

OBSTETRICS & GYNECOLOGY

University of Washington Medical Center

Dear Student,

We would like to welcome you to your Obstetrics and Gynecology Basic Clerkship. During this six week clerkship you will have the opportunity to apply and increase your knowledge in both clinical and didactic settings. Our faculty members enjoy teaching, especially in a one-on-one basis. We hope you will take advantage of their expertise and learn as much as possible; do not be afraid to ask questions.

The general orientation for Wasilla students takes place on the first morning of the clerkship at Generation Medical Center in Wasilla. You should review pelvic anatomy before the orientation. You will find the web based Course Guide especially useful because it contains a description of the clerkship, course requirements, and an explanation of the evaluation instruments. The Guide also includes the required topics for course reading. It will be to your benefit to be familiar with all the topics listed, either through experience or through reading. Core textbooks for the rotation will be on loan to you and distributed at orientation. Your rotation schedule will be given to you during orientation at the site. You will need your black bag of instruments for clinic and your white coat.

If you have questions or problems, you may call Michelle Devine, WWAMI Secretary, at (907)786-4747 She will be happy to help you.

Generation Medical Center
 3223 East palmer-Wasilla Hwy #1
 Wasilla, AK 99654

Complete, up-to-date clerkship and schedule information is available online at:
www.obgyn.uwmedicine.org/clerkship

Date to Remember	Time	Activity	Location
1 st day of Clerkship		Orientation	Generation Medical Center
Last day of Clerkship	8:00 AM	Final written exam Complete Evaluation	Anchorage or Seattle
	5:00 PM	Clerkship officially ends	

If you have any questions, either before or during the clerkship, please do not hesitate to call us.

Vicki Mendiratta, MD
 Clerkship Director
 OB/GYN Division of Education
 vmendira@u.washington.edu

Whitney Hiatt
 Clerkship Coordinator
 206-543-3892
 whiatt11@u.washington.edu

**TABLE OF CONTENTS
COMMUNITY HEALTH SYSTEMS
CODE OF CONDUCT**

	Page
STATEMENT OF BELIEFS	2
WELCOME	3
INTRODUCTION	4
THE ROLE OF MANAGEMENT	4
THE ROLE OF THE INDIVIDUAL	6
<i>Grievance Resolution</i>	6
CODE OF CONDUCT IN THE WORKPLACE	6
<i>Harassment and Violence</i>	6
<i>Equal Employment Opportunity</i>	7
<i>Conflicts of Interest</i>	7
<i>Relationships with Vendors and Suppliers</i>	7
<i>Professional Licenses, Certifications, and Credentials</i>	8
<i>Substance Abuse and Controlled Substances</i>	8
<i>Use of Organizational Assets</i>	8
<i>Outside Employment</i>	9
<i>Health, Safety, and the Environment</i>	9
<i>Inside Information and Securities Trading</i>	9
<i>Government or Union Officials</i>	9
THE CODE OF CONDUCT AND OUR CUSTOMERS	10
Patients	
<i>Confidentiality of Patient Information</i>	10
<i>Emergency Medical Treatment</i>	10
<i>Patient Rights</i>	11
<i>Human Subject Research</i>	12
Physicians	
<i>Financial Arrangements</i>	12
<i>Referrals</i>	12
Third Party Payers	
<i>Coding and Billing</i>	13
<i>Cost Reports</i>	13
ACCREDITING BODIES AND REGULATORY COMPLIANCE	13
FINANCIAL, BUSINESS AND MEDICAL INFORMATION	
AND INFORMATION SYSTEMS	14
<i>Financial Reporting and Records</i>	14
<i>Confidential Information</i>	15
<i>Retention, and Disposal of Documents and Records</i>	15
<i>Electronic Media, Records, and Documents</i>	15
15	
POLITICAL ACTIVITIES AND CONTRIBUTIONS	16
COMMUNITY SERVICE	16
THE CORPORATE COMPLIANCE PROGRAM	16
Program Structure	16
<i>Reporting Questions or Concerns</i>	17
<i>Reporting Violations</i>	18
<i>Federal and State False Claims Act Laws</i>	18
<i>Confidential Disclosure Program</i>	18
Confidential Disclosure Program Hotline: 1-800-495-9510	19

<i>Investigation of Known or Suspected Violations</i>	19
<i>Corrective Action</i>	19
<i>Discipline</i>	19
ACKNOWLEDGMENT	
20	
<i>Acknowledgement Signature Page Pullout Insert</i>	21

COMMUNITY HEALTH SYSTEMS¹

CODE OF CONDUCT

STATEMENT OF BELIEFS

Our organization believes that each community served is different and that the success of each hospital depends upon the actions of each employee, physician, contractor, and agent of that hospital. We have adopted the following Statement of Beliefs that summarizes the commitments of the organization’s constituents to our patients, employees, 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 employee in providing high quality, personalized care to our patients.

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

We advocate employee 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.

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. is a holding company. 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 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. Community Health Systems Professional Services Corporation (“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 Employees and Colleagues,

It is my pleasure to welcome you to employment or association with Community Health Systems.

When you decided to join Community Health Systems, 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 our company policies and procedures, applicable regulations and laws and good common sense. It serves as a solid framework for business decisions and it is mandatory that each of us comply with this Code of Conduct every single day.

As a condition of your relationship or employment with CHS, it is required that you read the Code of Conduct and follow 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, employees, 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 the Compliance Manual and other department policy manuals. The Compliance Manual and department policy and procedure manuals 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 manuals, as well as the Code of Conduct.

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 up to and including termination for employees 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 employees, physicians, contractors, agents, facilities, or CHS. Questions or concerns regarding interpretation of this Code or any Compliance Manual policy should be addressed to a supervisor, the Facility Compliance Officer (FCO), 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 Management 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, President and Chief Executive Officer
W. Larry Cash, Executive Vice President and Chief Financial Officer
Rachel A. Seifert, Senior Vice President and General Counsel
Martin G. Schweinhart, Senior Vice President, Operations
Carolyn Lipp, Senior Vice President, Quality and Resource Management
Michael Lynd, Vice President, Internal Audit
Andi Bosshart, Vice President, Corporate Compliance and Privacy Officer

Members of Community Health Systems Professional Services Corporation (“CHSPSC”), management consultant, provide advice and recommendations on particular functions or areas of expertise.

The Corporate Compliance and Privacy Officer for CHS 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 Management 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 employees 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 human resources officers to assure employees, 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 managers and employees to report suspected fraud and other improprieties without fear of retaliation.
- Preparing and submitting (after obtaining any appropriate committee approvals) all periodic reports required under the Compliance Program to the Management 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. All CHS colleagues are required to notify the Facility Compliance Officer, 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.

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. The 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 the Employee Handbook or contact the Human Resources Department for more information.

CODE OF CONDUCT IN THE WORKPLACE

Harassment and Violence

Every employee has a right to a work environment free of harassment or discrimination based on gender, age, race, ethnicity, religion, creed, national origin, sexual orientation or any other attribute or characteristic protected under federal or state law. All colleagues shall treat one another with courtesy, fairness, and respect. We will not tolerate any sexual, racial, ethnic, religious, or other forms of harassment of colleagues or applicants. The organization will take action to fairly and objectively address any complaints of harassment or inappropriate behavior. If you experience or witness such behavior, contact the facility Human Resources Department, the FCO, the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program.

In addition, physicians, nurses and other hospital employees who observe or are otherwise made aware of disruptive behavior by a practitioner must document the behavior and report it to the facility Human Resources Department, the FCO, or a member of administrative management. "Disruptive conduct" is any conduct which disrupts the smooth operation of the Hospital, poses a threat to patient care or exposes the Hospital and/or Medical Staff to liability.

Workplace violence, such as stalking, robbery, assault (verbal or physical), battery, vandalism, and other crimes committed by current or former employees or their associates is not acceptable and will not be tolerated. Colleagues must not bring firearms, explosive devices, or other weapons or dangerous materials onto any hospital or affiliate's property. Colleagues who witness any form of violence or harassment are required to report the conduct to the facility Human Resources Director, the Facility Compliance Officer, the Corporate Compliance and Privacy Officer, or the Confidential Disclosure Program.

Equal Employment Opportunity

We value the talents and skill sets of each colleague and applicant. The organization is determined to provide an equal opportunity environment and to comply with all laws, regulations, and policies regarding personnel actions. It is the policy of each CHS affiliate to provide equal opportunity without regard to race, religion, color, national origin, age, gender, disability, marital status, veteran status, sexual orientation, or any other characteristics protected by federal, state, or local laws.

CHS and its affiliates do not discriminate against anyone with a disability regarding terms or conditions of employment. Reasonable accommodations for the disability or other special needs of an employee will be made when conditions permit.

Conflicts of Interest

Employees should not have any personal interests or outside activities that are incompatible, or appear to be incompatible, with the loyalty and responsibility owed to the organization. Employees must avoid any outside financial interest that might influence decisions or actions in the performance of their duties for the organization. This restriction 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. Such interests 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 or the Division President. Divestiture of such interest may be required if the financial interest is deemed to be in conflict with the organization's best interests.

Relationships with Vendors and Suppliers

When conducting business with vendors or suppliers including physicians, CHS expects employees to make decisions that are in the best interest of the organization. Employees 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. Employees 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. Questions should be directed to the Corporate Compliance and Privacy Officer.

Employees 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: CHS Compliance Policy B7, Discounts and Waivers Policy, CHS Compliance Policy K7, Policy on Purchasing Goods and Vendor Relationships (Discounts), CHS Compliance Policy K8, Business Courtesies and Other Miscellaneous Financial Arrangements with Potential Referral Sources, and the employee handbook.

Professional Licenses, Certifications, and Credentials

Colleagues who are required to maintain professional licenses, certifications, or other credentials must maintain 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.

Substance Abuse and Controlled Substances

The use of intoxicants, substances causing impairment, or illegal drugs including prescription drugs prescribed for someone other than the employee 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 if such use impairs the colleague's job performance or endangers the health and safety of patients or other colleagues. All potential employees are subject to a pre-employment drug screen. In addition to pre-employment screening, the organization has implemented other drug screening programs to detect and deter the inappropriate use of drugs in the workplace.

At times, employees may need to take prescription or over-the-counter drugs that could impair their job performance. It is important for them to notify a 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 employee is responsible for assuring that assets are used only for valid purposes. These assets include, but are not limited to, physical plants, equipment, corporate funds, drugs, medical supplies, office supplies, business strategies, financial data, and other information about the organization's business. These assets will not be used to provide personal gain for employees 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.

Employees may not transfer any of the organization's assets to other people except for fair market value consideration and in the ordinary course of business. Occasionally, some assets of the organization deemed no longer needed in the business may be sold to employees. Such sales must be properly approved, documented, and signed by appropriate supervisory personnel other than the employee.

Outside Employment

Department heads and supervisory personnel above the department head level may not be employed by any other competing healthcare entity while employed by a CHS affiliated entity.

During nonworking (personal) times, nonexempt (hourly) employees may work for other healthcare entities provided it does not interfere with their job performance with their facility.

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 coworkers, utilizing pollution control systems, and following safe and sanitary procedures for the disposition of industrial and hazardous waste materials. Colleagues are encouraged to 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, a detailed "Statement of Company Policy – Securities Trades by Company Personnel" is available on the Legal Department intranet web page.

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 information about the competitor. Competitor's personnel, customers, or suppliers must not be urged or coerced to disclose confidential information, nor shall such information be sought from competitor's employees subsequently hired by the organization.

Government or Union Officials

Employees will not offer any government employee, union official, or their representatives any meals, entertainment, or gifts that would cause the recipient to be in violation of applicable 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. In addition, each facility has a designated Facility Privacy Officer who is available for questions and training, and who assists with investigations of potential privacy breaches.

Colleagues must never disclose or release confidential patient information including pictures 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 release of information laws, which may require the express written authorization of the patient. Colleagues should not access or use any patient information unless it is necessary to perform his/her job.

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 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 in a medical emergency. 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 Facility Privacy Officer or the Corporate Compliance and Privacy Officer.

Reference: CHS Compliance Policy / Procedure M1; Compliance with HIPAA Privacy Regulations, Definitions

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 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: CHS Compliance Policy / Procedure G2a; EMTALA – Medical Screening/Stabilization

Patient Rights

Patients have a right to healthcare at the organization's facilities without regard to gender, race, ethnicity, cultural, 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 will receive a written copy of the patients' rights and responsibilities. Patients' rights include, but are not limited to, the right to:

- Know the risks, benefits, and alternatives to proposed treatments or procedures.
- Information about the physicians or other clinicians that will be providing the patient's care or treatment.
- Receive information in easy to understand terms that will allow for an informed consent or refusal of the treatment or procedure.
- Privacy regarding their medical care.
- Participate in the plan of care.
- Formulate advanced directives and to have staff and practitioners comply with those directives.
- Reasonable responses to reasonable requests for service.
- Leave the hospital against the advice of the physician.
- Examine and receive an explanation of the bill for services regardless of the source of payment.
- Select providers of goods and services after discharge.
- Receive a Notice of Privacy Practices.
- Ask for a restriction on use or disclosure of their protected health information.
- Access their protected health information.
- Ask that amendments be made to their protected health information.
- Ask for an accounting of disclosures of their protected health information.

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

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: CHS Compliance Policy / Procedure K10 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 side agreement(s) 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 Manual 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 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.

Reference: CHS Compliance Policy/Procedure K8; 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 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, such as those provided in *AHA Coding Clinic for ICD-9-CM*.

The organization will audit and monitor using valid statistical sampling methodologies to verify the accuracy and validity of coded data and claims regardless of the source of payment.

Reference: CHS Compliance Policy K1; Coding Compliance Policy.

Cost Reports

We 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 must be directed to the Corporate Revenue Management Department.

ACCREDITING BODIES AND REGULATORY COMPLIANCE

CHS affiliated facilities seek accreditation from various agencies and accrediting bodies, and CHS mandates that all standards required by those accrediting bodies are 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.

The organization operates in many states where 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 donors, 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 the Senior Vice President, Quality and Resource Management, in the event of a visit by an inspection or survey team at 615-465-7503.

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 Senior Vice President, General Counsel at 615-465-7349.

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 CHS Financial Policies and Procedures Manual, 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, avoiding actual or apparent conflicts of interest in personal and professional relationships.
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 information acquired in the course of my work except when authorized or otherwise legally obligated to disclose. Confidential information acquired in the course of my work is not used for personal advantage.
6. I share knowledge and maintain skills important and relevant to my constituents' needs.
7. I proactively promote ethical behavior as a responsible partner among peers in my work environment.

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

Confidential Information

Confidential 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 organization 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 knowledge gained as a result of his/her employment. Upon termination, a colleague is prohibited from taking, retaining, copying, or directing any other person to take, retain, or copy any papers, data, clients lists, books, records, files, or any other type of documentation or confidential information belonging to the organization without prior written permission.

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. Employees 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: CHS Compliance Policy/Procedure K9; Document Retention

Electronic Media, Records, and Documents

Many different types of media are used by the organization 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. Any patient and/or confidential information must not be conveyed by any media sources unless appropriate security measures are in place. Colleagues must not use the organization's electronic media to distribute or transmit any threatening, malicious, false, or obscene materials.

E-mail and internet facilities and 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.

Colleagues shall not post pictures or other recordings of patients or individually identifiable patient information on any social networking site. The use of personal cell phones for capture and/or transmittal of patient recordings or pictures for use other than a specific patient care function are strictly prohibited and may lead to disciplinary action up to and including termination.

POLITICAL ACTIVITIES AND CONTRIBUTIONS

The organization supports employee 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 employee's work performance. Employees must recognize that involvement and participation in political activities is on an individual basis, on their own time, and at their own expense. When employees speak on public issues, they must make it clear to the audience that their comments are their own personal viewpoints.

No employee is authorized to contribute, directly or indirectly, any assets of any CHS affiliate including cash or the work time of any employee, to any political office holder, party or campaign of any candidate for federal, state, or local office without following the appropriate corporate approval process.

COMMUNITY SERVICE

The organization encourages colleagues to participate in community service projects. The service project must not create a conflict of interest with the organization nor reduce the colleague's work performance.

THE CORPORATE 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 employees 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 an organizational 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 Corporate Compliance Program is guided and approved by the Management Compliance Committee. There is also a Corporate Compliance and Privacy Officer, a Corporate Compliance Work Group, Facility Compliance Committees, and Facility Compliance Officers. Additional elements of the ongoing Compliance Program include:

- Maintenance, publication, and distribution of the Code of Conduct and Compliance Manual policies and procedures.
- Analysis 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, and regulations (e.g., the False Claims Act, HIPAA, PPS, 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 Vice President, Corporate Compliance and Privacy Officer for CHS is 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
- The Facility Compliance Officer
- The 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 their 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: CHS Compliance Policy K11; Preventing, Detecting and Reporting Fraud, Waste and Abuse. State DRA Guidelines are available as a subset to K11 on the Compliance Intranet site

Confidential Disclosure Program

We have established a Confidential Disclosure Program for all colleagues and other individuals of all subsidiaries and affiliates of the organization 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 Manual 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 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 Professional Services
Corporation
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 Work Group members and their staff will be made. The Corporate Compliance and Privacy Officer or her designee will coordinate any findings from the investigations and recommend corrective and/or disciplinary actions.

All employees are required to cooperate with the investigation efforts. Any employee that refuses to cooperate with an investigation may be subject to disciplinary action up to and including termination.

Corrective Action

Once a reported violation is substantiated through the investigation process, we will initiate corrective action. 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 facility or affiliate.

Discipline

Common sense, good business judgment, and ethical behavior are expected from each employee. Violations of the Code of Conduct or organization policies will be subject to the organization's normal disciplinary procedures. Disciplinary action that may be taken includes, but is not limited to, informal counseling, verbal and/or written warnings, investigative or disciplinary suspension, probation, demotion, or termination.

ACKNOWLEDGMENT

The Code of Conduct is a mandatory policy of the organization. All colleagues will sign a form indicating they have reviewed a copy of the Code and understand it. In addition, all colleagues will reaffirm these actions on an annual basis.

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

The Code of Conduct is a unilateral statement of policy by CHS. 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 December 9, 2009 (supersedes the revision adopted February 27, 2008).

ACKNOWLEDGEMENT

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

I agree to abide by the 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 12-09



Community Health Systems



Computer System User Rights and Responsibilities Agreement

You are responsible for following facility security policies related to use of CHS (hereafter referred to as the Company) systems and data. Please be aware that your conduct can reflect upon the reputation of the Company. What you say or do while on external networks may be interpreted as the Company's or this facility's position or policy. Access to Company systems is provided solely for business purposes. All access may be revoked at any time at the discretion of your supervisor and/or the Company.

Listed below are examples of inappropriate use of the systems. Please note that this list is not intended to be all-inclusive.

1. Sending harassing, libelous, or disruptive messages to others.
2. Transmitting personal data or unauthorized Company-owned data across the Internet without proper security measures or at any time for non-business related purposes.
3. Violating copyright laws.
4. Accessing from Company resources any obscene or pornographic material of any type.
5. Sending threatening, racially harassing, or sexually harassing messages.
6. Attempting to exceed access privileges or break into any computer system.
7. Willfully circumventing the security features of the automated information systems or network access systems at this or any other facility.
8. Using Company resources for personal or non-official business.
9. Downloading to Company computers from the Internet any program not directly related to your work responsibilities (i.e., games and screen savers).
10. Introducing computer viruses, worms, Trojan horses or other types of malicious computer codes.
11. Violating US export laws concerning the export of cryptographic products (contained in Lotus Notes, VPN Software, PC Guardian, and others.) *If you do not travel outside of the U.S. with your computer, this does not pertain to you.*
12. Violating any privacy or security standards covered by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA).

Non-Compliance

All users of data and systems are responsible for complying with the Company's computer security policies and procedures. Anyone suspecting misuse or attempted misuse of CHS information systems or resources must report such activity to their supervisor or the facility IT Director. Violations of standards, procedures, or practices in support of this policy will be brought to the attention of management for appropriate action. Penalties may include loss of access privileges and/or disciplinary action up to and including termination of employment.

CHS computer systems are restricted to, CHS Hospitals, Inc. and its subsidiaries and affiliates, authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited by CHS. Unauthorized users are subject to Company disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and acknowledges that access may be terminated by CHS at any time at its sole discretion. Anyone accessing this system is further advised that if monitoring reveals possible evidence of criminal activity, CHS may provide the evidence of such activity to law enforcement officials. All users must comply with CHS Corporate instructions regarding the protection of CHS information assets.



I have read and agree to the terms as set forth and recognize that my access may be monitored and recorded.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

User Signature Date

User Name (Please Print) Date

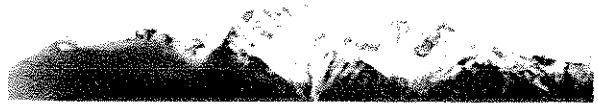
Supervisor's Signature Date

Supervisor's Name (Please Print) Date

Routing:

- ✓ **MSRMC Employees and Temp Staff – HR Director**
- ✓ **MSRMC Medical Staff – Medical Staff Coordinator**
- ✓ **Students – Education Director**
- ✓ **Vendors / Contractors & Others – IS Director**

MAT-SU REGIONAL
MEDICAL CENTER



2500 S. Woodworth Loop, Palmer AK 99645
(907) 861-6000

Confidentiality and Security Agreement:

This form is to be signed by all persons performing work either onsite at Mat-Su Regional Medical Center (MSRMC), or in a remote capacity for MSRMC. This form is to be signed by all persons prior to granting access to MSRMC confidential information. This form applies to employees, physicians, contractors, and other associates as deemed appropriate by MSRMC.

I understand that the facility or business entity (the "Company") in which or for whom I work, volunteer or provide services, or with whom the entity (e.g., physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information, has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment / assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the internet (under Ethics & Compliance). **I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.**

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.
2. I will not in any way divulge copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.
3. I will not discuss Confidential Information where others can overhear the conversation. It is not acceptable to discuss Confidential Information even if the patient's name is not used.
4. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
5. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
6. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
7. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company.
8. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
9. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.
10. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
11. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including e-mail, in order to manage systems and enforce security.
12. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and position screens away from public view.

13. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards.
14. I will:
 - a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
15. I will never:
 - a. Share/disclose user-IDs, passwords or tokens.
 - b. Use tools or techniques to break/exploit security measures.
 - c. Connect to unauthorized networks through the systems or devices.
16. I will notify my manager, Local Security Coordinator (LSC), or appropriate Information Services person if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information.

The following statements apply to physicians using Company systems containing patient identifiable health information:

17. I will only access software systems to review patient records when I have that patient's consent to do so. By accessing a patient's record, I am affirmatively representing to the Company at the time of each access that I have the requisite patient consent to do so, and the Company may rely on that representation in granting such access to me.
18. I will insure that only appropriate personnel in my office will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
19. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.

Signing this document I acknowledge that I have read this Agreement and I agree to comply with the terms and conditions stated above.

Signature:		Date:	
Facility Name & COID:			
Last Name (Printed):		First Name:	MI:
Job Title:		Department/Location:	
Work Phone:		FAX:	
Pager #:		Supervisor:	
Information Services Use:		Last 4 of SS#:	

Routing:

- ✓ **MSRMC Employees and Temp Staff – HR Director**
- ✓ **MSRMC Medical Staff – Medical Staff Coordinator**
- ✓ **Students – Education Director**
- ✓ **Vendors / Contractors & Others – IS Director**