law, the Code of Conduct, or Compliance Policy. The only way we can address concerns and live up to our expectations for ethical conduct is if we learn about those concerns as soon as they arise.

Grievance Resolution

If an individual is concerned about a personnel action that does not involve any violation of law, the Code of Conduct, or Compliance Policy, he/she may file a grievance at the facility where he/she is employed. Your facility Human Resources Department can provide a grievance resolution form and assistance in preparing and presenting a grievance. Information provided or received as part of the grievance process is held in strict confidence. Refer to your Handbook or contact your Human Resources Department for more information.

CODE OF CONDUCT IN THE WORKPLACE

Harassment, Discrimination, Retaliation, and Violence

Everyone has a right to a work environment free of unlawful harassment, discrimination, and retaliation based on race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability, genetic information, citizenship, veteran status, military or uniformed services, or other legally protected characteristics or conduct. We will not tolerate any unlawful harassment of colleagues or applicants. The organization will take action to fairly and objectively address any complaints of unlawful harassment, discrimination, retaliation, or workplace violence. If you experience or witness such behavior, contact your facility Human Resources Department, the FCO, the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program.

Licensure and certification boards have legal standards that govern medical practitioners', physicians', nurses' and other hospital personnel duties and behavior. Accordingly, anyone who observes or that is otherwise made aware of disruptive behavior by a practitioner should document the behavior and report it to the facility Human Resources Department, the FCO, or a member of administrative management. "Disruptive conduct" includes conduct that poses a threat to patient care or exposes the hospital and/or Medical Staff to liability.

Workplace violence, such as robbery, assault, battery, vandalism, and other crimes will not be tolerated. Colleagues may not bring firearms, explosive devices, or other weapons or dangerous materials into any hospital, practice, agency, home health agency, physician clinic, ambulatory surgery center, office building or affiliated facility. Colleagues who witness any form of violence are required to report the conduct to the facility Security Officers, the Human Resources Director, the FCO, the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program.

Equal Opportunity

We value the talents and skill sets of each colleague. The organization is determined to provide an equal opportunity environment and to comply with all laws, regulations, and policies. It is the policy of each CHS affiliate to provide equal opportunity without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability, genetic information, citizenship, veteran status, military or uniformed services, or other legally protected characteristics.

Investments and Conflicts of Interest

Outside financial interests that might influence decisions or actions of colleagues in the performance of their duties for the organization are to be avoided. Potential conflicts of interest might include:

- A personal or family interest in an enterprise that has a business relationship with the organization or a facility.
- An investment in another business that competes with the organization or a facility.

Any financial interest owned or acquired (including by gift or inheritance) must be disclosed immediately to the Corporate Compliance and Privacy Officer. Divestiture of such interest may be required if the financial interest is deemed to be in conflict with the organization's best interests. This does not apply to minimal holdings of the stock or other securities of a corporation whose shares are publicly traded and which may also do business or compete with a facility or the organization.

Relationships with Vendors and Suppliers

When conducting business with vendors or suppliers including physicians, colleagues are expected to maintain impartial relationships with the organization's vendors and suppliers and should be motivated solely to acquire goods, purchase services, and make other transactions on terms most favorable to the organization. Care must be exercised to avoid even the appearance of favoritism on behalf of a vendor or supplier due to personal relationships. Colleagues or their families may not accept any gifts (except those of nominal value), special discounts or loans (other than from established banking or financial institutions), excessive entertainment, or substantial favors from any organization or individual that conducts or is seeking to conduct business with the organization. Reasonable judgment should be used in the determination of "excessive or substantial," and acceptance made only with the approval of a department director or higher level member of management.

Periodically, a vendor may sponsor seminars, training, product demonstrations, or other types of meetings. Vendor-sponsored training offered by a vendor participating in the group purchasing organization, HealthTrust Purchasing Group (HPG), including travel and lodging, may be paid by the vendor when the business value outweighs any recreational or entertainment value of the event. Appropriate approvals must be obtained in advance. Questions should be directed to the Corporate Compliance and Privacy Officer.

Colleagues or their families should not offer, give, solicit, or accept kickbacks, rebates, or anything of value to or from any representative of a vendor, supplier, customer, potential customer, patient, physician, financial institution, or similar entity. Cash gifts or tips or cash substitutes in any amount or from any source are strictly prohibited. Such practices are unethical and in many cases illegal.

Reference: Discounts and Waivers Policy, Policy on Purchasing Goods and Vendor Relationships (Discounts), Business Courtesies and Other Miscellaneous Financial Arrangements with Potential Referral Sources, and your employee handbook.

Professional Licenses, Certifications, and Credentials

Colleagues who are required to maintain professional licenses, certifications, or other credentials are personally responsible for maintaining these items in a current and up-to-date status while complying with all pertinent federal, state, local, or professional requirements governing their field of expertise. Proof of current professional licenses, certifications, or credentials must be supplied upon request. No colleague requiring a professional license, certification, or credential will be allowed to perform his or her job duties or contracted assignments until such time he/she meets this requirement. Falsification of certification, licensure, or credentials will lead to disciplinary action up to and including termination.

Substance Abuse and Controlled Substances

The use of intoxicants, substances causing impairment, or illegal drugs including prescription drugs prescribed for someone other than the colleague while on the job or on the premises is prohibited. Use of such substances off the job or off premises may also be the subject of disciplinary action by your employing facility. Your facility will require substance testing on pre-employment, for cause, and random bases. In addition, we have implemented other drug screening programs to detect and deter the inappropriate use of drugs in the workplace.

At times, colleagues may need to take prescription or over-the-counter drugs that could impair their job performance. It is important for such persons to notify their supervisor if their medication could adversely affect their job performance.

Use of Organizational Assets

The assets of the organization are to be used solely for the benefit of the organization. Each colleague is responsible for assuring that assets are used only for valid purposes. These assets include, but are not limited to, physical plants, equipment, computers, corporate funds, drugs, medical supplies, services, office supplies and facility business operations that have not been shared with the general public. These assets will not be used to provide personal gain for colleagues or others. Improper use or removal of the organization's assets is a violation of the Code of Conduct and possibly a violation of the law.

Our organization may not transfer any of our assets to other people except for fair market value consideration and in the ordinary course of business. Computer equipment, hard drives, and other electronic media devices must be disposed of through a CHSPSC IT Security approved vendor such as Arrow. Donation, sale or trade of such equipment by vendors other than Arrow must be approved by the CHSPSC Security Officer and the Corporate Compliance and Privacy Officer. Occasionally, some assets of the organization deemed no longer needed in the business may be sold to colleagues. Such sales must be properly approved, documented, and signed by appropriate supervisory personnel other than the colleague.

Health, Safety, and the Environment

We are committed to providing a safe and healthy workplace for all colleagues, customers, patients, and visitors. We are equally committed to minimizing any negative impact upon the environment. These commitments can be achieved through the awareness and cooperation of all colleagues.

Each colleague is responsible for abiding by safe operating procedures, guarding his/her own health along with his/her colleagues, utilizing pollution control systems, and following safe and sanitary procedures for the disposition of industrial and hazardous waste materials. Colleagues should report to a supervisor, department head, the Facility Compliance Officer, the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program any condition they perceive to be unsafe, unhealthy, or hazardous to the environment.

Inside Information and Securities Trading

Inside information, such as acquisition plans, financial and operating data (before it is publicly released), marketing plans, or other business material is nonpublic information. At times, colleagues may become aware of inside information, but the use of inside information for personal gain is strictly prohibited and possibly against the law. In addition, disclosing inside information to colleagues, relatives, or friends in an effort to influence their decision to buy, sell, or hold the parent company's or any other company's securities or stock options is strictly prohibited. Inside information should only be shared with people inside the organization whose jobs require the information. For more information, see the Insider Trading Policy in myPolicies.

Colleagues may not engage in any illegal or improper acts to acquire a competitor's trade secrets, customer lists, technical developments, or operations. In addition, a competitor's employees shall not be hired for the purpose of obtaining confidential or proprietary information about the competitor. Competitor's personnel, customers, or suppliers must not be urged or coerced to disclose confidential or proprietary information about the competitor, nor shall such information be sought from competitor's employees subsequently hired by the organization.

Government or Union Officials

Colleagues will not offer any government employee, union official, or their representatives any meals, entertainment, or gifts that would cause the donor or the recipient to be in violation of any law, regulation, or policy.

THE CODE OF CONDUCT AND OUR CUSTOMERS

Patients

Confidentiality of Patient Information

When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected and used to satisfy information needs including the ability to make decisions about a patient's care. We consider patient information highly confidential. Colleagues are expected to take care to protect the privacy of individually identifiable health information at all times. All of the facilities within the organization have specific policies describing patient confidentiality and release of information rules that conform to federal, state, and local laws governing the release or disclosure of health information. Each facility has a designated Facility Privacy Officer who conducts or assists with investigations of potential privacy breaches.

Colleagues must never disclose or release confidential patient information including pictures, texts, or recordings in a manner that violates the privacy rights of a patient. Policies on obtaining patient authorization for release of information and confidentiality, and consent to photography or cinematography must be strictly followed before creating or obtaining video, pictures or recordings of patients, patient information, or activities occurring in patient care areas. Patient information may only be discussed or released in accordance with our HIPAA policies in the myPolicies library, which may require the express written authorization of the patient. Colleagues should not access or use any patient information, including that of themselves, their family members or friends, or of subordinates or co-workers, unless it is necessary to perform his/her job.

Because of privacy laws, colleagues shall not post statements, stories, pictures, or recordings of patients or individually identifiable patient information on any social networking site including but not limited to Instagram, SnapChat, Linkedin, Pinterest, Facebook, Tumblr, Twitter or YouTube. The use of personal devices for capture and/or transmittal of patient recordings or pictures for use other than a specific patient care function are strictly prohibited.

Anyone who inappropriately accesses, obtains, uses, or discloses individually identifiable health information may be in violation of the Health Insurance Portability and Accountability Act ("HIPAA") Privacy or Security Rules and may face criminal and/or civil penalties of up to $250,000 and up to ten years imprisonment.

In some circumstances, a patient's written authorization for release of information is not required. For example, patient information can be requested from another healthcare institution or physician without the patient's authorization for treatment purposes. Some federal, state, and local agencies may require hospitals to release information without the patient's written authorization under such circumstances as a court order, a search warrant, a subpoena duces tecum, situations of suspected child abuse, various registries, and federal healthcare programs. When in doubt, contact the Health Information Management Director, the FPO, the Vice President of Health Information Management, or the Senior Vice President, Corporate Compliance and Privacy Officer.

Reference: Compliance with HIPAA Privacy Regulations, Definitions; HIPAA Policies and Procedures; Disclosure of PHI to Law Enforcement; Privacy Sanctions Policy; Notice of Privacy Practices

Emergency Medical Treatment

All hospitals must comply with the Emergency Medical Treatment and Active Labor Act ("EMTALA") when providing emergency medical care. All persons arriving on a hospital's property or in the emergency department and requesting a medical examination for an emergency medical condition will receive a medical screening examination to determine if such a condition exists. Colleagues should escort any person seeking this examination and/or treatment to the emergency department. If an emergency medical condition exists, the patient will be provided with medical treatment to stabilize the condition and/or an appropriate transfer to another facility. Medical screening or treatment will not be delayed to inquire about an individual's ability to pay including obtaining or verifying insurance information or advising the patient of his/her financial responsibility for payment of services rendered if he/she receives treatment.

Reference: EMTALA – Medical Screening/Stabilization

Patient Rights

Patients have a right to healthcare at the organization's facilities without regard to age, gender, sexual orientation, gender identity or expression, race, ethnicity, cultural, language, physical or mental disability, or religious background. Facilities shall not discriminate against patients whose care is paid for under the Medicare, Medicaid, or other governmental payer programs.

Upon admission, each patient, or when appropriate the patient's representative, will receive a written copy of the patients' rights and responsibilities. Patients' rights include but are not limited to the following concepts:

- Informed consent
- A safe environment
- Patient choice for providers of goods and services
- Privacy and confidentiality
- Accommodations for vision, speech, hearing, cognitive impairments or language translation services, free of charge
- Pain management
- Participation in care decisions, including the provision of advanced directives to providers
- Risks, benefits, and alternatives to treatments and procedures
- Outcomes of care and treatment
- Information about the bill for services
- Receipt of the Notice of Privacy Practices
- Ability to request an accounting of disclosures, a restriction of use or disclosure of protected health information, or an amendment to the medical record

All patients' rights also apply to persons who may have legal guardianship or responsibility for healthcare decisions on behalf of the patient.

Reference: Patient Rights and Responsibilities Policy; Patient Rights and Responsibilities Form 100-ADM-1901

Human Subject Research

All human subject research activities, regardless of whether the research is subject to U.S. federal regulations, will be guided by one of the following statements of ethical principles: (a) The World Medical Association's Declaration of Helsinki (as adopted in 1996 or 2000); (b) The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research of the U.S. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research; or (c) other appropriate international ethical standards recognized by U.S. federal departments and agencies that have adopted the U.S. Federal Policy for the Protection of Human Subjects, known as the Common Rule.

Reference: Human Subjects Research and Institutional Review Board Policy; and Federal-wide Assurance (FWA) for the Protection of Human Subjects; US Department of Health and Human Services (HHS), Office for Human Research Protections (OHRP).

Physicians

Financial Arrangements

The organization has established policies regarding the financial relationships, including ownership and compensation arrangements, between CHS affiliates and physicians and any other referral sources. All agreements for the payment or receipt of money, goods, services, or anything of value with physicians must be in writing and comply with the federal law and regulations commonly known as the Stark Law. Such financial relationships must also be reviewed to ensure compliance with the federal Anti-Kickback Statute. All facilities are prohibited from entering into side agreement(s) (written or verbal agreements that modify a formal written contract) with physicians. Before accepting physician agreements, they must be approved by both the appropriate Division President and the Corporate Legal Department. These approvals must be obtained even if the agreement complies with the Compliance policies. Issuance of payment to physicians under agreements must be supported by all required documentation, e.g., certification of hours of service or submission of executed agreement with request for payment.

Referrals

We will not pay for referrals nor will we accept payment for referrals made to other entities. All payments made to physicians and/or other entities must be pursuant to current fully executed written agreements and must be at fair market value for actual services performed. We will not consider the value or volume of referrals, or other business generated between parties in determining where to enter into an arrangement or in setting the compensation to be paid or received.

Reference: Business Courtesies and Other Miscellaneous Financial Arrangements with Potential Referral Sources

Third Party Payers

Coding and Billing

All individuals responsible for coding and billing for services will adhere to all official coding and billing guidelines, rules, regulations, statutes, and laws. Colleagues are prohibited from knowingly causing or permitting false or fraudulent claims. Furthermore, colleagues shall not engage in any intentional deception or misrepresentation intended to influence any entitlement or payment under any state or federal healthcare benefit program. Claims must only reflect the actual services ordered, documented, and performed. Coding of diagnoses and procedures will be in accordance with CMS recognized coding guidelines.

The organization will maintain a routine auditing and monitoring program to verify the accuracy and validity of coded data and claims regardless of the source of payment.

Reference: Coding Compliance Policy.

Cost Reports

Facilities receive reimbursement under government and certain non-government healthcare programs that require the filing of reports on the costs of operation. The organization will comply with all federal, state, and local laws, rules, and regulations relating to all cost reports. We will utilize acceptable practices to determine allowable costs and reimbursement for the costs of services provided to program beneficiaries. Questions regarding the completion and/or settlement of a cost report should be directed to the CHSPSC Revenue Management Department.

ACCREDITING BODIES AND REGULATORY COMPLIANCE

CHS affiliated facilities seek accreditation from various agencies and accrediting bodies; all standards required by those accrediting bodies must be followed. All colleagues should relate with accrediting agencies and bodies in a forthright manner. No action, either directly or indirectly, will be taken to mislead a surveyor or survey team.

Healthcare services may be provided only pursuant to federal, state, and local laws, rules, and regulations. These laws and regulations may include, but are not limited to, certificates of need, licenses, permits, certifications, access to treatment, consent to treatment, medical record maintenance, release of information and confidentiality, patient rights, advance directives, medical staff membership and privileges, organ donation, and Medicare and Medicaid regulations.

Facilities and colleagues must comply with all applicable federal, state, and local laws, rules, and regulations. Any colleague who witnesses or suspects any violations of any law or regulation must immediately report said violation or suspected violation to a supervisor, the Facility Compliance officer, the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program.

During a survey or government inspection, colleagues must not destroy, conceal, or alter any documents. Furthermore, colleagues must not lie or make misleading comments to a surveyor or government inspector. Colleagues must not obstruct others from providing accurate information to the surveyor or government inspector, nor mislead nor delay the communication of information or provision of records relating to a surveyor or inspector's requests.

Facilities must notify their assigned Corporate Survey Management Director, preferably by email, in the event of a visit or inspection by a survey team.

Upon presentation of a search warrant, subpoena, or other criminal or administrative legal process by a law enforcement official (e.g., FBI, State Bureau of Investigation, US Department of Justice, HHS Office of the Inspector General, etc.), notify the Executive Vice President, General Counsel at 615-465-7349.

Reference: Regulatory Survey Notification Process Policy.

FINANCIAL, BUSINESS AND MEDICAL INFORMATION, AND INFORMATION SYSTEMS

Financial Reporting and Records

As a public organization, our integrity and reputation depend upon the accuracy and completeness of our financial statements. All accounts and financial records must be maintained strictly in accordance with the CHSPSC Financial Policies and Procedures, as amended from time to time. Colleagues must always keep in mind that each bookkeeping and financial entry will ultimately be incorporated into our consolidated financial statements. Our consolidated financial statements are certified by our officers as being true and correct and not misleading and are presented to the public and the federal government in accordance with generally accepted accounting principles and all Securities and Exchange Commission

rules and regulations. All personnel who make bookkeeping and financial entries, prepare financial reports and statements, and disperse assets (especially cash) have special ethical obligations as you perform your duties. When you sign your annual acknowledgement of the CHS Code of Conduct, you are certifying adherence with the following principles:

To the best of my knowledge and ability:

1. I act with honesty and integrity, and I avoid actual or apparent conflicts of interest.

2. I provide constituents with information that is accurate, complete, objective, relevant, timely and understandable.

3. I comply with the rules and regulations of federal, state, provincial and local governments, and other appropriate private and public regulatory agencies.

4. I act in good faith, responsibly, with due care, competence and diligence, without misrepresenting material facts or allowing my independent judgment to be subordinated.

5. I respect the confidentiality of proprietary financial and accounting information acquired in the course of my work except when authorized or otherwise legally obligated to disclose.

6. I share knowledge and maintain skills important and relevant to my constituents' needs.

7. I proactively promote ethical behavior in the preparation and maintenance of the organization's books and accounts and financial records.

8. I achieve responsible use of and control over all assets and resources employed or entrusted to me.

Proprietary Information

Many laws and regulations govern publicly traded companies associated with healthcare. Proprietary information acquired during the course of employment or contract with the organization is not to be discussed with anyone outside the organization and only discussed within the organization on a need to know basis. Except with proper written authorization by the appropriate personnel of your facility or where required by law, colleagues may not use, or disclose to others, any trade secrets or confidential technology, proprietary information, customer lists, or any other proprietary knowledge gained as a result of his/her employment. Upon separation of employment from your facility, colleagues are prohibited from taking, retaining, copying, or directing any other person to take, retain or copy any proprietary or confidential information belonging to any CHS-affiliated entity without prior written permission, regardless of the form the proprietary or confidential information takes: papers, data, client lists, books, records, files, or any other form.

Retention, and Disposal of Documents and Records

Legal and regulatory practice requires the retention of certain records for various periods of time, particularly in the following areas: health information, patient accounting, tax, personnel, health and safety, environment, contract, and corporate office. In addition, no records or files may be destroyed when there is pending or imminent litigation, government investigation, or an audit; relevant records must not be destroyed until the matter is concluded. Destruction of records and/or files to avoid disclosure in a legal proceeding may constitute a criminal offense. Colleagues should consult the organization's various record retention policies before any records and/or files are destroyed. All medical and business records must be retained in accordance with the laws in the state in which the facility is located.

Reference: Document Retention Policy; Document Retention Schedule

Electronic Media, Records, and Documents

Many different types of media are used by us to create, store, maintain, and communicate information. Electronic media such as telephones, other communications systems, e-mail, Internet access, and voice mail are provided to colleagues for business use. Since these electronic media are the property of the organization, colleagues should assume these communications are not private and may be monitored. Unless authorized by the appropriate personnel at your facility or required or authorized by law, any confidential patient information, non-public proprietary business information (trade secrets, intellectual property, company financial data, plans, strategies, research, analyses), or other legally confidential information must not be conveyed by any media sources unless appropriate security measures are in place. Unless authorized, never send or forward such information via email unless approval has been granted by the CHSPSC Security Officer. Colleagues must not use the organization's electronic media to distribute or transmit any unlawful or obscene materials.

E-mail and internet access shall be used only by authorized users in the performance of their assigned job duties. Responsible, incidental personal use is acceptable, provided that it does not (a) interfere with the colleague's (or another colleague's) performance of job duties, (b) use the resources in a manner that limits or impedes their use of access for legitimate business purposes, or (c) violate this or any other organization or facility policy.

Reference: Electronic Communications Policy

POLITICAL ACTIVITIES AND CONTRIBUTIONS

We support colleague participation in civic affairs and political activities. However, these affairs and activities must not create a conflict of interest with the organization nor reduce the individual's work performance. Colleagues must recognize that involvement and participation in political activities is on an individual basis, on their own time, and at their own expense. When colleagues speak on public issues, they must make it clear to the audience that their comments are their own personal viewpoints.

No colleague is authorized to contribute, directly or indirectly, any assets of any CHS affiliate including cash or the work time of any colleague, to any political office holder, party or campaign of any candidate for federal, state, or local office without following the appropriate approval process set forth in the CHSPSC Financial Policies and Procedures.

COMMUNITY SERVICE

We encourage colleagues to participate in community service projects.

THE COMPLIANCE PROGRAM

Program Structure

The Compliance Program has been developed and adopted in furtherance of the understanding and commitment of the management of the organization that all activities of the organization and the organization's colleagues and those acting on their behalf shall be conducted in a legal and ethical manner. Although aspects of the Compliance Program focus on various legal areas, the primary focus of the Compliance Program is to ensure that internal policies and controls, training and education, and auditing and monitoring are in place to help prevent, detect, and deter fraud, abuse, and waste in government health care programs.

We are committed to the development and implementation of an effective and voluntary compliance program that meets or exceeds the requirements and expectations of government regulators and industry norms and standards.

We are committed to creating and maintaining a culture that promotes prevention, detection, and resolution of instances of conduct that do not conform to federal, state, or local laws, rules, and regulations; federal health care benefit program requirements; or the Code of Conduct.

The structure of the Compliance Program is guided and approved by the Executive Compliance Committee. There is also a Corporate Compliance and Privacy Officer, a Corporate Compliance Work Group, Facility Compliance Committees, FPOs, and FCOs. Additional elements of the ongoing Compliance Program include:

- Maintenance, publication, and distribution of the Code of Conduct and Compliance policies and procedures.
- Design and implementation of standard auditing and monitoring functions.
- Use of standard audit results to determine targets for improvement and education.
- Preparation and implementation of system-wide policies, procedures, and tools to comply with federal, state and local laws, statutes, regulations, and any Corporate Integrity Agreement requirements (e.g., the False Claims Act, Stark, Anti-Kickback Statute, HIPAA, etc.).
- Performance of new hospital acquisition compliance assessments.
- Continuation of the compliance training and education program.
- Enhancement of the Confidential Disclosure Program.
- Investigation of reports received through the Confidential Disclosure Program.
- Assessment of CHS affiliates and of the Compliance Program.
- Periodic reports to the CHS Board of Directors Audit and Compliance Committee (Board Compliance Committee).

The Senior Vice President, Corporate Compliance and Privacy Officer for CHS is Ms. Andi Bosshart.

Reporting Questions or Concerns

Questions or concerns about potential compliance or privacy violations may be addressed to any of the following:

- Your supervisor or department head
- Any supervisor or department head
- Your Facility Compliance Officer
- Your Facility Privacy Officer
- The Corporate Compliance and Privacy Officer
- The Confidential Disclosure Program Hotline at 1-800-495-9510

If a colleague feels a question or concern is not resolved appropriately, the colleague should report the matter immediately to the Confidential Disclosure Program hotline or to the Corporate Compliance and Privacy Officer.

Reporting Violations

Violations and unresolved suspected violations of any laws, rules, regulations, and/or the Code of Conduct must be reported to the Corporate Compliance and Privacy Officer or through the Confidential Disclosure Program.

Failure to report a known or suspected violation of the law, Code of Conduct, or any Compliance Policy could subject an individual to disciplinary action. However, intentionally false or misleading reports made with the intent to damage another person's reputation violate the Code of Conduct.

Federal and State False Claims Act Laws

The federal Deficit Reduction Act requires that certain entities, such as CHS, provide affiliated employees, contractors, and agents with information related to the federal False Claims Act (FCA) law. This law provides that civil penalties may be imposed against any person or entity that knowingly presents or causes to be presented a false or fraudulent claim to a federal healthcare program for payment. In addition to civil monetary penalties, violators of the federal False Claims Act may be subject to treble damages for each false claim submitted to federal healthcare programs. The federal False Claims Act includes whistleblower protection provisions that protect any individual who is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against for filing an action under the federal False Claims Act.

Many states have enacted False Claims Act statutes that contain provisions that are similar to the federal statute, including whistleblower provisions.

Reference: Preventing, Detecting and Reporting Fraud, Waste and Abuse. State DRA Guidelines are available as a subset to this policy

Confidential Disclosure Program

We have established a Confidential Disclosure Program for all colleagues and other individuals of all subsidiaries and affiliated facilities to report known or suspected conduct or activities by any person engaged in the performance of duties for the organization that violates the Code of Conduct, any Compliance Policy, HIPAA Privacy Policy, or any federal, state, or local laws, rules, and regulations. This program may also be used for individuals who are uncertain whether an action violates the Code and would like to communicate with the organization on a confidential basis.

An individual reporting known or suspected improper conduct is not required to identify himself/herself. Anonymous calls and communications will be investigated and acted upon in the same manner as calls where the caller or writer reveals his/her identity. No effort will be made to determine the identity of an individual making an anonymous report unless the individual admits to engaging in improper conduct. Individuals are encouraged to describe the conduct or incident in sufficient detail to enable the organization to investigate the matter.

CHS policy, the Deficit Reduction Act, the Fraud Enforcement Recovery Act, the FCA, and other state and federal laws provide protection from retribution or retaliation against any person for reporting actual or suspected violations of the Code, law, or policy. Any supervisor who attempts to divert, discourage, or retaliate against a colleague for reporting a compliance concern will be subject to severe discipline, up to and including discharge.

Confidential Disclosure Program Hotline: 1-800-495-9510

Address: **Corporate Compliance and Privacy Officer**
Community Health Systems
4000 Meridian Boulevard
Franklin, Tennessee 37067

Investigation of Known or Suspected Violations

Prompt, appropriate, confidential investigations into all Program calls, letters, and other forms of communication, both direct and indirect, including reports of site visits conducted by Compliance Work Group members, their staff, or consultants will be made. The CHSPSC Compliance and Privacy Officer or her designee will coordinate any findings from the investigations and recommend corrective and/or disciplinary actions.

All colleagues are required to cooperate with the investigation efforts.

Corrective Action

Once a reported violation is substantiated through the investigation process, corrective action will be initiated. When appropriate, the affiliated facility will return any overpayment amounts, notifying the correct governmental agency of the overpayment situation. Corrective action will be taken promptly to prevent similar occurrences at any CHS affiliated facility.

Discipline

Violations of the Code of Conduct or the organization's compliance policies will be subject to the organization's normal disciplinary procedures. Disciplinary action that may be taken by your facility includes, but is not limited to, informal counseling, verbal and/or written warnings, investigative or disciplinary suspension, termination, probation, demotion, and/or incentive compensation withholding. The type of disciplinary action that is applicable is decided on the facts of each situation.

Acknowledgement

Under applicable laws such as the Affordable Care Act, the Code of Conduct is a mandatory policy. All colleagues will sign a form indicating they have reviewed a copy of the Code and agree to abide by the Code of Conduct, all laws and regulations. In addition, all colleagues will reaffirm these actions on an annual basis.

Compliance with the Code of Conduct and other policies will be considered by affiliated entities in employee evaluations and in decisions regarding promotion and compensation for all their employees.

Nothing in this Code is intended to create enforceable employee contract rights.

Revision adopted by the Board of Directors of Community Health Systems, Inc. on September 13, 2016 (supersedes the revision adopted September 2, 2015).

ACKNOWLEDGEMENT

I acknowledge that I have received, read and understand
the Community Health Systems ("CHS") Code of Conduct.

I agree to abide by the compliance policies summarized in the Code of Conduct
and all federal, state, and local laws, rules and regulations
for the duration of my association with CHS.

_____

Signature

_____

Printed Name

_____

Date

_____

Facility

CHS-CODE-ACK 09-16

4852-2554-1686, v. 3

Community
Health Systems

HIPAA

Protecting Patient Privacy

What is HIPAA?

- A set of Federal regulations known as the Health Insurance Portability and Accountability Act of 1996
- HIPAA provides guidance for how patient information can be used, stored, disclosed and maintained by health care providers and members of their workforce.
- HIPAA also provides patients with certain rights related to controlling the use and disclosure of the patient's protected health information (PHI) as well as the patient's right to access their own PHI.

What is Protected Health Information?

- Patient information in any form: written, verbal, or electronic (including email and text)
- PHI Includes:
  - Any information that can be used to identify the patient. For example: name, address, social security number, medical record number, telephone number, patient account number
  - Anything about a patient's medical condition and treatment – past, present, or future
  - Billing and payment records

Compliance is the Expectation

When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected and used to satisfy information needs including the ability to make decisions about a patient's care. We consider patient information highly confidential. Colleagues are expected to take care to protect the privacy of individually identifiable health information at all times. All of the facilities within the organization have specific policies describing patient confidentiality and release of information rules that conform to federal, state, and local laws governing the release or disclosure of health information. Each facility has a designated Facility Privacy Officer who conducts or assists with investigations of potential privacy breaches.

Colleagues must never disclose or release confidential patient information including pictures, texts, or recordings in a manner that violates the privacy rights of a patient. Policies on obtaining patient authorization for release of information and confidentiality, and consent to photography or cinematography must be strictly followed before creating or obtaining video, pictures or recordings of patients, patient information, or activities occurring in patient care areas. Patient information may only be discussed or released in accordance with our HIPAA policies in the myPolicies library, which may require the express written authorization of the patient. Colleagues should not access or use any patient information, including that of themselves, their family members or friends, or of subordinates or coworkers, unless it is necessary to perform his/her job.
[CHS Code of Conduct, pg 10]

The Notice of Privacy Practices

The Notice of Privacy Practices (sometimes referred to as the NPP) is:

- Is an explanation to our patients of how their PHI may be used and disclosed
- The start of a dialogue with our patients regarding the purpose of the uses of their information
- An explanation of the patient's rights as defined by the HIPAA Privacy Regulations
- The Notice of Privacy Practices is:
  - Available in a paper copy
  - On the facility web site
  - Posted in the facility
- The NPP must be posted in the area where patients are registered. This generally includes:
  - Hospital Inpatient/Outpatient Registration
  - OB Department
  - Emergency Department Registration
  - Physician office room

Facility Directory Disclosures

- The patient must be given the opportunity to opt-out of the directory (census of patients in the facility).
- If the patient has opted out of the patient directory, **no information may be disclosed.**
- If the patient has not opted out of the directory, the following information may be included in the facility directory and given to those individuals who ask about the patient by name:
  - Name
  - Location within the facility
  - Condition of the patient in general terms (e.g., good, critical, serious)
  - Only members of the clergy may have access to the religious affiliation of the patient, if provided [Note: Members of the clergy are not required to ask for the patient by name to obtain any of the above information. This exception applies only to the clergy].

Before You Access Patient Information, Ask Yourself

- Is the patient information I am about to access necessary for me to complete my job?
- Am I accessing only the minimum necessary to complete my job, no more and no less?
- Am I accessing, using, or disclosing this information for treatment, payment, or health care operations reasons?
- If I am accessing, using, or disclosing this information, should I have a signed authorization from the patient?

When is it Appropriate to Disclose PHI?

- Share only the minimum amount of PHI necessary to fulfill the job responsibility (minimum necessary)
- Share PHI only with those with a clinical or business need to know
- Share only the amount of PHI requested. The entire medical record may not be needed.

Examples of Minimum Necessary

- A billing clerk may need to know what laboratory test was done, but not the result
- An admissions clerk does not need to have access to the full medical record in order to carry out his/her job
- A patient transporter typically does not need to access the full medical record to do his/her job

Snooping and Casual Disregard…our Greatest Risk

- Accessing the medical records of family members, friends, ex-spouses, neighbors, celebrities, etc.
- Failure to verify the authority of the individual receiving the PHI
- Inappropriate use of technology such as camera phones, texting, and social networking sites
- Volunteers sharing with friends and family information about patients

What is the Difference Between Use and Disclosure of PHI?

- USE is sharing PHI ***within*** the facility
- DISCLOSURE is sharing PHI ***outside*** of the facility

What is a Breach

- Breach means the unauthorized acquisition, access, use, or disclosure of PHI maintained by or on behalf of a person.
- A breach does not include any unintentional acquisition, access, use or disclosure made in good faith and done within the course and scope of your job; and, provided such information is not further acquired, accessed, used or disclosed.
- In other words, just looking up someone's PHI, even if you don't print it or tell someone else, is a breach – yes, and you may be subject to disciplinary action up to and including termination.

Examples of a Breach

- A biller accesses registration information to obtain her ex-husband's new cell phone number.
- A Volunteer learns that a close friend was hospitalized over the weekend. After leaving the hospital that day, she calls several friends to organize meals for her friend and explains to her friends the hospitalization.
- A workforce member takes work home that contains PHI which is not protected as required by HIPAA and it is lost or stolen.

Other Forms of a Breach

- Texting information about a patient, even his/her presence at the facility, to someone who does not have a business need to know
- Taking cell phone pictures or video of a patient, patient body part, a patient's x-ray film, medical record, family members, etc.
- Posting information on Facebook or other social media site about a patient – even when you don't give a patient's name

Photographs and Recordings

- Photographs, video recording, audio recording, or other imaging of patients, visitors, and workforce members are **generally prohibited**!
- **Contact** the Facility Privacy Officer for guidance on where photography and recordings may be permitted.
- Authorized devices used for these purposes should be secure at all times.



What Happens When a Breach is Suspected?

- The incident must be immediately reported to the Facility Privacy Officer (FPO);
- The FPO will determine whether the loss of the information meets the definition of a Data Breach;
- The FPO will perform a risk assessment of the incident, including analysis of several factors, to determine the risk of compromise to the information

What Happens When a Breach is Confirmed?

- In some instances, the patients must be notified of the breach of their information;
- The federal Department of Health and Human Services must be notified of the incident;
- Notice may have to be posted in the local media;
- The facility/provider may be fined;
- The individual responsible may face disciplinary actions, civil or criminal fines and/or jail time.

Incidental Use or Disclosure of PHI

- Customary and essential communications and practices used to ensure patients receive prompt and effective healthcare which may occasionally result in another individual overhearing or glimpsing protected health information, are not breaches.

Examples of Incidental Uses & Disclosures

- Discussions among providers during teaching rounds
- A patient overhearing a physician talking with another patient while in an ER treatment room with the curtain drawn closed
- Calling out a patient's name in the waiting room
- Sign in sheets in hospitals and clinics containing the minimum information necessary

Protecting Patient Privacy

DO:

- Close curtains and speak softly when discussing treatments in semi-private rooms
- Log off of the computer when not attended
- Dispose of patient information (patient labels, documents, prescription bottles and IV bags or lab slides with patient information on them) in accordance with hospital policy and procedure
- Clear patient information off of your desk and place in a secure location when not in use
- Verify fax numbers and addresses before sending PHI

Protecting Patient Privacy

DON'T:

- Discuss a patient in public areas such as an elevator, hallway, cafeteria or outside the facility or office
- Share your computer username, ID, or password
- Look at information about a patient unless you need it to do your job
- Take information about patients (including nursing report notes) home
- Discuss patient information in front of visitors without the explicit, documented authorization from the patient
- Post any patient related information in church bulletins, Facebook, MySpace, or any other social networking websites
- Bring friends or family into areas of the facility, clinic, or agency where they can see or hear patients receiving care or where they might have access to PHI

Areas of Concern

- Friends/family/self – when you are seeking information on your family, friends or yourself, you are not acting as a workforce member and you must access PHI using the procedures required for non-employees. This means you need a written authorization for release of information which may be obtained in the HIM or medical records department
- You are ***not*** permitted to access your own medical records without a written authorization for release of information

Areas of Concern

- When an workforce member of the hospital, clinic, or healthcare entity is a patient, the healthcare entity does not generally have the right to access the workforce member's PHI in the role of the employer.
- For example, if workforce member comes into the ED – his/her supervisor or co-workers should not be accessing his/her ED information.
- This can be a challenging area: call the Facility Privacy Officer if questions arise.

No Excuses

- Good intentions such as "I needed to let his mother know he was in the hospital," or "she is my best friend and she wouldn't mind me looking," do not count.
- Just plain nosiness is also no excuse.

Reporting Suspected Violations of our Privacy Policies

Suspected HIPAA violations should be reported to:

- Your Supervisor
- The Facility Privacy Officer
- The Corporate Compliance and Privacy Officer

The Confidential Disclosure Program Hotline may also be used by calling 1-800-495-9510

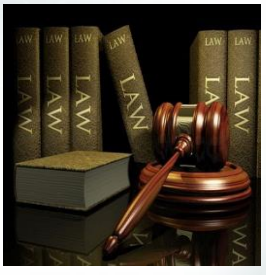
Non-retaliation

Our policy and state and federal laws provide protection from retribution or retaliation against any person for reporting actual or suspected violations

It is your duty and responsibility to report inappropriate use, access or disclosure of PHI to the Facility Privacy Officer, the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program Hotline

What Can Happen if I Violate Policy or Break the Law?

- Under recent changes in the law, state and federal authorities may now hold workforce members individually responsible for their actions
- Fines ranging from $50,000 per violation to as much as $250,000
- Criminal prosecution and up to 10 years in jail may occur depending on the type of violation
- Civil suits by state Attorneys General against the facility
- Violation of policy will result in appropriate disciplinary action up to and including termination



Recap

- The facility is committed to and serious about patient privacy
- All complaints regarding patient privacy will be taken seriously
- The facility will investigate all privacy complaints
- Workforce members who violate the HIPAA Privacy Policies or any privacy procedures will be subject to disciplinary action which could include verbal or written warnings, suspension from duties, or termination from employment or volunteer program participation
- Retaliation against any person for reporting actual or suspected violations will not be tolerated

Remember….

It could be ***your*** health information about which someone is talking.

General Compliance Training

2016-2017

1

Objectives

This module has been created to provide you with an understanding about the fundamentals of the Compliance Program and its integration into the culture of Community Health Systems Professional Services Corporation (CHSPSC). After completion of this module you will:

- See the value each of our colleagues has in helping to ensure the success of the Compliance Program;
- Understand your role in the Compliance Program;
- Know CHSPSC is committed to a high standard for ethical and legal behavior;
- Possess the information needed to report concerns through the appropriate processes; and
- Know where to locate Compliance policies and procedures and other departmental policies in the Policy Library.

2

Why do we need a Compliance Program?

- To create, cultivate, and maintain a culture of doing the right things right.
- To prevent improper or criminal conduct.
- To detect potential risk areas and processes; work to correct and mitigate any errors identified.
- To avoid penalties or punishment by correcting overpayments or other errors.

3

Introduction to the CHSPSC Compliance Program

- CHSPSC developed and implemented a comprehensive Compliance Program in 1997 and is based upon the elements outlined in the *Federal Sentencing Guidelines*. Furthermore, *"The OIG believes that every effective compliance program must begin with a formal commitment by the governing body to include all of the applicable elements…"*
- The creation and adoption of the Compliance Program by CHSPSC is evidence of management's continued commitment to conduct business activities in a manner exemplifying a high standard of legal and ethical behavior while empowering colleagues to uphold the same standard.

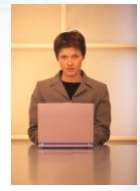
4

Corporate Integrity Agreement

- CHS has entered into a Corporate Integrity Agreement (CIA) with the Office of Inspector General (OIG) for a period of 5 years. The CIA requires our organization to have a compliance program meeting the seven elements of a Compliance Program identified in the U.S. Federal Sentencing Guidelines as well as:
  - Specific training for certain staff involved in Billing and Reimbursement, Clinical Documentation and Decision-Making, Case Management, and Arrangements (contracts at Laredo Medical Center);
  - Certain policies and procedures;
  - Defined, implemented and audited processes meeting the criteria of the CIA; and
  - Routine reporting requirements demonstrating our adherence to CIA obligations.

5

Elements of the CHSPSC Compliance Program



- Written Policies and Procedures
- The Code of Conduct
- Corporate Compliance Officer and Compliance Committees
  - Facility Compliance Officers
  - Facility Privacy Officers
- Training & Education
- Exclusion Screening
- Auditing & Monitoring
- Confidential Disclosure Program & Hotline

6

myPolicies

- As noted throughout the Code of Conduct, CHSPSC has a robust compilation of policies and procedures that address most functional areas.
- All policies are available through the Policy Library for all staff and serve to provide guidance on appropriate behavior and task performance.
- The Policy Library is located on the CHSPSC intranet page on the navigation bar by clicking "myPolicies".

7

What is the Code of Conduct?

- The Code (the "Code") is the cornerstone of the CHSPSC Compliance Program and reflects our commitment of high standards of business ethics and compliance and supports our culture of acting with integrity even if no one is watching.
- The Code reinforces the leadership's ability to lead by example with integrity and resolve.
- The Code is a collection of policy statements. Most sections of the Code of Conduct refer to more detailed policies covered in various operational areas.

8

"CHSPSC is committed to operating with the highest standards of integrity and behavior."

Wayne T. Smith, Chairman and CEO

9

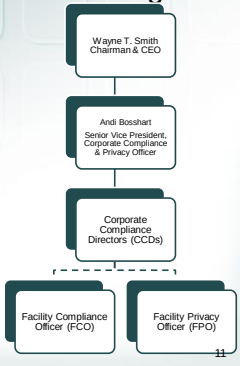
Management's Role in Compliance

Though all CHSPSC colleagues are required to follow the Code of Conduct, all managers, directors, supervisors, board members, and corporate staff are expected to set the example by conducting their business affairs consistent with the highest ethical and legal standards.

10

Compliance Structure & Oversight

- Ms. Andi Bosshart is the Senior Vice President, Corporate Compliance & Privacy Officer. She reports to the Chairman and CEO of the CHSPSC Board of Directors.
- Each Division has two or more dedicated Corporate Compliance Directors.
- Each facility has a Facility Compliance Officer and a Facility Privacy Officer.



11

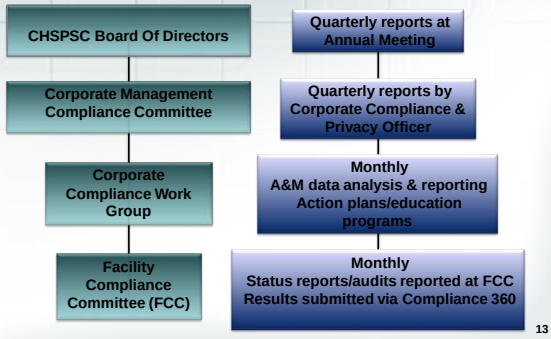
Senior Vice President Corporate Compliance & Privacy Officer

- Develops and implements policies, procedures, and practices designed to ensure compliance with the requirements set forth in the Compliance Program and with the requirements of federal healthcare programs.
- Revises the Compliance Program periodically in light of changes in the needs of the organization, federal regulations, or for the purpose of increasing effectiveness of the program.
- Reports on a routine basis the activities of the Compliance Program to the CHSPSC Management Compliance Committee and to the CHSPSC Board of Directors.

Andi Bosshart, SVP Corporate Compliance & Privacy Officer

12

Compliance Reporting



13

Corporate Management Compliance Committee

- Consists of several individuals from senior leadership and meets quarterly to discuss reports provided from the Senior Vice President Corporate Compliance & Privacy Officer.
- Tasked to demonstrate the company's commitment to ethical business conduct and compliance with the letter and spirit of the law in all aspects of the company's operations.
- Facilitates the creation of an environment where employees feel safe to report when they see an issue, and
- Seeks methods to engage employees in a culture where employees are encouraged and expected to identify areas for compliance.

14

Corporate Compliance Work Group ("CWG")

- Comprises a team of departmental subject matter experts which serve as resources for the Compliance Program.
- Suggests policies and tools for furtherance of compliance initiatives.
- Reviews auditing and monitoring activities to identify areas of risk, educational opportunities for key operating areas, and strengthens processes to conform to company policy, or federal or state regulation.
- Evaluates the Compliance Program with a view to future development and improvement.

15

The Facility Compliance Committee ("FCC")

- Requires attendance by core membership consisting of members from the leadership team and various department directors along with the Facility Compliance Officer, who serves as the Chair, and Facility Privacy Officer.
- Conducts training and education programs.
- Communicates "downstream" and "upstream".
- Reports auditing and monitoring and certifies results.
- Develops and implements action plans for issues identified during auditing and monitoring activities.
- Conducts additional activities as specifically designated by the Senior Vice President Corporate Compliance & Privacy Officer or Corporate Compliance Directors such as investigations.

16

Corporate Compliance Department

- CHSPSC management recognizes the Corporate Compliance Department as a conduit for communicating requirements of the Compliance Program for the organization and values the department's contributions to the overall success of the program.
- The Corporate Compliance Department, under the direction of the Senior Vice President Compliance & Privacy Officer, administers programs and provides resources to CHS affiliated entities to create and maintain an organizational culture that promotes prevention, detection, and resolution of healthcare fraud, waste, and abuse.
- The Corporate Compliance Department has created an intranet web page containing useful resources for Facility Compliance and Facility Privacy Officers and is accessible to all employees.

17

Training & Education

- Compliance training and education, in the words of the CHSPSC Compliance Manual, "are significant and important elements of the Compliance Program". CHSPSC offers many additional training opportunities to a wide variety of staff, contractors, and physicians throughout the year.
- An array of training and education programs are offered through the Advanced Learning Center. Required training includes:
  - General Compliance Training,
  - Job-Specific Compliance Training,
  - HIPAA Privacy and Security Training, and
  - Identity Theft.

18

General Compliance Training

- CHSPSC elected to provide general compliance training via PowerPoint presentation and computer-based training. Computer-based training is also used for the purpose of retraining all existing employees, physicians with medical staff privileges at any CHSPSC affiliate, and all contractors and agents of CHSPSC with direct responsibility for the delivery, billing, or coding of healthcare services on an annual basis.
- The Facility Compliance Officer also presents general compliance training at new hire orientations.
- General compliance training consists of:
  - the Code of Conduct;
  - a General Compliance PowerPoint presentation; and
  - a strong message from the CHSPSC Chairman and CEO outlining the importance of compliance in the company's day-to-day activities.

19

Job-Specific Compliance Training

- CHSPSC also chose computer-based interactive training software to deploy job-specific compliance training.
- Job-specific compliance training lessons are required for certain job types.
- The Advanced Learning Center ("ALC") enables CHSPSC to "enroll" intended audiences into a database for job-specific training modules. Since we tailored the specific training to be job specific, we have multiple training curricula targeted to compliance with job requirements for each area addressed for both new hires/ contractors (within 30 days of start date) and thereafter on an annual basis.

20

HIPAA Privacy & Security Training

- HIPAA Privacy & Security Training is presented by the Facility Privacy Officer during new hire orientation but also required for completion by our workforce using computer-based training within 30 days of start date or hire date.
- HIPAA Privacy & Security computer-based training is also required for purposes of retraining the workforce on an annual basis.

Compliance...
HIPAA Compliance
It's the Law!

21

Identity Theft

Identity Theft training was developed by CHSPSC pursuant to the Federal Trade Commission (FTC) Red Flag Rules to raise awareness of the potential for identity theft and the associated "red flags" which may be recognized to help deter the theft of medical, personal, or financial information.

- This training is required for completion within 30 days of hire date or start date using computer-based training.
- Identity Theft Training is also required to be completed annually.

22

Exclusion Screening

- An ineligible person is any individual or entity who:
  i. is currently excluded, suspended, debarred or otherwise ineligible to participate in the federal health care programs; or
  ii. has been convicted of a criminal offense related to the provision of health care items or services and has not been reinstated in the federal health care programs after a period of exclusion, suspension, debarment, or ineligibility.
  iii. Anyone who requires a current professional license by a state, and whose license is expired, suspended, revoked, lapsed, etc., is not eligible for hire, contract, or privileging.
- The company will not employ, retain, or otherwise do business with any Ineligible Person; this standard applies to all employees, contractors, medical staff, and vendors.

23

Exclusion Screening (continued)

- State and Federal Exclusion Databases are checked every month
  - Office of Inspector General (OIG -LEIE)
  - General Services Administration (GSA-EPLS)
  - SAM – System for Award Management
  - OFAC – Office of Foreign Assets Control/Specially Designated Nationals
  - Individual State Exclusion Databases
- If you receive a notice from any agency you **must** notify your department leader **immediately.**

24

Auditing and Monitoring

- Auditing and Monitoring is routinely performed in an effort to prevent, detect and mitigate inappropriate conduct or activities.
- Auditing and Monitoring activities are designed to assess the effectiveness of our compliance program.
- Auditing and Monitoring topics include, but are not limited to a routine coding assessment at each CHSPSC affiliate, various claims (patient bill) audits, physician transaction and payment reviews, privacy and security audits, various quality of patient care audits, and a check to ensure all employees and medical staff are eligible to provide services to our patients.

25

Coding & Billing

- CHSPSC has developed a comprehensive coding audit program to monitor the accuracy of inpatient and outpatient coding for each CHSPSC facility. The basic protocol for the review is as follows:
  - Each quarter, for each hospital, a targeted list of certain MS-DRG-based discharges shall be reviewed on a pre-billing basis;
  - For any billing errors or inaccuracies found, the coding personnel at that hospital shall receive training regarding the errors or inaccuracies;
  - Facilities are required to rebill all accounts with inaccuracies identified during the audit process; and
  - Affiliates, including hospitals, physician practices, and free-standing ambulatory surgery centers, are also subjected to routine outpatient coding and documentation assessments.

26

Non-Retaliation and No Retribution for Reporting

- Any reports of suspected misconduct may be provided anonymously through the Confidential Disclosure Program Hotline.
- Any supervisor or other colleague shall not prevent, or attempt to prevent another from using the Compliance Disclosure Program (hotline), Compliance Post Office Box, or other method to report suspected misconduct.
- If any supervisor or other colleague attempts to prevent another person from reporting suspected misconduct or otherwise retaliates against anyone for reporting suspected misconduct, he or she is subject to disciplinary action up to, and including, termination.

27

Stark Law

- Stark prohibits physicians from referring Medicare or Medicaid patients for certain services known as designated health services to any health care entity where the physician has a financial relationship, unless a legal exception applies.
- A physician or healthcare organization does not have to intend to violate Stark; even a technical violation is considered a violation.
- A Stark violation may trigger False Claims Act liability and significant civil monetary penalties and fines may be assessed for violations.

28

Anti-Kickback Statute

- The Anti-Kickback Statute (AKS) prohibits the offer, payment, solicitation, or receipt of anything of value to induce or reward referrals or to generate Federal healthcare program business.
- AKS applies to any person or business; and, any item or service.
- Violation of AKS is intent-based; a business or person must knowingly and willfully set out to induce or reward referrals.
- AKS includes both criminal and civil penalties with possible jail time and significant civil money penalties.

29

HIPAA Privacy and Security

- HIPAA is a federal law which provides standards for protection of protected health information (PHI) and for individual rights to understand and control how PHI is used.
- Guidance for compliance with HIPAA exists at each CHSPSC affiliate in the form of:
  - Detailed policies and procedures for managing HIPAA privacy and security standards,
  - A designated Facility Privacy Officer,
  - Annual training requirements,
  - Administrative, physical and technical safeguards to prevent intentional or accidental inappropriate use or disclosure of PHI,
  - A documented process to mitigate harm to a patient or patients whose PHI may have been inappropriately used or disclosed,
  - A procedure for individuals to share complaints regarding use or disclosure of their PHI, and
  - Other protections as required by HIPAA and state laws which may be more stringent than HIPAA.

30

Important Reminders

- Review compliance risk areas related to your job duties with your department leader.
- Ask if you are not sure about something and ALWAYS….
- Report concerns and suspected misconduct.

31