CAPELLA HEALTHCARE™

2013 CODE OF CONDUCT

www.capellahealthcare.com/ethics

TABLE OF CONTENTS

FOREWORD 5

CHAPTER 1: HOW ETHICS & COMPLIANCE WORKS FOR YOU 6

CHAPTER 2: PATIENT CARE 8

PATIENT SAFETY 8

PATIENT QUALITY 8

PATIENT GRIEVANCES 9

PATIENT EMERGENCIES 9

PATIENT PRIVACY 10

ALTERNATIVE MEANS OF REPORTING POTENTIAL PATIENT SAFETY OR QUALITY ISSUES 10

CHAPTER 3: PRIVACY & INFORMATION SECURITY 11

COVERED ENTITY 11

DISCLOSURE FOR TREATMENT, PAYMENT AND OPERATIONS (TPO) 12

MINIMUM NECESSARY STANDARD 12

UNAUTHORIZED DISCLOSURES OF PHI 12

INAPPROPRIATE ACCESS TO PHI 13

SAFEGUARDING PHI 13

IDENTITY THEFT 14

HIPAA ENFORCEMENT 15

FACEBOOK, TWITTER & OTHER SOCIAL MEDIA 15

PRIVACY & INFORMATION SECURITY POLICIES 15

CHAPTER 4: WORKPLACE RULES 16

CONFIDENTIALITY OF BUSINESS INFORMATION 16

CONFLICT OF INTEREST 16

DIVERSITY & EQUAL OPPORTUNITY . . . 17
HARASSMENT . . . 18
WORKPLACE VIOLENCE . . . 18
GIFTS FROM VENDORS . . . 18
GIFTS TO OFFICIALS . . . 19
INFORMATION TECHNOLOGY SYSTEMS . . . 19
PERSONAL USE OF COMPANY RESOURCES . . . 20
COPYRIGHTS & INTELLECTUAL PROPERTY . . . 20
SUBSTANCE ABUSE . . . 20

CHAPTER 5: LAWS & REGULATIONS 21

ANTI-KICKBACK AND STARK . . . 21
ANTI-TRUST . . . 22
BILLING AND CODING . . . 22
FALSE CLAIMS AND FRAUDULENT CLAIMS . . . 22
INELIGIBLE INDIVIDUALS AND VENDORS . . . 23
ENVIRONMENTAL LAWS . . . 23
POLITICAL ACTIVITIES . . . 24
RESPONDING TO SEARCH WARRANTS . . . 24

CHAPTER 6: REPORTING VIOLATIONS & CONCERNS 25

HOW TO REPORT INFRACTIONS OR CONCERNS . . . 26
THE ETHICS LINE . . . 26
SUGGESTIONS FOR EFFECTIVE REPORTING . . . 27
ACKNOWLEDGMENT OF THE CODE OF CONDUCT . . . 27
2013 CALENDAR YEAR ACKNOWLEDGMENT . . . 29
APPENDIX . . . 31–35

FOREWORD

We are privileged to be able to spend our lives in the service of others as we seek to help individuals and communities manage health and illness. Whether it was a childhood dream of yours to become a healthcare professional, or whether you came to this career later in life, you are no doubt aware of how very challenging it has become to manage the business of healthcare.

In fact, the healthcare industry is probably the single most regulated industry in the nation. Almost every healthcare activity, from dispensing drugs to serving meals to billing for services, is covered by laws and regulations at the city, county, state and federal level. In addition, our industry must adhere to standards set forth by numerous licensing and accrediting bodies, such as The Joint Commission (TJC) and the Centers for Medicaid and Medicare Services (CMS).

It is important that you read this booklet in its entirety and understand all the requirements of our Ethics and Compliance program. It is also important that you retain this booklet and keep it in a prominent place, such as on your desk or at your workstation. This booklet will serve as a reference guide for compliance and other related issues that may arise during the year.

It is also important to know the names and phone numbers of your local Ethics & Compliance team. Please ask your supervisor for this information and write it below.

Title	Name	Phone
Ethics & Compliance Officer		
Associate Ethics & Compliance Officer		
Human Resources Director		
Privacy Officer		
Identity Integrity Officer		
Information Security Officer		

CHAPTER 1:
How Ethics & Compliance Works For You

Capella's Ethics & Compliance program is designed around the seven elements of an effective compliance program, as set forth by the HHS Office of Inspector General (OIG) in its model hospital compliance program. These seven elements are also reflected in the federal sentencing guidelines established by the U.S. Department of Justice. The following summarizes the structure of our program and its relevance to the seven elements.

1. **Governance and Oversight** Our Ethics & Compliance program is governed at the highest levels of Capella. For example, the hospital Ethics & Compliance committees report to the hospital Board of Trustees and the corporate Ethics & Compliance committee. The corporate Ethics & Compliance committee, in turn, reports to the Capella Board of Directors.

2. **Standard and Procedures** We have adopted almost 200 policies and procedures that aim to address various areas of regulatory risk and compliance. This Code of Conduct booklet is intended to be a high level summary of those policies. The appendix in this booklet contains a list of all of the compliance policies, which are accessible on the local intranets of each hospital. Each workforce member is responsible for fully understanding the compliance policies that affect their particular role in the organization. For example, if you work in the HIM department and perform medical records coding, you must become familiar with the Hospital Coding Compliance (HCC) policies.

3. **Education Programs** We have established various education modules to ensure our workforce members are properly trained on the requirements of the compliance policies that impact their respective jobs. These training programs are provided through a variety of platforms, including HealthStream, webinars, live training and self study courses.

4. **Auditing and Monitoring** We routinely audit and monitor adherence to our compliance policies, especially in areas we deem to be at high risk of potential non-compliance.

5. **Standards of Discipline** To ensure that our compliance policies are followed and that workforce members are treated equally, we have adopted standard levels of disciplinary action for violations of our compliance policies. These standards also state that workforce members who self-report accidental or non-purposeful violations of our compliance policies will not be disciplined but instead, will be provided additional education on the policies in question.

6. **Reporting Options for Compliance Issues** As set forth in this booklet, we have established various means to report compliance issues, including the operation of a secure, third-party Ethics Line that is staffed 24 hours a day, every day of the year. All workforce members who file a report with the Ethics Line can choose to remain anonymous. We have a strong non-retaliation policy which states there will be no retaliation against any workforce member for contacting the Ethics Line or otherwise reporting a compliance concern. Retaliation against a person who reports a compliance issue will be subject to disciplinary action up to, and including, termination. Civil penalties may also apply.

7. **Response and Prevention** Our compliance policies state that we will respond to all compliance issues raised by our compliance program, whether it is an Ethics Line call, an audit finding or a referral from an outside agency. We will remediate the issue raised, take steps to mitigate the risk of a future occurrence and, if necessary, pay back any excess payments we may have received as a result of non-compliance.

CHAPTER 2: Patient Care

Patient Safety

The safety of our patients is our top priority. Safety means protecting patients from harm, such as fires and natural disasters. It also means protecting patients from falling, taking the wrong medications, and safeguarding them when they are under sedation. Patient safety is a priority for all of us, not just the doctors, nurses and technicians who attend to patients. Personnel in other occupations, such as housekeeping or food services, must also stay alert for any possible harm which may jeopardize a patient.

A great culture of safety is our goal; to that end, all of us (physicians, nurses and others) must work together to develop an environment of self-respect and trust. A great culture of safety is free from harassment, retaliation, finger-pointing and blame shifting. All of us are on the same team and the patient is always our top priority.

Patient Quality

We strive to provide the highest quality of service to our patients. Quality is providing the appropriate level of patient care delivered in the right amount to meet the needs of the patient. This means each plan of care is tailored to the needs of the individual patient with the goal that our patient will not receive too few or too many services, but the right amount. Quality also means delivering our services on a timely basis as outlined by the physician's plan of care.

Quality includes great customer service. All of us should show compassion for patients and their families and try to make their experience as positive as possible. Keep in mind patients and their families are often anxious about a hospital visit, so be understanding, treat them with kindness and work with your team to make their stay a positive one.

Patient Grievances

Because patients and their family members are often anxious about being in the hospital, they may lodge a complaint or grievance about our service. These grievances could be directed at physicians, nurses or other caregivers. Even a grievance about our food should be taken seriously.

Our policy is to investigate each and every patient grievance. You have a duty to promptly report grievances to your supervisor. In turn, you or your supervisor will report the grievance to your facility Chief Quality Officer or CQO. Your CQO will coordinate the investigation and respond to the person who raised the grievance.

Patient Emergencies

A significant portion of our patients enter the hospital through the emergency department. A federal law known as the Emergency Medical Treatment and Active Labor Act (EMTALA) requires us to take special care regarding emergencies. These measures include:

- Making sure anyone who comes to our facility and expresses a need for medical assistance (or, if it is clear from the circumstances that medical assistance is needed) is provided a prompt medical screening examination to determine if the patient has a true emergency. This screening must be provided without regard to the patient's ability to pay.

- If an emergency medical condition is present, the patient must be stabilized to the extent possible and to the best of our hospital's ability, without regard to the patient's ability to pay for this treatment.

- If the patient needs to, or wants to, be transferred to another hospital, we must determine that the benefits of the transfer outweigh the risks. We must also coordinate the transfer with the other hospital.

Most, but not all, patients in need of emergency care arrive at the emergency department. Some patients mistakenly come to the front lobby or the outpatient entrance. You should be on alert for anyone who appears in distress

or in need of emergency medical care. Every situation is different and you should become familiar with whom to call if you see an emergency. In many cases, a caregiver such as a doctor or nurse will be close by. If this is the case, you should immediately alert one of them.

Patient Privacy

Patients have a right to privacy. This is mandated by a federal law known by its acronym HIPAA. Under HIPAA, any "Workforce Member" (that is, anyone working in the facility including employees, contractors, volunteers, physicians, etc.), must honor the privacy rights of our patients. This means you cannot disclose any unauthorized information about a patient. However, certain exceptions apply, as you will see in Chapter 3.

Alternative Means of Reporting Potential Patient Safety or Quality Issues

In the event you see a patient safety issue that is not being properly resolved, you have the duty to report this matter using one of several reporting methods. Under each of these methods, you have the option to remain anonymous.

- You may bring this matter directly to the attention of the facility Chief Quality Officer.
- You may make a report to Capella's Ethics Line. See Chapter 6 for more details.
- You may lodge a report with The Joint Commission by calling them at 1-800-994-6640 or sending them an email at complaints@jointcommission.org.

Regardless of the method you use, we have a written non-retaliation policy that protects you for reporting patient care issues or any other patient saftey or quality issues.

CHAPTER 3: Privacy & Information Security

Our goal is to have great information security, compliance, and privacy programs. These programs are centered on protecting patient and company information. In general:

- Information Security addresses how we protect electronic patient and company information. Easy examples include firewalls, email and hard drive encryption, and reviewing user access to our systems and applications.
- Compliance means showing how we follow regulatory requirements and standards to protect patient and company information. HIPAA Security and Privacy rules are a well known example.
- Privacy is how we collect and share patient and company information with others. We should collect only the necessary information to provide services to others while sharing this information with only those who are authorized to see it.

This chapter lays out an overview of our programs. You will receive more detailed security, compliance, and privacy training throughout the year. The HIPAA regulations (which include privacy and security) begin with the premise that all protected health information (PHI) is private and cannot be shared with anyone. However, the authors of HIPAA realized this level of protection could actually hinder patient care. Accordingly, HIPAA makes certain exceptions to the privacy rule to make it more workable in healthcare. Let's start with who is governed by HIPAA.

Covered Entity

HIPAA only applies to Covered Entities. A covered entity is defined as a healthcare provider, a health insurer or a healthcare clearinghouse. Healthcare providers include hospitals, nursing homes, doctors, walk-in clinics, sports medicine centers and any other entity that delivers healthcare to patients. Health insurance companies include many companies you would recognize, but also include more obscure companies, such as the firm that manages your flex spending account. Healthcare clearinghouses are companies that exchange patient information between providers and insurance companies.

One common misconception is HIPAA applies to everyone. In fact, HIPAA only applies to Covered Entities and their business associates. For example, if your friend told another friend that you were in the hospital for an operation, it might seem like a HIPAA violation, but it is not, unless your friend worked at the hospital and learned of your operation while working at the hospital.

Disclosure for Treatment, Payment and Operations (TPO)

HIPAA allows covered entities to share certain PHI in the course of treating a patient, billing on behalf of a patient or operating the facility which is treating a patient. These three activities are commonly referred to as TPO.

Some examples include:

- A doctor and a nurse can exchange information about a patient that they are both treating
- A hospital can exchange information with the patient's insurance company in order to bill for the service
- A healthcare clearinghouse can serve as the entity by which electronic information is exchanged between providers and insurers

Minimum Necessary Standard

Information exchanged for TPO purposes must meet the "minimum necessary" standard. This simply means you do not share more PHI than you have to. You would provide the other party the necessary and minimum information they need to perform their part of the TPO process. The same rule applies when you access PHI. You should only access the information you need for your specific task. Do not look at an entire record out of curiosity.

Unauthorized Disclosures of PHI

An unauthorized disclosure is any disclosure that is not part of TPO and does not meet the minimum necessary standard. The most common examples are

- Discussing a patient's case, by name, with persons who are not involved in the patient's treatment, payment and operations process

- Losing PHI, even for a short period of time (such as leaving a record in the break room)
- Taking pictures of patients without their consent
- Posting PHI on social networking websites, such as Facebook, Twitter, Tumblr, etc.

Inappropriate Access to PHI

An inappropriate access results when someone gains access to PHI for which they have no valid reason to access. The most common examples are

- Looking at the electronic medical record of a patient with whom you have no involvement
- Looking at your own electronic medical record. (You must request this access by going through the HIM Department and signing an authorization)
- Discovering a chart that was misplaced and reading it before you return it
- Gazing at a computer screen out of curiosity

Safeguarding PHI

HIPAA requires Covered Entities to take strong measures to safeguard PHI. Safeguards include both physical safeguards and electronic safeguards. Physical safeguards include securing paper PHI where it cannot be easily accessed. Electronic safeguards include securing our computer systems so that they are not vulnerable to unauthorized access.

We have specific rules that must be followed in order to properly safeguard PHI.

- Active paper records, such as a chart for a patient who is still in-house, must be secured at all times. You cannot leave them open on a desk or at a workstation if the desk or workstation is unattended.
- Paper records that are on file or in storage must have adequate safeguards including locks, limited access and fire-proofing and natural disaster protections.
- For electronic records, you cannot share your login with any other person. This is an absolute requirement because the electronic medical record system keeps track of the entries that are made and by whom they are made.

- For portable media, such as thumb drives, you must safeguard these by keeping them locked up and having them encrypted.
- You cannot email PHI unless the email (or the file containing the PHI) is encrypted.
- You cannot text PHI; for example, between a doctor and a nurse.

Identity Theft

Identity theft is a growing issue in the healthcare sector. Many individuals illegally share their Medicaid cards and this could result in a medical record that has entries involving numerous patients. This is dangerous because vital information, such as blood type, could be incorrect in the record. In turn, this could lead to a severe injury or death of a patient.

Another problem with identity theft is the victim often does not know that her or his identity has been stolen. In many cases, the victim has never come to our hospital. A victim's credit rating could end up being damaged or worse, their bank accounts and credit cards could be compromised.

We have a duty to monitor identity theft and report it to law enforcement if we have reasonable grounds to believe it exists. Moreover, we have identified the 5 "Red Flags" that all workforce members must understand:

1. A photo ID that does not match the person.
2. Family members or friends calling the patient by a name other than the name in the medical record.
3. A social security number that is different than the one used on the last visit.
4. A person providing personal information that does not match the information on file.
5. A person being registered who has been flagged in the system as a potential identity theft.

If you suspect identity theft, you have a duty to report it to your supervisor or the facility Identity Integrity Officer. More information about Identity Theft can be found at policy PA.015 *Identity Theft and Patient Mis-Identification*.

HIPAA Enforcement

The HIPAA rules require us to have a standard, consistently applied disciplinary policy for violations of HIPAA. In general, you will not be disciplined if you self-report any unintentional violations of our policies. You may receive HIPAA re-training and we will work with you to take steps to prevent any future, accidental HIPAA infractions.

Purposeful infractions, or repeated unintentional infractions, are subject to discipline based on the severity of the infraction. More information can be found in policy HIPAA.011, *Standards of Discipline for HIPAA Violations*. The violations subject to dismissal include, but are not limited to:

- Posting PHI, patient pictures, x-rays or any patient information on Facebook or any other social network
- Stealing PHI and selling it
- Accessing the PHI of an estranged spouse for a divorce proceeding
- Telling friends the name of someone in the psychiatric unit
- Stealing any information for the purpose of identity theft
- Unauthorized trespass into the computer system (includes hacking, unauthorized entry or disabling security protocols)

Facebook, Twitter and Other Social Media

Most likely, you have an account with Facebook, Twitter, LinkedIn or some other type of social media. As mentioned before, posting any patient information on social media can be grounds for dismissal, if the appropriate PHI authorization by the patient has not been signed. Other infractions include using social media to bully or embarrass fellow staff members, post false information about the hospital, engage in illegal activity or divulge confidential business information. Although not a requirement, we recommend that staff members who are supervisors consider not “friending” the staff members who report to them.

Privacy and Information Security Policies

More information about our privacy policies can be found at HIPAA.001 through HIPAA.011 and ITSEC.001 through ITSEC.024.

CHAPTER 4: Workplace Rules

Our goal is to create a positive work environment for all workforce members based on mutual respect and open lines of communications. We need you to help us create that environment by your willingness to assist your co-workers and peers to create a culture where patient safety and quality will flourish. This chapter covers the required workplace rules to ensure we continue to be a great place to work.

If you observe any persons violating these rules, you have a duty to report the violation to your supervisor, the human resources department or the Ethics Line. See Chapter 6 for more on the Ethics Line. We will not tolerate retaliation or harassment against any workforce member in response to the member filing a report with the Ethics Line or reporting workplace concerns through other channels.

Confidentiality of Business Information

Because Capella is a private business, you must safeguard our business information. Business information includes, but is not limited to, billing records, computer data, contracts, emails, financial records, internal communications, letters, marketing plans, personnel records, and prices. If you use business information as part of your job, you have a duty to safeguard this information and keep it confidential. The same measures of safeguarding PHI (as explained in Chapter 3) also apply to safeguarding business information.

Conflicts of Interest

A conflict of interest is any activity which involves, or appears to involve, an arrangement that could be detrimental to Capella. You may have a conflict of interest if your outside activities or personal interests influence, or appear to influence, your ability to make objective decisions on behalf of Capella. There is nothing wrong with having a conflict of interest—our objective is to manage conflicts of interest.

Conflicts of interest not only extend to your personal interests, but also the interests of your spouse, your spouse's family, your grandparents, your children and your brothers and sisters. For example, if your sister-in-law owns a catering company and you were in charge of arranging for a catered event at the hospital, you have a conflict of interest with the catering company. What this means is you must remove yourself from the decision to select the caterer; however, it does not mean the hospital cannot use the caterer. In this example, there is a conflict of interest and removing yourself from the catering decision is a way of properly managing that particular conflict of interest.

Because conflicts of interest can include your extended family, most of us will, at one time or another, encounter a situation where there is a conflict of interest. In order to properly manage any potential conflicts, and to protect you from any accusations that you may have improperly acted on a conflict of interest, we have established a policy that requires all workforce members to annually report any actual or potential conflicts they may have now or might have in the future. This annual disclosure is accomplished by noting the conflicts on the attestation card contained in this booklet. By properly disclosing your conflicts, we will be able to manage the conflicts of interest and ensure our business transactions are fair to all parties involved.

For more information, see policy EC.021 *Conflicts of Interest*.

Diversity and Equal Opportunity

Our workforce is diverse, and includes people from many places and many ancestries. Their talents and different viewpoints contribute greatly to our success. We are committed to providing an equal opportunity work environment where everyone is treated with fairness, dignity and respect. Accordingly, we will not discriminate based on sex (including pregnancy), race, religion, creed, color, national origin, age, sexual orientation, genetic information, disability, family medical history, or any other protected category. Our policy applies to all personnel actions such as hiring, staff reductions, terminations, transfers, evaluations, recruiting, compensation, corrective action, discipline, promotions and training.

Harassment

Harassment covers a wide range of behaviors of an offensive nature. It may include behavior which is found threatening, disturbing, or upsetting. Sexual harassment may include unwelcome sexual advances, requests for sexual favors in conjunction with employment decisions, and/or verbal or physical conduct that creates an intimidating, hostile or offensive work environment or otherwise interferes with work performance. Degrading or humiliating jokes, slurs or intimidation will not be tolerated. Harassment in our workplace will not be tolerated. Workforce members engaging in this behavior will be subject to disciplinary action, up to and including termination of employment.

Workplace Violence

We will maintain a violence-free work environment. Workplace violence may include harassment, assault, blackmail, and other acts that may threaten the safety of another person, impact another person's physical or psychological well-being, or cause property damage. Any workforce member who commits an act of violence will be subject to discipline up to and including termination.

If you experience or observe any form of harassment or violence in the workplace, or become aware of threats of potential violence, you have a duty to immediately report the incident to a supervisor, the human resources department, the corporate compliance officer or call the Ethics Line. We take all complaints of workplace violence and/or harassment very seriously. All reports will be promptly investigated.

Firearms, explosive devices, fireworks, lasers, tasers and other dangerous materials are prohibited on our property, with the exception of law enforcement officers and on-duty facility security members.

Gifts from Vendors

You are allowed to accept gifts from vendors, not to exceed $100 per year per vendor. This gift must be for an item or service, such as a clock or sporting tickets. You cannot accept cash or cash equivalents, such as gift cards or savings bonds. You may accept a coupon for a "targeted use" item, such as

a restaurant coupon or gym pass. If a vendor offers you free overnight travel, you must get advance permission of your Ethics & Compliance Officer. See policy EC.005, *Entertainment*.

Gifts to Officials

You must never offer a gift to, or accept a gift from, an agent of any governmental or accrediting agency. See policy EC.015, *Limitations on Gifts to Government Employees and Agents*.

Information Technology Systems

Because our information technology systems contain sensitive and private information, it is critical that you understand our concern about properly safeguarding electronic information. Information systems include computers, databases, handheld devices, email, smartphones, video monitoring systems, scanners, etc. Information must be kept confidential, and email, internet or phone systems are to be used primarily for business purposes.

Our IT systems are monitored on a continuous basis. This monitoring includes emails, internet, file access, systems access, etc. You must never login to any systems with another person's login (user name and password). The systems may not be used for viewing or transmitting pornographic or other offensive material, or for threatening, harassing, spreading rumors, or actively supporting or opposing a candidate for public office. The IT department will notify Human Resources if they detect you have viewed inappropriate websites or sent explicit emails, and Human Resources along with your manager will be in contact with you. They will also contact you if you accessed a file you were not entitled to access or viewed a medical record you were not entitled to view. Various levels of discipline will apply. See policies ITSEC.001 through ITSEC.023.

Personal Use of Company Resources

Company resources, such as photocopiers, computers and paper, are meant for company use. However, it is permissible to use company resources, in a very limited way, as long as your supervisor consents to such use. Some examples of limited use include making a copy of your tax return or limited personal use of email.

Copyrights and Intellectual Property

Print and electronic materials (including photography, audio recordings, video recordings and software) are usually protected by copyright laws. Capella workforce members are expected to respect and comply with these laws, which ensure those who created these materials receive proper credit and compensation for their work. We will not reproduce articles, pamphlets, software or other electronic materials, without written permission from the writer or publisher.

- We will maintain proper licenses (such as BMI, ASCAP OR MPAA) to play copyrighted music or video in public areas.
- We will not make copies of copyrighted magazines, books or other publications without having prior permission or a blanket license.
- We will not use trademarks or logos of other organizations without prior permission.
- We will not make copies of licensed software for distribution without having a license.
- We will not use photographs of people in our promotional publications without their written consent.

For more information, see policy LL.GEN.002, *Copyrights*

Substance Abuse

For the safety of our patients, it is vital that we have a drug and alcohol-free workforce. Our policy is to perform drug testing upon hiring. We may also perform drug or alcohol testing randomly, if there is an on-site accident or other incident, or if there is a reasonable suspicion that a workforce member is

under the influence of drugs or alcohol.

If you are taking a legally-prescribed prescription that may impair your performance, you must advise your supervisor immediately. If you report to work under the influence of alcohol or drugs, you will be subject to disciplinary action, up to and including termination of employment.

CHAPTER 5: Laws & Regulations

Our industry is complex and heavily regulated. There are numerous laws and regulations that apply to healthcare and hospitals. It is very important that you understand the specific laws that apply to your role in the company. The purpose of this chapter is not to explain every applicable law in great detail, but to briefly highlight the laws of greatest compliance concern and give you the tools to get further information.

Anti-Kickback and Stark

The Anti-Kickback law makes it unlawful to knowingly pay a Potential Referral Source for admitting a patient or referring other business to our facility. A Potential Referral Source is a physician, but it could also include any person who can order services at our facility. The Anti-Kickback law is unique to healthcare. In most industries, it is permissible to pay a customer for referring another potential customer. Under the Anti-Kickback law, you could be prosecuted for knowingly paying for referrals.

Stark, on the other hand, governs our legal relationships with physicians and other referral sources. For example, we may pay a cardiologist to read our EKGs. That is permissible but our payments to the cardiologist must be proper. To be proper, they must be evidenced by a signed contract, with a term of at least a year and payments to the cardiologist must be at fair market value. The idea behind Stark is to prevent the use of legal relationships to reward referrals. For example, if we paid the cardiologist twice the value for the EKG reads, we will have violated Stark.

Because of the compliance risk associated with physician contracts, we require all physician contracts, no matter how limited in scope, to be reviewed, in

advance, by the corporate legal department. Also, because these laws involve medical staff members in marketing and publicity, we have provided very specific guidelines to our Administrative and Marketing leadership.

Anti-Trust

We often think of Anti-Trust in terms of the federal government trying to stop a merger of two big companies or making a company sell off some of its business lines because they have cornered the market. In our industry, Anti-Trust comes into play when we work with our competitors to set prices or wages. Accordingly, you must not discuss our pricing policies or wage rates with other hospitals in our market. Sharing such information could implicate the facility and the individuals involved.

Billing and Coding

Our billing and coding activities generate the bills we send to the patient's insurance provider. The two biggest insurers—Medicare and Medicaid—are government entities. Most other insurers are private companies such as Blue Cross and Cigna. As an industry, we are heavily scrutinized for our bills, especially those sent to Medicare and Medicaid. If you are involved with billing or medical record coding, you must become familiar with the following policies:

- Hospital Patient Accounting personnel: PA001 through PA015
- Hospital Medical Record (HIM) coding personnel: HCC001 through HCC011
- Physician billing and coding personnel: PCC101 through PCC502
- Lab personnel: LAB.001 through LAB.011

False Claims and Fraudulent Claims

Fraud laws make it a crime to intentionally bill for more services than we actually provide. Different fraud laws come into play, depending on whether the party paying the claim is a government agency (Medicare, Medicaid, TriCare, etc.) or a private insurance company. Fraud cases are usually prosecuted as criminal cases. Defendants found guilty are often sent to prison.

False claims laws, on the other hand, allow the government to collect civil penalties in cases where intent cannot be determined. The federal False Claims Act was first passed in 1863. It was a way for the U.S. government to bring lawsuits against gun suppliers who sold the Army substandard or nonexistent guns. Moreover, under the False Claims Act, a private citizen may sue on behalf of the government. The government may choose to join the lawsuit or allow the citizen to pursue it alone. In either case, if the citizen's lawsuit prevails, the government gets the proceeds, but the private citizen usually receives around 20% of the settlement as a reward.

Unlike fraud laws, the government does not have to prove intent that we over-billed for services. They only need to show that we billed for claims with a reckless disregard of billing regulations or failure to correct a billing problem. In a healthcare false claims case, the damages can range up to $11,500 per each claim, plus treble damages, plus interest. To learn more about the False Claims Act, including state-specific False Claims Acts, go on-line and visit www.capellahealthcare/ethics.

Ineligible Individuals and Vendors

As a Medicare provider, we are not allowed to hire ineligible persons or contract with ineligible vendors. Ineligible persons or vendors include anyone on the terror watch list, anyone who has defaulted on a federal loan or contract or anyone who has been debarred from the Medicare and Medicaid programs for violating billing and other regulations. As a workforce member, you were cleared prior to being hired. In the case of vendors and contractors, we must check the so-called sanction lists before we contract with them and then quarterly thereafter. See MM001 *Contracting with Ineligible Persons* for more detail.

Environmental Laws

Healthcare facilities routinely handle hazardous materials, such as radioactive isotopes, chemicals, biologicals and pharmaceuticals. A variety of laws and regulations must be understood and followed in order to keep our patients, workforce members and the general public safe. If your job role includes

any potentially hazardous materials, you should read and understand our environmental policies. See policies ENV.001 through ENV.018 for more information.

Political Activities

We live in a great country and enjoy freedom of speech and the right to fair elections. We encourage you to vote and be as active in politics as you like.

As a corporation, our policy is to remain neutral in politics. Therefore, we do not permit "electioneering" on company property. This means you cannot use the company's resources to either support or oppose a candidate; this includes email, internet, photocopiers and phone. See policies GR001 and GR002 for more details.

Responding to Search Warrants

In the event that law enforcement agents present any workforce member with a search warrant seeking to access company material, you should cooperate with the agents and immediately notify the General Counsel's office at (615) 764-3015 and the facility CEO or the house supervisor on call at the time. If for any reason the General Counsel cannot be reached, immediately contact the Ethics Line and report that your facility has been served. Be sure to provide your name and clearly state to the Ethics Line intake dispatcher that this is our established protocol for reporting search warrants. The Ethics Line can be contacted at 1-866-384-4276 or on-line at www.capellahealthcare.com/ethics.

You should ask for identification from the agent in charge of executing the warrant, and ask for a copy of both the search warrant and the affidavit submitted to the court in order to obtain the warrant.

It is our policy to cooperate fully with the agents. It is absolutely critical that no workforce member interferes with the agents in any way during their search or prevents them from accessing anything listed in the search warrant. Obstructing or interfering with a lawful search can constitute a serious offense. When agents attempt to search certain sensitive areas, such as Central Sterile

or Pharmacy, the agents should be advised of the safety concerns and the regulations governing safety in these areas. The agents may ask workforce members questions during the search. Workforce members have the right to either talk to the agents or not to talk to them, except to the extent that it is necessary to talk to them to comply with the warrant.

Agents may take original documents. You should ask for a detailed inventory of the material the agents are taking. They are required to provide a receipt for the articles taken.

For more information, see policy EC.025 *Responding to Search Warrants*.

CHAPTER 6: Reporting Violations & Concerns

Our Code of Conduct requires you to report infractions of our policies if you feel these infractions are going undetected, are the result of collusion, or are being neglected by management. A few examples of infractions or concerns you should report **without delay**, include:

- Patient safety concerns or patient endangerment
- Patient complaints and grievances
- Performance of unnecessary procedures or surgeries
- EMTALA violations
- Billing or coding errors and lack of willingness to correct these
- Harassment or a hostile workplace environment
- Stealing or other criminal acts
- Intentional non-compliance with internal control systems
- Breaches of patient privacy
- Substance abuse or someone who is intoxicated at work
- Failure to safeguard narcotics

HOW TO REPORT INFRACTIONS OR CONCERNS

Always consider reporting infractions first to your **direct supervisor**. If you are not comfortable doing this, the following suggestions will assist you in reporting infractions and concerns in an effective manner.

- Reports of a **human resource** nature, such as sexual harassment or a hostile workplace, should be directed to the facility Human Resources Director.

- Reports involving **breaches of patient privacy** should be directed to the Facility Privacy Officer.
- Reports involving potential identity theft should be directed to the Facility Identity Integrity Officer.
- All other Reports should be directed to the facility or corporate ECO.

THE ETHICS LINE: **1-866-384-4276 or www.capellahealthcare.com/ethics**

The **Capella Ethics Line** is your opportunity to report concerns or infractions that you believe are not being handled properly by the facility or in cases where you are uncomfortable discussing these issues with facility personnel.

Your call will be handled by **EthicsPoint**, an outside firm based in Portland, Oregon. This firm is not affiliated with Capella Healthcare Inc. EthicsPoint serves a variety of major organizations and is staffed 24 hours a day, seven days a week. They will discuss your concern with you and provide the corporate ECO with a written synopsis. You will be given a case number which you can use to call back or login on the internet to get an update on your case. You can also report a concern via the internet by going to www.capellahealthcare.com/ethics.

You **DO NOT** have to give your name and contact information, but if you do, it will allow the Ethics & Compliance Department to contact you for follow-up information.
Neither Capella nor any of its affiliates will make any attempt to determine who you are or where you are if you wish to remain anonymous.
If you remain anonymous, you will have no way of knowing if any follow-up occurs because all investigations, including any disciplinary actions, will be kept strictly confidential.

SUGGESTIONS FOR EFFECTIVE REPORTING

Whether you bring your concern to a person at the facility level, the Capella Ethics Line, or report via the internet, it is a good idea to have all your facts together first.

Gather documentation. This could include:

- Copies of erroneous bills
- Examples of privacy breaches
- Evidence of theft or other illegal acts
- Letters or emails

Organize your account of the situation. Often times, there will be no physical evidence that you can easily obtain to demonstrate a concern. In this case, it is especially important that you organize the details of your concern. Writing out your story often helps you to think through the actual history of your concern. When organizing your facts, be as factual and specific as possible.

ACKNOWLEDGMENT OF THE CODE OF CONDUCT

Every year, Capella requires all employees to sign an acknowledgment confirming they have received the Code of Conduct, understand that it represents mandatory policies of Capella and agree to abide by it. Employees should expect to complete the acknowledgment process annually, as the *Code of Conduct* is a living, changing document. New employees are required to sign this acknowledgment as a condition of employment and must receive *Code of Conduct* training within 30 days of employment.

2013 CALENDAR YEAR ACKNOWLEDGMENT

I have read and understand this Code of Conduct and I agree to follow its policies and practices. I understand I must adhere to the Code of Conduct and the associated Ethics & Compliance policies as a condition of my continued employment. I also understand that it is my responsibility to report any activity or behavior that violates this Code. All potential conflicts of interest are noted below on the disclosure form.

PRINT NAME HERE

SIGNATURE

DATE

DISCLOSURE OF ACTUAL OR POTENTIAL CONFLICTS OF INTEREST

The following actual or potential conflicts of interest are being disclosed in accordance with provisions of this Code of Conduct:
(Note: you must disclose actual or potential conflicts each year by means of this form.)

Ethics Line (866) 384-4276

www.CapellaHealthcare.com/ethics

Appendix

LIST OF ETHICS & COMPLIANCE POLICIES

The material in the Code of Conduct is a brief summary of the Ethics & Compliance policies of Capella Healthcare. These policies can be found on the corporate "Z" drive. Please contact your facility Informations Systems Director for access.

ENVIRONMENTAL (ENV)

ENV.001	Environmental - General
ENV.002	Environmental - Polychlorinated Biphenyls (PCBs) Handling
ENV.003	Environmental - Indoor Air Quality
ENV.004	Environmental - Air Pollutant Emission
ENV.005	Environmental - Asbestos Containing Material (ACM) Management
ENV.006	Environmental - Environmental Due Diligence for Property Transfer
ENV.007	Environmental - Emergency Response
ENV.008	Environmental - Biomedical Waste Management
ENV.009	Environmental - Low-Level Radioactive Waste Management
ENV.010	Environmental - Hazardous Waste Management
ENV.011	Environmental - Fuel Storage Tank Management
ENV.012	Environmental - Waste Oil Management
ENV.013	Environmental - Wastewater Discharge
ENV.014	Environmental - Potable (Drinking) Water Supply
ENV.015	Environmental – Infection Control Risk Assessment
ENV.016	Environmental – Universal Waste Management
ENV.017	Environmental – Management of Lead (Pb) Materials
ENV.018	Environmental – Environmental Self Audit of Facilities

ETHICS AND COMPLIANCE (EC)

EC.001	Policy and Procedure Development
EC.002	Coordination of Ethics Line Investigations
EC.004	Code of Conduct, Effective Date
EC.005	Business Courtesies to Potential Referral Sources
EC.006	Entertainment
EC.008	Approval of tokens of Appreciation in Recognition of Volunteer Efforts from Non-Referral Sources
EC.010	Ethics and Compliance Officer
EC.011	Code of Conduct Distribution and Training
EC.012	Correction of Errors Related to Federal Health Care Program Reimbursement
EC.013	Physician Access to the Internet
EC.014	Records Management
EC.015	Limitations on Gifts to Fiscal Intermediary Employees
EC.016	Ethics and Compliance Program Contracts
EC.017	Notification Regarding Certain Investigations or Legal Proceedings
EC.018	ECO Quarterly Reports

EC.021	Conflict of Interest
EC.022	Education Requirements of the Deficit Reduction Act of 2005
EC.023	Guidelines for Human Photography
EC.024	Use of Social Media by Company Personnel
EC.025	Responding to Search Warrants
EC.026	Monitoring Requirments Regarding Ineligible Persons

EMTALA

EMTALA.001	Medical Screening
EMTALA.002	Stabilization
EMTALA.003	Transfer
EMTALA.004	Signage
EMTALA.005	Central Log
EMTALA.006	Duty to Accept
EMTALA.007	Provision of On-Call Coverage
EMTALA.007	MSE Guidelines for Non-Emergency Patients

GOVERNMENT RELATIONS (GR)

GR.001	Contributions to Political Campaigns
GR.002	Use of Outside Lobbyists

HOSPITAL CODING COMPLIANCE (HCC)

HCC.001	Coding Documentation for Inpatient Services
HCC.002	Coding Documentation for Outpatient Services
HCC.003	Coding References and Tools
HCC.004	Coding Documentation for Inpatient Rehabilitation Facilities and Units
HCC.005	Coding Orientation and Training
HCC.006	Coding Continuing Education Requirements
HCC.007	Reimbursement of Professional Exam Fees for Coding Personnel
HCC.008	Additional Compensation Plans for Coding Personnel
HCC.009	Prohibition of Contingency-Based Coding Arrangements
HCC.011	Certified External Vendors for Coding Reviews and Related Ed.
HCC.001	Outpatient Services and Medicare Three Day Window

HIPAA PRIVACY (HIPAA)

HIPAA.001	Patient Privacy – Program Requirements
HIPAA.002	Privacy Official
HIPAA.003	Patient Privacy – Protection
HIPAA.004	Patient Privacy – Patients' Right to Access
HIPAA.005	Patient Privacy – Patients' Right to Amend
HIPAA.006	Patient Privacy – Right to Request Privacy Restrictions
HIPAA.007	Notice of Privacy Practices
HIPAA.008	Patient Privacy – Right to Request Confidential Communications
HIPAA.009	Patient Privacy – Accounting of Disclosures
HIPAA.010	Patient Privacy – Notification of Breaches of Protected Health Information
HIPAA.011	Standards of Discipline for HIPAA Violations

HUMAN RESOURCES (HR)

HR.001	Background Investigations
HR.002	Equal Employment Opportunity
HR.003	Limitations on Employment
HR.004	Performance Management
HR.005	Non-Discrimination and Non-Harrassment

INFORMATION TECHNOLOGY & SECURITY (IT.SEC)

IT.SEC.001	Information Systems Security
IT.SEC.002	Electronic Communication
IT.SEC.003	PC Software License Management
IT.SEC.005	Information Confidentiality and Security Agreements
IT.SEC.006	Facility Information Security Official
IT.SEC.008	Physician Access to the Facility Information Systems
IT.SEC.009	IT Project Request Approval
IT.SEC.010	Destruction of Computer Equipment, Media and Data
IT.SEC.011	Third-Party Access Procedure
IT.SEC.012	IT Security Risk Assessment
IT.SEC.014	Global E-Mail Distribution List
IT.SEC.015	Network Resources
IT.SEC.017	Network Security
IT.SEC.018	Data Security (Classification)
IT.SEC.019	User Access (Security)
IT.SEC.020	Physicians and Physicians Office Staff (Meditech only)
IT.SEC.021	CPCS Conformance and Monitoring (Meditech only)
IT.SEC.022	Data Encryption

LABORATORY (LAB)

LAB.001	Billing for Hematology Procedures
LAB.002	Billing for Urinalysis Procedures
LAB.003	Organ and Disease Panels
LAB.004	Billing for Outpatient Specimen Collection
LAB.005	Billing for Custom Profiles
LAB.006	Billing for Reference Laboratory Testing
LAB.007	Reflex Tests
LAB.008	Technical Component for Pathology Tests
LAB.009	Billing for Laboratory Services to SNFs
LAB.011	Standard Laboratory Charge Description Master

LEGAL (LL)

LL.001(a)	Physician Relationship Checklist
LL.001	General Statement on Agreements with Referral Sources; Approval Process
LL.002	Professional Services Agreements
LL.003	Physician Recruiting Agreements
LL.004	Physician Equipment or Space Leases
LL.005	Physician Management Services Agreements/Business Office Services
LL.006	Physician Employment
LL.009	Loans and Loan Guaranties

LL.010	Non-Employed Physician Education Expenses
LL.011	Providing Free and/or Discounted Training and Equipment to Referral
LL.012	Physician Access to Vendor Agreements
LL.013	Physician Referral Services
LL.016	Discharge Planning & Referrals of Patients to Post Discharge Providers
LL.018	Professional Courtesy Discounts
LL.020	Physician Relationship Training
LL.021	Physicians Purchasing Items or Services from the Facility
LL.022	Reimbursement of Expenses and Extending Tokens Related to Voluntary
LL.023	Contract Review and Approval Process
LL.029	Facility Marketing and Advertising Practices Relating to Physicians
LL.GEN.001	Waiver of Medicare Copays and Deductibles; Offering of Add. Benefits
LL.GEN.002	Copyright
LL.SEC.001	Securities Trading
LL.SEC.002	Corporate Disclosure Policy

MATERIALS MANAGEMENT (MM)

MM.001	Contracting with Ineligible Persons
MM.002	Vendor Relations
MM.003	Prohibition on Resale of Items Purchased Under Group Purchasing Contract
MM.004	Educational Funding From Vendors
MM.005	Research Grant Funding From Vendors
MM.006	Restocking of Third-Party Ambulances

PATIENT ACCOUNTING (PA)

PA.001	Billing Monitoring for Governmental Payors
PA.002	Ensuring Medical Necessary Services to Medicare Patients
PA.003	Advance Beneficiary Notices (ABNs) for Medicare Outpatient Services
PA.004	Orders for Outpatient Tests and Services
PA.005	Continuing Education Requirements for Billing Personnel
PA.006	Physician Certification and Recertification for Post Acute Services
PA.007	Medicare Outpatient Rehabilitation Services
PA.008	Outpatient Services and Medicare Three Day Window
PA.009	Collection of Financial Information under EMTALA
PA.010	Billing for Outpatient Self-Administered Drugs
PA.011	Confirming and Processing Overpayments
PA.012	Stat Fees, Call Back and Standby Charges
PA.013	Medicare Billing for Investigational Devices and Related Services
PA.014	Billing for Never Events
PA.015	Identity Theft and Patient Mis-Identification

PHYSICIAN CODING COMPLIANCE (PCC)

PCC.101	Compliance – Coding Manual for Requirement in Physician Services
PCC.102	Compliance – Forms, Billing Standards, Provider Documentation
PCC.103	Compliance – Confirming and Processing Overpayments
PCC.104	Compliance – Post Audit Correction of Coding and Billing Errors
PCC.105	Compliance – Physician Practices – Using Third-Party Billing Vendors
PCC.201	Documentation Standards – Physician Practice Medical Records

PCC.202	Documentation Requirements for Time Based Codes
PCC.203	Documentation – Discrepancies Correcting Physician/Provider Documentation
PCC.301	Assignment of CPT (Level 1) and HCPCS (Level II) Codes
PCC.302	Assignment of CPT and HCPCS Level II Modifiers
PCC.303	Assignment of ICD-9 Diagnosis Codes
PCC.304	Assignment of Place of Service Codes
PCC.401	Coding Discrepancies – Process for Resolution
PCC.402	Coding Consultation Services, Documentation and Billing
PCC.403	Coding "Incident To" Outpatient Services for Medicare—Documentation and Billing
PCC.404	Coding Concurrent Care Services, Documentation and Billing
PCC.405	Coding Locum Tenens and Reciprocal Billing – Documentation and Billing
PCC.406	Coding/Reporting of Physician Services Without Direct Face-to-Face Patient Contact for Medicare, Medicaid and Governmental Payors
PCC.501	Electronic Medical Record Code Selection and Prompt Functions
PCC.502	Electronic Medical Record Copy and Paste Functions

QUALITY MANAGEMENT (QM)

QM.001	Regulatory Compliance Notification
QM.002	Licensure and Certification
QM.003	Patient Grievance and Complaint Management

QUALITY MANAGEMENT: RESEARCH (QM.RES)

QM.RES.001	IRB Guidance Policy
QM.RES.002	IRB Protocol—Initial and Continuing Review
QM.RES.003	Informed Consent IRB Review
QM.RES.004	Development of Local Standard Operating Procedures for IRB
QM.RES.005	Adverse Event Review
QM.RES.006	Use of Non-Local, Cooperative and Multi-Institutional IRB
QM.RES.007	Recruitment of Vulnerable Subject Populations

REIMBURSEMENT (RB)

RB.001	Reimbursement Manual
RB.002	Standardized Workpaper Package with Instructions
RB.003	Review of Cost Report
RB.004	Identification of Non-Allowable Costs
RB.005	Adequate Documentation
RB.006	Protested Items
RB.007	Submission of the Medicare Cost Report
RB.008	Disclosure Procedure
RB.009	Error in Reporting
RB.010	Fiscal Intermediary, Carrier and MAC Audits
RB.013	Arrangements with External Consultants
RB.014	Education and Training

TREASURY (TRE)

TRE.001	Medical Staff Funds