



STUDENT TRAINING MODULE

MEDICAL CENTER CLINIC PENSACOLA, FLORIDA

Students are required to:

1. Read all documents included in this Student Training Module*
2. Print and complete the pages in the Student Training Confirmation document:
 - a. HIPAA Privacy Security Agreement and Certification (two pages)
 - b. OSHA Agreement
 - c. Risk Management Agreement
3. Provide the following to the Medical Center Clinic Department Manager prior to or on the first day of your student rotation opportunity.
 - a. Completed documents listed above (4 pages)
 - b. Copy of your driver's license or other form of picture ID
 - c. Proof of the following immunizations. Medical Center Clinic cannot provide you with any of these immunizations.
 - TB Skin Test
 - Hepatitis B Vaccine (You must have received the first immunization, and will be required to provide proof of second immunization if still with us as a student when the second immunization is due.)
 - MMR
 - Rubella Titer

*We recommend that you DO NOT print the Student Training Module due to the number of pages in the module. Only print the Student Training Confirmation document.

**WEST FLORIDA MEDICAL CENTER CLINIC, P.A.
COMPLIANCE, PRIVACY, AND SECURITY AGREEMENT AND CERTIFICATION**

Legibly Print Your First and Last Name Here

Legibly Print the Name of Your Department Here

As a member of the workforce at West Florida Medical Center, P.A. ("MCC") or MCC subsidiary, you are required to sign MCC's Compliance, Privacy, and Security Acknowledgment and Certification Statement (the "Certification Statement") within five (5) days of joining the workforce, and annually thereafter.

Workforce member means:

- Physicians, physician extenders, staff, volunteers, and students,
- Third Parties under the direct control of MCC,
- Whether full-time or part-time, temporary or permanent, paid or not paid

MCC subsidiary includes but is not limited to:

Doctors Call Center, Gulf Region Clinical Research Institute, Gulf Region Postal Center, Gulf Region Surgery Center, Medical Management Services, and MedPro Solutions.

By signing this Certification Statement, you are representing that you have read, understand and agree to the following:

- I am responsible for reading the standards and procedures in MCC's Compliance, Privacy, and Security Manual (the "Manual") and directing any questions regarding the Manual to the Corporate Compliance and Privacy Officer, my supervisor, and/or department manager.
- I understand the Manual has been posted on MCC's Employee Intranet at www.medicalcenterclinic.com.
- I agree to follow MCC's Code of Conduct and all standards and procedures set forth in the Manual and understand that failure to do so may lead to corrective and/or disciplinary action.
- I have read, understand and agree to abide by the following **Confidentiality Statement**:

I acknowledge MCC's Confidentiality Statement applies to all members of the workforce, including but not limited to physicians, physician extenders, staff, volunteers, students, and third parties, whether full time or part time, temporary or permanent, paid or not paid, who are employed by, contracted to, or under the direct control of West Florida Medical Center Clinic (MCC) or any MCC subsidiary.

I acknowledge that MCC has formally stated in the Privacy Standards its commitment to preserving the confidentiality and security of protected health information ("PHI"), whether it is maintained or distributed in paper, electronic, video, verbal, or any other medium or format. I understand that I am required, if I am granted access to such PHI, to maintain its confidentiality and security at all times.

I understand that the following identifiers of a MCC patient or of relatives, employers, or household members of a MCC patient when used individually or collectively by MCC or its subsidiaries constitute PHI:

- 1) Names
- 2) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes, except for the initial three digits of a zip code;
- 3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- 4) Telephone numbers;
- 5) Fax numbers;
- 6) Electronic mail addresses;
- 7) Social security numbers;
- 8) Medical record numbers;

WEST FLORIDA MEDICAL CENTER CLINIC, P.A.
COMPLIANCE, PRIVACY, AND SECURITY AGREEMENT AND CERTIFICATION

Continued from page one...

- 9) Health plan beneficiary numbers;
- 10) Account numbers;
- 11) Certificate/license numbers;
- 12) Vehicle identifiers and serial numbers, including license plate numbers;
- 13) Device identifiers and serial numbers;
- 14) Web Universal Resource Locators (URLs);
- 15) Internet Protocol (IP) address numbers;
- 16) Biometric identifiers, including finger and voice prints;
- 17) Full face photographic images and any comparable images; and
- 18) Any other unique identifying number, characteristic, or code, except as permitted in item two above.

I understand that access to PHI created, received, or maintained by MCC or its subsidiaries in any location is limited to those who have a valid business or medical need for the information. I understand that there are many administrative, physical and technical safeguards in place to protect the privacy and security of this PHI, and that any attempt to bypass or override these safeguards is a violation of federal and state laws and the privacy and security policies of MCC.

I understand that anyone who is authorized to access electronic PHI within MCC's network systems or those of its subsidiaries will be issued a unique user identification (ID) and password, and that any person who knowingly discloses their user ID or password to others, uses or discloses another individual's user ID or password, or accesses any electronic PHI without authorization is subject to disciplinary action, up to and including termination of employment. In addition, I understand that all workforce members of MCC and its subsidiaries must also comply with all applicable Information Technology Security Standards and Procedures.

I understand that approved methods and purposes for access to, uses and disclosures of, and requests for any and all PHI created, received or maintained by MCC or its subsidiaries are limited to those described in MCC's Privacy Standards and Procedures. I further understand that, with the exception of purposes related to treatment, access to, uses and disclosures of, and requests for an individual's health information must, to the extent practicable, be limited to the minimum necessary to accomplish the intended purpose of the approved use, disclosure or request.

I understand that I am not authorized to access or review my own PHI, the PHI of family members, or the PHI of friends or coworkers except where the scope of my job responsibilities requires me to do so or as authorized by MCC policy.

*I understand that any known or suspected violation of an individual's privacy rights as described in MCC's Notice of Health Information Privacy Practices or the confidentiality or security of an individual's PHI must be immediately reported to my supervisor and/or my department manager, **and** to Sharon Hoyle, Corporate Compliance and Privacy Officer.*

- I am not aware of any improper or illegal conduct by MCC or any provider, employee or contractor of MCC which I have not made known to the Compliance and Privacy Officer on or before the date of this Certification Statement.
- I am not aware of any compliance, privacy, or security violations and/or breaches of PHI which I have not made known to the Compliance and Privacy Officer on or before the date of this Certification Statement.

By signing below, I LEGIBLY PRINT FIRST AND LAST NAME HERE hereby certify that I have: 1) read, 2) understand, and 3) agree to abide by the foregoing statements and ALL other Compliance, Privacy, and Security Standards and Procedures.

Physician/Employee Signature

Date

OSHA Training Agreement

I, _____, acknowledge the following:

I have completed Medical Center Clinic's OSHA training for students.

The training reviewed the OSHA Bloodborne Pathogens Statute (29 CFR 1910.1030), the Hazardous Communications Statute (29 CFR 1910.1200), the Florida Administrative Code covering Biomedical Waste (64-E16), or the Alabama Chapter for Biomedical Waste (335-17-3), the Employee Fire and Emergency Statute (29 CFR 1910.38,157) and the TB Guidelines, MMWR-1994:43.

The training provided a plan or process for the following:

- The OSHA Bloodborne Pathogen Statute and the Hazardous Communication Statute.
- The Exposure Control Plan and Hazardous Communication Plan implemented for Medical Center Clinic.
- Medical Center Clinic's Hepatitis B Policy.
- My ***right to know*** what hazardous chemicals I work with.
- How to locate and interpret the various MSDS's for hazardous chemicals.
- Medical Center Clinic's Biomedical Waste Policy.
- What to do in case of an exposure or incident.
- Medical Center Clinic's Fire and Emergency Plan.
- Who are resource managers and what type of information they can provide regarding my job safety.
- Medical Center Clinic's TB Guidelines and Policy.

I agree to abide by Medical Center Clinic's policies and procedures and to inform my manager/supervisor of any OSHA or safety related occurrences involving patients or visitors of which I am aware.

Student Name (please print): _____

Student Signature: _____ Date: _____



RISK MANAGEMENT COMPLIANCE AGREEMENT

I, _____, acknowledge the following:

I have completed the Medical Center Clinic's Risk Management Training for students.

I understand Medical Center Clinic's Risk Management Policy.

I have been informed of my responsibilities and my role in Medical Center Clinic's Risk Management Program.

I agree to abide by Medical Center Clinic's Risk Management procedures and to inform my manager/supervisor and the Risk Manager, Debbie Ray Kings, 474-8625, through the incident reporting system of any occurrences involving patients or visitors of which I am aware.

Student Name (Please print): _____

Student Signature: _____ Date: _____



WELCOME TO THE MEDICAL CENTER CLINIC!

Thank you for choosing to complete a portion of your educational requirements at Medical Center Clinic. Medical Center Clinic is a multi-specialty clinic that is among the largest and most respected of its kind in America. Currently we have over 60 physicians representing almost all the specialties, and over 500 employees made up of nurses, technicians, clinicians, coding and billing specialists, and other support staff. Approximately 500,000 patients are treated here annually. Because of its size and economies of scale, Medical Center Clinic (MCC) has consistently been a pacesetter in obtaining and maintaining equipment and services on the cutting edge of medical progress.

We trust you will have a positive experience at MCC, and wish you great success in your educational endeavors.

GOVERNANCE:

Medical Center Clinic is governed by a seven-member physician Board of Directors, elected annually on a rotational basis by the Corporate Physician Shareholders. It is the function of Medical Center Clinic's Administrative Staff to assure that the Corporation operates consistent with Board policy.

HISTORY:

Medical Center Clinic was founded in 1938 in Pensacola, Florida. Six local physicians, each in a different specialty, chose to organize themselves into the Medical Center Clinic. That sextet included Drs. C.C. Webb, E.V. Anderson, W.P. Hixon, C.C. Heinberg, L. Sharp, and A.E. Mock.

The Medical Center Clinic's first home was a former downtown residence, which also came to house selected diagnostic equipment and -especially important- a professional processing of patient documents. By 1945, the practice had increased 50% and MCC's home was enlarged and modernized. By 1954, MCC outgrew its original facilities and built a new structure half a mile away. Within a decade MCC had outgrown that building as well.

Recognizing the growth of Pensacola's population northward Medical Center Clinic joined forces with Hospital Corporation of America (HCA) to bring West Florida Hospital to the community. In 1975, MCC moved to its current 11-story home on North Davis Highway, next door to the hospital.

In 2008 the MCC campus name was changed to Gulf Region Campus, and includes the 11-story Gulf Region Tower, Gulf Region Radiation Oncology Center, and Ambulatory Surgical Center.

OUR CORE PURPOSE:

Be the premier provider of compassionate, quality healthcare.

OUR CORE VALUES:

- Provide exceptional service with integrity.
- Foster innovation and resource development.
- Promote a unified team of healthcare professionals.
- Attract the highest qualified medical and support staff.
- Maintain ethical balance of corporate and individual visions.

OUR CORE VISION:

Be independently recognized as the most sought after provider of coordinated healthcare by patients, physicians, employees, hospitals, and carriers.

OUR SERVICE STANDARDS:

- Make first impressions positive ones.
- Maintain a professional appearance.
- Demonstrate a positive attitude.
- Demonstrate a team attitude.
- Make lasting impressions positive ones.

OUR TEN FOOT RULE:

The Ten Foot Rule demonstrates MCC's culture. Everywhere you go, and in everything you do, if someone gets within 10 feet of you, it is your responsibility to speak to that person. It doesn't matter who – patient, physician, coworker, visitor, vendor, etc. – where, or when; you have an obligation to smile, say hello, or ask if that person needs help. Don't wait for the other person to speak to you, take the initiative. If they need help, help them. Don't give directions and walk off, take them to their destination. These small gestures of hospitality mean a lot!

Every member of the MCC team - students, volunteers, employees, and physicians - contributes to the health and success of MCC.

OUR TOBACCO FREE POLICY:

Medical Center Clinic has a Tobacco Free Policy. The use or sale of all tobacco products (cigarettes, including electronic; cigars; pipes and smokeless tobacco) is prohibited on all MCC premises, including parking lots and grounds associated with MCC premises (owned or leased). The policy applies to all individuals in MCC buildings and/or on MCC premises. The policy does not mandate anyone discontinue tobacco product use entirely; it only prohibits tobacco product use on MCC premises.

Support Services

The Medical Center Clinic provides many administrative services ranging from technologically advanced information systems to billing services that are showcased throughout the country. This section provides an overview of these high quality administrative services.

Medical Center Clinic Administration

A seven member Board of Directors, elected annually on a rotational basis by the Corporate Physician Shareholders, governs Medical Center Clinic. It is the function of Medical Center Clinic's Administrative Staff to assure that the Corporation operates consistent with Board policy. Administration gives guidance and recommendations to the Board and to Shareholder and Associate physicians on a number of complex issues, and manages the areas of Finance, Marketing, Information Systems, Human Resources, Operations, and Quality Assurance.

It is the goal of Administration to provide physicians with a working environment that allows the physician to focus on the practice of medicine but still have the opportunity to be involved in the decision making process affecting his or her practice. It is also Administration's responsibility to provide physicians with information that gives the physician insight into details of his or her practice. With this information, physicians are able to be actively involved in the future direction of Medical Center Clinic.

Corporate Compliance

In 1998 Medical Center Clinic established the Compliance Department to serve as a resource for Medical Center Clinic healthcare providers and employees in understanding and complying with the laws, rules, and regulations that govern the documentation, coding, and billing of healthcare services. The Compliance Department is overseen by our Executive Director. Our Corporate Compliance and Privacy Officer is a certified physician coder (CPC) through the American Academy of Professional Coders and is certified in Healthcare Compliance (CHC) through the Health Care Compliance Association. The CHC designation affirms an individual has knowledge of relevant regulations and expertise in compliance processes sufficient to assist the healthcare industry to understand and address legal obligations, and promote organizational integrity through the operation of effective compliance programs. The Corporate Compliance and Privacy Officer can be reached at ext 8246.

Corporate Marketing

The Corporate Marketing Department provides internal and external marketing services for the Medical Center Clinic and all of its business entities. The Corporate Marketing Department assists the providers of the Medical Center Clinic in the promotion of their practices. With the assistance of a professional marketing firm, the marketing staff creates marketing plans for providers which include multiple media options. The Corporate Marketing Department also works to enhance the image and promote the organization as a whole. Some areas of responsibility include updating the local telephone directory, improving both the interior and exterior building signs, coordinating employee social events, managing the MCC website, and coordinating organizational advertising campaigns. The VP of Corporate Marketing & Strategies can be reached at ext 8202.



The Courtyard Café is located on the first floor of Gulf Region Medical Tower and is open to patients, visitors, and employees. The Café is open from 7:00am to 4:00pm, and offers a selection of coffee beverages, frozen fruit beverages, and snacks. Vending machines and tables/chairs are available. The Café accepts cash, Visa, Mastercard, American Express, and Discover Card, and gift certificates are available. Call 969-2233 (ext 2233) to speak with a Courtyard Café employee.

Electronic Medical Records (EMR)

The Medical Center Clinic enjoys the benefit of a state-of-the-art Electronic Medical Record System, gathering and storing patient record information to serve its patients and health care providers. The system is built on software from Physician Micro Systems, Inc., of Seattle, Washington, and stores record information back through 1994, when the system was first implemented. The system is the exclusive medical record for virtually all patient encounters, and provides physicians and health care providers with access to progress notes, nurse notes, laboratory and ancillary study data, including data from encounters and ancillaries from West Florida Hospital. All chart entries are made via the EMR, and each physician and nurse has access to the system via their dedicated desktop workstation, which also provides other resources such as e-mail, registration, billing, and scheduling. More recent upgrades include document imaging to handle incoming correspondence and data from outside institutions, not otherwise available in electronic format, and the option of direct entry into the EMR for providers. The Health Information Management Department, which is responsible for the integrity of our EMR, can be reached at ext 8774.

Employee Intranet

MCC maintains an Employee Intranet (EI), which serves as the primary corporate communication tool and a reference library for all employees. Information available on the EI includes: the Employee Handbook, benefit overviews and forms, employee social events, community involvement events, employee recognition such as the Core Values Award, patient and employee incident/injury forms, Corporate Compliance policies, HIPAA policies, Risk Management policies, and the bi-monthly corporate newsletter: MCC Operations. Any problems utilizing the EI, or any suggestions regarding information available on the EI, should be directed to 969-2692 (ext 2692).

Facilities Management and Maintenance

The Facilities Department is responsible for the management of our buildings. The team responds to emergency situations such as a burst pipe, non-emergency situations such as replacement of light bulbs, and performs routine maintenance and checks of all the physical plant operations. The Facilities Department is involved in all new and renovation construction projects, ensuring MCC standards are maintained. Non-emergency maintenance requests should be presented to each department manager who in turn will submit the requests to the maintenance department via a computerized work order system.

Finance Department

The Finance Department is responsible for accounts payable, payroll, benefits, 401(K), and financial statement reporting, and is staffed with high caliber, seasoned accounting professionals including CPAs. Accounts payable expenses are directed to the appropriate physician and/or department at the time invoices are processed for payment. Direct and indirect expenses incurred through the operation of the business, from the electric bill to supply costs to employee payroll, are charged to each physician as an expense in the calculation of their monthly compensation.

Guest Services

Guest Services provides transport services, general information about MCC, and directions to our patients as they enter our building. A Door Greeter welcomes patients and ascertains if a patient needs transport; if so another member of the guest services team will transport the patient to a department within Gulf Region Medical Tower or the Surgery Center building.

When a patient's visit is concluded the department contacts guest services via pager number 5051 for the patient to be transported back to the lobby area. Guest Services can be reached at ext 5050.



Patient shuttles traverse the patient parking areas throughout the day, transporting patients to and from their vehicles to the front door of Gulf Region Medical Tower and the Surgery Center. Our shuttle drivers actively look for patients who may be waiting for the shuttle; patients can also contact the shuttle driver by calling 291-2646. Each parking area is labeled with a color code, number and letter to help patients direct the shuttle driver to their vehicle.

Human Resources

The Human Resources Department offers a multitude of services to physicians, managers, and employees, to include development and administration of HR-related corporate policies, recruitment and retention, and wage and salary administration. The department coordinates New Employee Orientation and other onboarding and training activities. A member of the HR Department focuses on employee health issues, such as immunizations, drug screens, medical leave requests, and workers' comp accidents/injuries. The department maintains an open door policy and encourages employees to bring any concerns to their attention. The department reports to Sr VP, Administration. The Sr VP, Administration is a nationally certified Professional in Human Resources (PHR). The Human Resources Department can be reached at ext 5308 if calling from an MCC telephone.

Information Services

Management Information Services (MIS) offers state-of-the-art information management. MIS staff provide a high level of technical participation and interaction with end-users so that all requirements and expectations are met to achieve maximum productivity. MIS Help Desk personnel are available to assist with computer or telephone problems at ext 8010.

Managed Care

The Managed Care Department is a central depository for payor agreements and information on how various insurance programs operate, thus eliminating the need for each MCC provider to review each payor contract. This allows our providers to concentrate on patient care with the assurance that agreement terms are standard for all departments and affords provider offices a resource related to obtaining prior authorizations when necessary. The Managed Care Department can be reached at ext 2160.

MedPro Solutions, LLC

MedPro Solutions is responsible for billing and collection activities for Medical Center Clinic providers. MedPro Solutions employs certified physician coders and uses a front-end claims scrubber (Claims Editor) to ensure claims are coded appropriately before being sent to an insurance carrier for processing. The true measurement of the account receivables (AR) is the management of AR days. Medical Center Clinic AR days are typically less than 50. MedPro Solutions can be reached at ext. 8100.



Risk Management

Medical Center Clinic has a very active risk management program, from solid policies and procedures actively monitored by a Risk Management Committee to a very advanced Electronic Medical Record system. The risk management team includes a Senior Administrator, a manager who is a RN and Certified Risk Manager in the State of Florida, a Medical Director who also acts as the Chairman of the Professional Practices Committee, and finally, a legal firm that has represented Medical Center Clinic for almost two decades. This key team combined with an organization-wide approach to Risk Management has resulted in a safe environment where quality patient care is practiced in a manner that significantly reduces the organization's exposure to malpractice losses. The Risk Manager can be reached at ext 8625.

Specialties

The following is an overview of the many specialty services available at Medical Center Clinic.

Adult and Internal Medicine

The Department of Adult and Internal Medicine provides comprehensive care to adult patients including health maintenance examinations, diabetic and hypertension treatment, removal of skin lesions and even offers several laboratory services within the office. The Adult and Internal Medicine Department can be reached at ext 8385.

Allergy and Immunology

Located at 2114 Airport Blvd. Suite 1500, in the Corporate Woods office complex, the Allergy and Immunology Department treats all allergic conditions, such as asthma, allergic rhinitis, chronic urticaria, food allergy, atopic dermatitis and drug reactions. Allergic skin testing for inhalants, foods, penicillin, insulin and local anesthetics is available as well as pulmonary function testing for obstructive lung disease to determine if patients with questionable history and physical examination have asthma. The Allergy Department can be reached at 969-2340.



Business Health Services/Occupational Medicine

Business Health Services is a comprehensive occupational and industrial medical services program. Services to business and industry include physical examinations for pre-placement, periodic physicals, DOT, OSHA Mandated, Regulatory and Executives. Injury evaluation and treatment, Non-NIDA Drug Screening, NIDA and HRS certified Drug Screen Specimen collection, and individualized development of corporate occupational medicine program are also available. Business Health Services can be reached at ext 8572.

Dermatology

The physicians of the Dermatology & Laser Center diagnose and treat all diseases of the skin. Various modalities are utilized for treatment of benign and malignant skin growths.

These include cryosurgery, surgical excision, and MOHS micrographic surgery. A CO2 laser is present within the department and is utilized for treatment of selected cases. A full time PUVA psoriasis treatment center is available for treatment of psoriasis and other skin conditions with both UVA and UVB actinotherapy. The department offers latest laser treatments serving both cosmetic and diagnostic patients. These treatments include N-Light, IPL, Thermage, Hair Laser, Rhytec Resurfacing, Microdermabrasion, and Diolite. DermaAscreen skin mapping is also available. Dermatology can be reached at ext 8386.



Skin Care Center

The Skin Care Center, under the direction of Dr. Kevin Welch, carries products for correction of hyperpigmentation, sun damage, dead skin, fine lines, dark circles, spider veins, and broken capillaries. These products can only be sold through a physician's office. The Center is staffed by a licensed aesthetician that is experienced in the application of make-up and the use of various cleansing regimens.



ENT/Facial Plastic Surgery

ENT specializes in the diagnosis and medical and surgical management of diseases of the ear, throat, head and neck. Department members have extensive experience in head and neck oncology, pediatric otology, neurotology, and endoscopic sinus surgery. In addition the physicians perform facial plastic surgery of facial defects and skin cancer and reconstruction after maxillofacial trauma, as well as cosmetic facial surgery. Treatment for sleep disorders specifically relating to obstructive sleep apnea, including the backup of a certified sleep laboratory, is also available. ENT/Facial Plastic Surgery can be reached at ext 8320.

Hearing Center (Audiology)

The Hearing Center is a community-care facility that is dedicated to providing quality, comprehensive care for all hearing health needs. Located in the ENT department, the group adheres to a clinical otoaudiological team approach for dispensing hearing aids. A physician provides ear examinations and an audiologist administers an audiological evaluation. The Hearing Center also provides a wide variety of audiological services, including industrial audiological monitoring, hearing aid evaluations and dispensing, hearing aid repairs for all makes and models, and special audiological diagnostics, including neurodiagnostic auditory brainstem response tests, threshold-seeking auditory brainstem response tests, and electrocochleography. The Medical Center Clinic Hearing Center employs state-licensed, nationally certified masters-level audiologists to provide all hearing related services. The Hearing Center can be reached at ext 8328.



Gastroenterology

The Gastroenterology Department provides modern diagnostic and therapeutic assessment of diseases of the digestive system, including the esophagus, stomach, small intestine, colon, liver, pancreas, and biliary tract. Some areas of special interest are diseases of the liver, motor disorders of the gastrointestinal tract, inflammatory bowel disease, absorptive disorders, nutritional support and the use of diagnostic and therapeutic endoscopy and laparoscopic diagnostic techniques. The Gastroenterology Department can be reached at ext 8428.



Gulf Region Radiation Oncology Center

Medical Center Clinic's Radiation Oncology physicians see patients at the Gulf Region Radiation Oncology Center (GRROC) located on the campus. GRROC provides a full range of radiation therapy services including external beam treatments with both photons and electrons, low and high dose-rate brachytherapy implants of both the intracavitary and interstitial variety, and intraperitoneal radiophosphorus when indicated. GRROC can be reached at ext 8264.

Infectious Disease

The Department of Infectious Disease offers consultations in the diagnosis and management of infectious diseases in all body systems, including systemic fungal disease, endocarditis, acquired immune deficiency syndrome (AIDS), endophthalmitis and complicated postoperative infections. Parasitic and other tropic infectious diseases are also evaluated and treated. In addition, the Department has an outpatient infusion therapy clinic, which administers antibiotics and other drugs to patients in a convenient non-threatening environment. The Infectious Disease department can be reached at ext 8187.

Neurology

The Department of Neurology provides evaluation and treatment of all neurological disorders in both the inpatient and outpatient setting. Physicians in the department are fellowship trained and/or board certified in the subspecialties of Neurophysiology, Epilepsy, and Sleep Medicine. All electrodiagnostic studies are available including electroencephalography (EEG), electromyography (EMG) and visual, auditory and sensory evoked potentials. Full neuroradiology services are available on campus. Both digital and conventional angiography are routinely performed, as well as noninvasive assessment in the carotid and vertebral arteries. A sleep lab managed by the department is now available to evaluate sleep disorders. Neurology can be reached at ext 8353.



Neurological Psychology

The Department of Neuropsychology provides evaluation and counseling for patients with neuropsychological disorders in both the inpatient and outpatient setting. This field of study is concentrated on the brain and its functions. Neuropsychological testing is designed to determine the brain's capacity with respect to short and long term memory, abstract reasoning, attention, concentration, executive functioning, motor skills and other cognitive and psychological factors. Counseling is also provided to patients with head injuries and anxiety disorders. Neuropsychology can be reached at ext 8353.

Neurosurgery

The Department of Neurosurgery has an office on this campus in the Gulf Region Medical Tower. The Department offers extensive experience in pituitary tumors, eighth-nerve tumors, carotid artery surgery, peripheral nerve surgery, surgical treatment of trigeminal neuralgia and surgery of cervical, lumbar and thoracic discs. Physicians perform surgery at both Sacred Heart Hospital and West Florida Hospital. The Department of Neurosurgery can be reached at 969-2226 (ext 2226).



Ophthalmology

Fellowship trained surgeons provide specialty care in the areas of retina, ocular plastics, glaucoma, cornea and pediatrics. The facility contains a fully equipped surgery suite and laser center, as well as a complete ophthalmic diagnostic department. Services range from routine ocular examinations to the most complex diagnostic and therapeutic ophthalmic procedures. The facility is devoted to providing patients with cost effective, convenient, state of the art and ophthalmic care under one roof. The Ophthalmology Department can be reached at ext 8436.



Orthopaedic Surgery

Medical Center Clinic's Department of Orthopaedics is a group of board certified physicians providing comprehensive orthopaedic care with an emphasis on complex subspecialty surgical treatment of the musculoskeletal system - bones, joints, ligaments, muscles, nerves and related structures - whether caused by accident or disease. All of our specialists have extensive experience in both adult and pediatric surgery, including trauma, re-constructive joint surgery, and sports medicine. Orthopaedic Surgery can be reached at ext 8300.



Pain Management

The Department of Pain Management is committed to the treatment of musculoskeletal pain disorders using a multidisciplinary approach, including interventional pain management procedures. The procedures include lumbar radio frequency, selective rhizolysis, lumbar discography, percutaneous lysis of epidural adhesions, transforminal epidural steroid injections, hypogastric plexus block, celiac plexus blocks and lumbar sympathetic blocks. The Pain Management Department can be reached at 969-2222 (ext 2222).

Physical/Rehabilitative Medicine

The Department of Physical Medicine and Rehabilitation offers consultations for evaluation of physical conditions and disabilities such as arthritis, neck pain, back pain, cerebrovascular accident, head and spinal cord injury, neurological and muscular diseases, amputees, peripheral nerve injuries as well as evaluation for causes of chronic pain. Treatment emphasizes the use of non-invasive techniques in a coordinated manner with the departments of Physical Therapy, Occupational Therapy, Speech Therapy, and Recreational Therapy. Other treatment includes pharmacological agents, physical modalities and adjuvant therapies such as transcutaneous electrical nerve stimulation. Instructions in home programs, prescription supports, orthoses, prostheses, wheelchairs and other assistive devices and appliances are available. The Physical/Rehabilitative Medicine Department can be reached at 969-2563 (ext 2563).

Plastic Surgery

The Department of Plastic, Reconstructive & Cosmetic Surgery is dedicated to improving the quality of patients' lives through the restoration of form and function. Patients requiring reconstructive and cosmetic surgery are evaluated and treated on both an inpatient and outpatient basis. Reconstructive surgery includes the treatment of burns, malignancies of the skin, and reconstruction of the breast and body surface. The Department of Plastic, Reconstructive & Cosmetic Surgery can be reached at ext 8333.



Rheumatology

The Rheumatology Department provides full diagnostic evaluations of degenerative or inflammatory joint and muscle diseases. Evaluation includes complete medical examinations, laboratory testing including ANA profiling, blood, synovial and crystal analysis; bone and joint scanning; and muscle, joint and skin biopsy with immunofluorescent studies.

Appropriate orthopedic, neurosurgical and psychiatric referrals are available if needed via close liaison with these departments. Similarly, psychiatric referral and stress management is available for chronic pain syndromes. Full physical and occupational therapeutic modalities are also available. Rheumatology can be reached at ext 8387.



Urgent Care

The Department of Urgent Care offers patients an opportunity to see a physician quickly. Patients are seen the same day and usually within 30 minutes of arrival. Urgent Care has extended hours including weekends and some holidays. Urgent Care physicians consult with or refer patients to Medical Center Clinic specialists as appropriate. Urgent Care can be reached at ext 8572.

Urology

The Department of Urology provides state-of-the-art treatment, evaluation, and consultation for all pediatric and adult urological problems including corporal shockwave lithotripsy, laser prostatectomy, radial prostatectomy, and penile prosthesis for impotency. Laparoscopic and robotics-guided procedures provide for the latest techniques in minimally invasive urological surgery. The Urology Department can be reached at ext 8398.

Ancillary Services

Medical Center Clinic patients benefit from having many ancillary services on our campus.

Ambulatory Surgery Center

The Ambulatory Surgery Center (ASC) at Medical Center Clinic is a multi-specialty outpatient surgery center dedicated to providing same-day procedures in a warm and caring environment. The ASC is the most convenient and cost-effective setting for providing outpatient surgical care. Unparalleled professionalism, quality and safety are important reasons why patients and physicians alike choose the ASC. Patient satisfaction is one of our hallmarks, with patients reporting an overall 98 percent satisfaction rate. The ASC also boasts faster recovery times and lesser costs than associated with the traditional hospital outpatient setting.

The ASC is a state licensed 26,000 square foot facility located on the first floor of Building 2 and performs over 10,000 procedures each year. It consists of 6 state-of-the-art operating rooms, a gastroenterology suite, a dedicated special procedure room for pain management procedures, pre-operative and recovery areas and a large, comfortable waiting area for family and friends. In addition to gastroenterology and pain management procedures, the ASC performs procedures in the specialties of ophthalmology, ENT, urology, plastic surgery, orthopedic surgery, and general surgery.

Certified by the Accreditation Association for Ambulatory Healthcare, Inc., the ASC successfully meets and exceeds a wide range of demanding clinical, operational and quality standards.

To call the ASC surgery scheduling department, dial 969-2122 (or extension 2122), and the front desk/admissions department can be reached by dialing 969-2121 (or extension 2121).



Diagnostic Imaging



The Diagnostic Imaging Center is conveniently located on the first floor of the Gulf Region Medical Tower, next to the Laboratory. Services provided include MRI (Magnetic Resonance Imaging), CT (Computerized Tomography) and Digital Radiography. All procedures that are performed are stored digitally within a PACS system. Images and reports are made available to MCC physicians via 24-hour web access, as well as in film printed version or on compact disk. Report turnaround is guaranteed within 24 hours of performing a procedure. For assistance or to schedule procedures for a physician, contact the Diagnostic Imaging Department at 969-2134 (ext 2134).

Gulf Region Clinical Research Institute

Gulf Region Clinical Research Institute provides full service phase II-IV clinical research trials. Gulf Region Clinical Research Institute is located on the sixth floor of the Gulf Region Medical Tower, across from the Infectious Disease department. GRCRI works with many providers and departments within MCC. For questions or assistance contact GRCRI at 969-2560 (ext 2560).



Laboratory



The Medical Center Clinic Laboratory provides a full range of services from routine blood work to immunological to tissue type testing. The Laboratory is also conveniently located on the first floor of the Gulf Region Medical Tower, next to the Diagnostic Imaging Center. The Laboratory can be reached at ext 8301.

Optometry/Optical Shop

Medical Center Clinic operates a full-service optical shop on the first floor of the Medical Center Eye Institute/Surgery Center Building. It offers eye examinations, and a wide selection of frames, lenses, contact lenses, repair services and complimentary adjustments. Discounts are provided to Medical Center Clinic employees and physicians. The Optometry/Optical Shop can be reached at ext 8220.



Physical Therapy

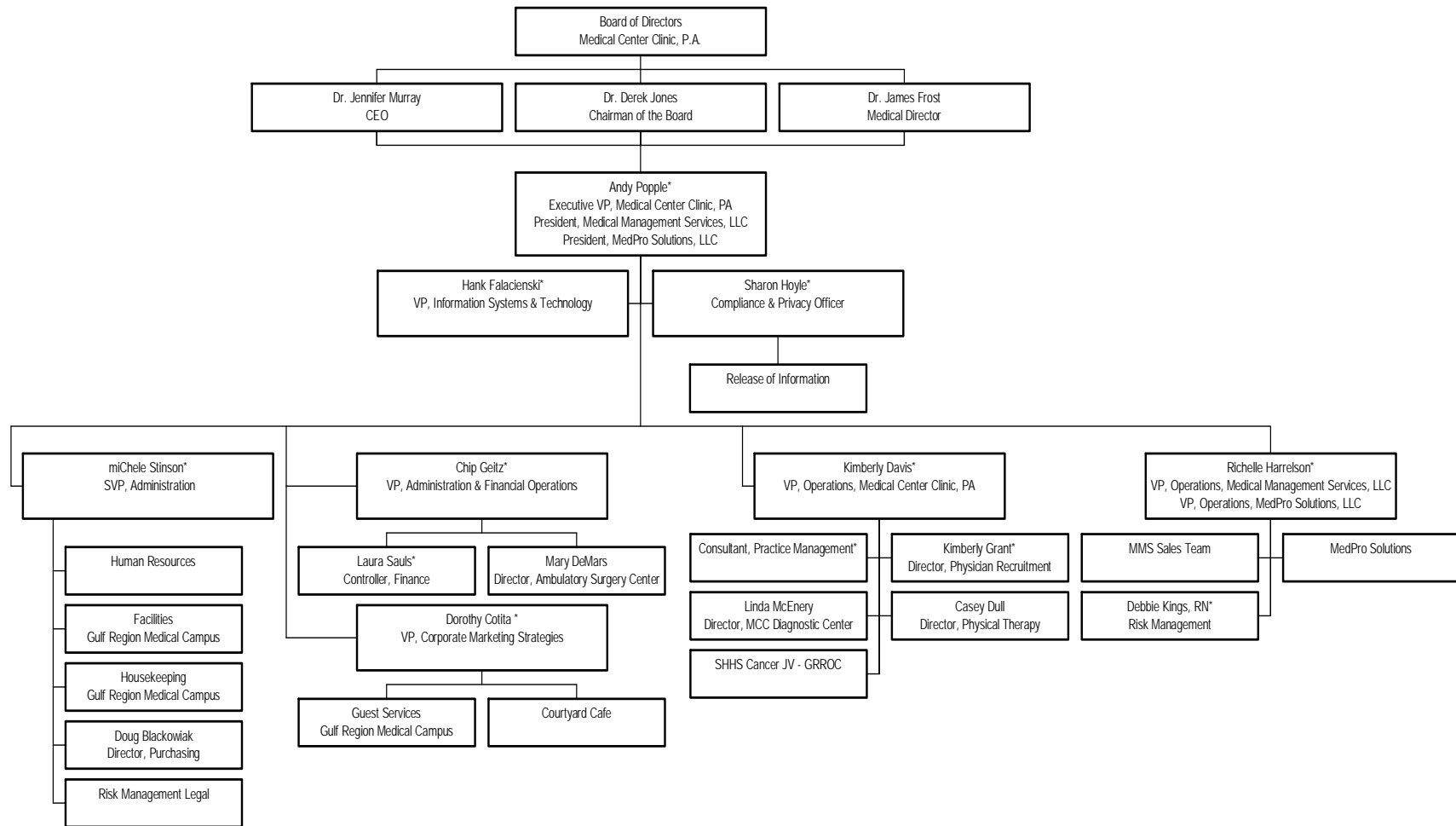
Medical Center Clinic operates a full service Physical Therapy department for its patients. Located on the first floor of the Medical Center Eye Institute/Surgery Center Building, our Physical Therapy service provides professional individualized treatment with quality outcomes for patients and physicians. Our therapy staff is skilled in the evaluation and treatment of many different types of injuries and utilizes a variety of technologies in the rehabilitation process. The Physical Therapy Department can be reached at 969-2600 (ext 2600).

Walgreens' Pharmacy

For the convenience of patients and staff, a Walgreens' pharmacy is located just inside the Gulf Region Medical Tower's main entrance on the first floor. It operates Monday through Friday from 8:30 a.m. to 6:00 p.m. A multitude of services are offered, including delivery and mail-out service, patient medication counseling, over-the-counter products, and special product ordering. The Walgreens' pharmacy can be reached at ext 8223.



Corporate Organizational Chart 2014



*Medical Management Services

Medical Center Clinic Parking Policy

Effective as of January 1, 2009

Patients: Patients are permitted to park anywhere on campus.

Providers: Providers have gated parking at the rear entrance of the Gulf Region Medical Tower. Please contact Practice Management to obtain access to these parking areas.

Volunteers: Volunteers are allowed to park anywhere on the Gulf Region Medical campus, except a Disabled slot unless they have a State issued disability placard or tag.

Employees, Tenants, Students, Contract and Temporary Workers: Other staff working in the Gulf Region Medical Tower and the ASC Building are required to park across Davis Highway, in the parking lot at the corner of Davis Highway and Johnson Street.

Non-Approved Parking Lots: West Florida Hospital parking lots, other than the one across Davis Highway are not approved parking areas for any employees, volunteers, tenants, students, contract or temporary workers who work in the Gulf Region Medical Tower or the ASC Building. West Florida Hospital staff are not permitted to park in MCC campus parking.

Parking Policy Violation Results: The parking policy violator's vehicle will be automatically booted (see picture). The cost to release the vehicle is \$50, and payment must be received before the boot will be removed. MCC employees will have a copy of the incident placed in their personnel file and sent to their department manager.



Exceptions to the Above Stated Parking Policy:

Parking Permits: Permit parking is by the Cancer Institute on the Davis side of the lot all the way around the back to the front edge of the Cancer Institute on the University Parkway side. There is a yellow strip that indicates where permit parking begins. The following employees may obtain a permit to park in the permit parking area:

- 1) Members of MCC's Management Team.
- 2) Staff who support off-site locations on a regular basis.
- 3) Cancer Institute staff.
- 4) Temporarily disabled staff.

A parking permit is required to park in the permitted area. Parking permits must be requested by the staff member's manager.

Temporary Disability Permits: On-campus parking permits for a temporary disability must be requested by the staff member by contacting the Employee Services Specialist in Human Resources. Temporary disability permits are approved for a limited period of time and must be supported by medical documentation signed and dated by a treating provider.

Permanent Disability Permits. Staff members with a state issued disabled parking permit are required to provide the Employee Services Specialist in Human Resources with a copy of the permit paperwork signed by a provider and stamped by the DMV, along with a copy of the placard that hangs from the rearview mirror. If they have a tag with the wheelchair insignia, then a copy of the permit paperwork and the vehicle registration is required.

Tips for Great Customer Service

- ❖ **Patient Contact Rule:** Always make eye contact, smile and give a greeting. Use the patient's name when possible. Acknowledge the patient and have positive body language.
- ❖ **Giving Directions:** Escort patients to their destination whenever possible; at the very least take the first five steps with them to make sure they are walking in the correct direction and provide them with specific landmarks. Avoid short answers and pointing.
- ❖ **Answering the Telephone:** Give a greeting (good morning, afternoon, evening), say the name of your department name and your name, followed by "How may I help you?" Smile when you answer the phone. Use the patient's name, if possible, during the conversation. Answer the phone promptly (strive for within three rings) and do not automatically place the caller on hold. Return follow-up calls by the end of the business day.
- ❖ **Name tag and work attire:** Your work attire must be clean, neat, and pressed since this is your first impression to the patient. Follow your department's dress code and your position's dress code. Always wear your name tag. Familiarize yourself with MCC's Emergency codes and Telephone Numbers, which are located on the back of your name tag. The telephone number for calling an MRT (medical response team) is 3911.
- ❖ **Eliminate "reality intrusions:"** Avoid conversations, internal problems, personal phone calls, etc., in the presence of our patients. Make personal phone calls during a break or at lunch, away from patient areas. A patient should never feel that you are placing personal business over them. Be aware of how small the waiting room is and that patients can overhear conversations.
- ❖ **Patient problems:** Take complete ownership of a patient's problem until resolution. Make sure that the patient has everything they need, or are in the correct department, before you excuse yourself.
- ❖ **Positive attitude:** Use positive words: "I'll be happy to," "Certainly," "My pleasure," "Yes," "Of course". Always have an alternative to the answer "no." Always speak positively of MCC physicians, Doctor's Call Center, MedPro, MCC as a corporation, managers, and co-workers; be a good ambassador. Speak positive of all issues and do not let situations frustrate you.
- ❖ **Patient names:** Use the patient's name whenever possible. Address patients by their full complete name. Use Mr., Mrs., and Miss. Refrain from referring to patients as "honey", "sweetie", "baby", "darling", etc.
- ❖ **Be proactive:** Take care of people by showing the initiative to anticipate and fulfill their needs. If they look like they need assistance, offer to help.
- ❖ **Be knowledgeable:** Understand all parts of your job so that you always contribute 100% to servicing patients. Know the specifics of your job.
- ❖ **Environment:** Uncompromising levels of cleanliness are the responsibility of every employee. Clean as you go and maintain a safe and neat area. Potential dangers, such as water on the floor, should be addressed as soon as possible to avoid injuries. Contact Doctor's Call Center with location of hazard.
- ❖ **Fond farewell:** Use phrases like "Thank you for choosing us to be your healthcare provider," or "Thank you for trusting your care to us." Be genuine.

Tips for Communicating With People Who Have Hearing Loss

Successful communication requires the efforts of all people involved in a conversation. Even when the person with hearing loss utilizes hearing aids and active listens, it is important that others involved with the communication process consistently use good communication strategies.

- ❖ **Face the patient directly**, on the same level and in good light. **Never** turn your back to the patient. Don't look at the chart or the prescription you are writing. Look at the patient.
- ❖ Avoid covering your mouth with your hands or paper.
- ❖ **Speak clearly, slowly, distinctly, but naturally, without shouting or exaggerating mouth movements.** Shouting distorts the sound of speech and may make speech reading more difficult.
- ❖ **Say the person's name or get his/her attention before talking.** This gives the listener a chance to focus attention and reduces the chance of missing words at the beginning of the conversation.
- ❖ **Slow down**; avoid talking too rapidly or using sentences that are too complex. Pause between sentences and phrases, and make sure you have been understood before continuing.
- ❖ **Position yourself properly**; ask if they hear better out of one ear or the other.
- ❖ **Reduce environmental noise.**
- ❖ **Never speak directly to their ear**, this distorts sound and hides visual cues.
- ❖ **Rephrase instead of repeating.**
- ❖ **Give more time to respond**, as processing takes longer.
- ❖ Have the patient **repeat information back to you** to confirm that they understood your message.
- ❖ **Provide pertinent information in writing**, such as appointment times, etc.
- ❖ Recognize that everyone, especially the hard of hearing, has a harder time hearing and understanding when ill or tired.
- ❖ Recognize that all of these strategies and hearing aids may still not be enough. Some people will have difficulty understanding speech no matter what...**BE PATIENT.**

Work Environment Policies

It is the policy of Medical Center Clinic that team members maintain a working environment that encourages mutual respect, promotes civil and congenial relationships among team members and is free from all forms of harassment and discrimination. Team members have an obligation to report any concerns/issues regarding harassment, discrimination, or workplace violence to their manager, or to the Sr VP, Administration if they do not feel comfortable talking with their manager about the issue. If the Sr VP, Administration is not readily available, you can contact another member of the HR Department, Risk Management, Compliance & Privacy Officer, or anyone at the senior level of management for assistance.

❖ Professional Conduct Policy

All MCC team members are expected to conduct themselves in a manner that reflects a high standard of performance and shows consideration and respect to others. Conduct that interferes with company operations, brings discredit, and/or is offensive to patients or other team members will not be tolerated and may result in termination of team member status.

❖ Harassment Policy

MCC prohibits harassment of its team members by other team members and will take immediate and appropriate action to prevent and to correct behavior that violates this policy once notified of a violation. MCC also strives to protect its employees from any form of harassment by third parties, including customers and vendors. If you have any questions or concerns about what may or may not be deemed as harassment, including sexual harassment, contact the Sr VP, Administration via telephone at 474-8544.

❖ Discrimination Policy

It is the policy of Medical Center Clinic that all team members have a right to work in an environment that is free from discriminatory harassment based on sex, gender, race, age, national origin, religion, disability/handicap, marital status, veteran status, or any other protected discriminatory factor.

❖ Workplace Violence Policy

Threats and acts of workplace violence, including those intended or perceived to be made in jest, are unacceptable and can signal a serious safety issue. Verbal or physical threats, physical acts, fighting, possession of firearms or weapons (other than by uniformed law enforcement and security officers on duty) and other improper conduct towards any person on the premises, including parking lots, of any Medical Center Clinic facility is prohibited. Under no circumstances may a team member bring a weapon into an MCC facility for any reason.

❖ Open Door Policy

Medical Center Clinic has an "Open Door Policy" for team members to discuss any issues pertaining to their relationship with MCC. While it is a good idea for the team member to notify their supervisor of any such complaint, notifying the supervisor alone is not sufficient to put MCC on notice of a problem.

❖ Use of Company Property Policy

Use of any company property is limited to team members for the performance of their job duties. An occasional personal phone call or e-mail is permissible, but such usage is a privilege, not a right. There is no expectation of privacy when using any company property. Team members are not permitted to load software programs onto company computers.

Company property is never to be used to transmit, receive, or store any data or communication that is harassing or discriminatory in nature. Company property is never to be used in the commission of a crime.

When using company property that requires password access team members must use their own passwords. Passwords are confidential and are not to be shared with anyone, including your manager.

**West Florida Medical Center Clinic, P.A.
Privacy and Security
Policies & Procedures Manual**

TABLE OF CONTENTS

Section One: Privacy Policies and Procedures

Designation of Privacy Officer.....	4
Notice of Health Information Privacy Practices.....	6
Acknowledgment of Receipt of Notice of Health Information Privacy Practices.....	8
Authorization to Use and Disclose Protected Health Information (PHI).....	10
Employee Sanctions for HIPAA Privacy Violations.....	15
Minimum Necessary Information.....	17
HIPAA Privacy Training.....	19
De-Identification of Protected Health Information.....	20
Request to Access and Copy Protected Health Information (PHI).....	22
Request to Amend Protected Health Information (PHI).....	26
Request for Confidential Communication of Protected Health Information (PHI).....	29
Request to Restrict Use and Disclosure of Protected Health Information (PHI).....	32
Accounting for Disclosures.....	34
Patient/Other Individual Privacy Complaint Process.....	37
Disposal of Documents Containing Protected Health Information (PHI).....	40
Authorization to E-mail Protected Health Information (PHI).....	41
FAX Transmission of Protected Health Information (PHI).....	44
Business Associate Contracts.....	46

Section Two: Security Policies and Procedures

Designation of HIPAA Security Officer.....	48
Security Management Process.....	49
Workforce Security.....	52
Information Access Management.....	54
Security Awareness and Training.....	55
Privacy /Security Incident Procedures.....	57
Contingency Plan.....	61
Evaluation.....	63
Business Associate Contracts or Other Arrangements.....	64
Facility Access Controls.....	65
Work Station Use.....	66
Work Station Security.....	68
Device and Media Controls.....	69
Access Control.....	71
Audit Control.....	73
Data Authentication.....	74
Person or Entity Authentication.....	75
Transmission Security.....	76

SECTION ONE
PRIVACY POLICIES AND PROCEDURES

DESIGNATION OF HIPAA PRIVACY OFFICER

Effective Date: November 27, 2006

From: Andy Popple, Executive Director
To: Sharon Hoyle
Subject: Designation as the MCC HIPAA Privacy Officer

Under the "Standards for Privacy of Individually Identifiable Health Information" promulgated pursuant to The Health Insurance Portability and Accountability Act of 1996 (HIPAA), health care organizations that transmit or maintain protected health information (PHI) are required to designate an individual as the "privacy official" for their organization.

Privacy Officer Duties and Responsibilities:

- Provide leadership to the Clinic's HIPAA Compliance Committee and any workgroups or taskforces charged with creating and implementing an enterprise-wide health information privacy program.
- Maintaining compliance with federal and state laws related to privacy, security, confidentiality, of PHI resources.
- Collaborate with the Director of Information Services and the Clinic's Network Administrator to ensure policies and procedures relating to (cyber) privacy and security are developed and implemented for the organization's hardware, software and telecommunications systems.
- Collaborate with other departments such as corporate compliance, human resources, accounting, IS, medical records, legal counsel, and medical services to ensure compliance with specific privacy requirements.
- With the assistance of the Compliance Committee membership, monitor all departmental systems and operations for privacy and security compliance.
- Oversee the development of the Clinic's policies and procedures regarding, but not limited to:
 - Notice of Health Information Privacy Practices to be given to all patients
 - Clinic's use and disclosure of PHI
 - Handling (creation, acquisition, and management) of PHI by Clinic employees
 - Patient requests for restriction of use and disclosure of PHI
 - Patient's rights to access, inspect, and copy their medical records
 - Patient's rights to request amendment of their PHI
 - Patient complaint regarding privacy practices
 - Clinic's accounting of disclosures of PHI
 - Disclosure required by law for judicial or administrative proceedings
 - Research related requests.
 - Public health oversight bodies
 - Privacy record keeping and administrative procedures
 - Administrative technical, and administrative safeguards of PHI (e.g. email and fax of PHI)
- Oversee the Clinic-wide privacy awareness-training program for all employees.
- Report the status of the HIPAA privacy program to the Executive Director and other responsible individuals or committees as requested.
- Oversee and coordinate the development of privacy risk assessment policies and procedures designed to measure the performance and quality of the Clinic's privacy program.
- Ensure that the HIPAA privacy program is revised as changes in laws, regulations, or Clinic policy dictate.
- Establish an internal privacy audit program to ensure organization-wide compliance with Clinic's HIPAA privacy policies and procedures.
- Coordinate with the Compliance Officer and the HR Department to develop appropriate sanctions for violations of the Clinic HIPAA privacy policies and procedures.
- Implement and oversee the development and application of corrective action procedures that are designed to mitigate any deleterious effects of a use or disclosure of PHI by members of the Clinic's workforce or business partners. This includes exercising any affirmative duty to address breaches of contract with respect to the treatment of PHI by the Clinic's business partners to Clinic's legal counsel.
- Coordinate with the Compliance Officer and HR to ensure no intimidating, discriminatory, or other retaliatory actions occur against a person who files, testifies, assists or participates in any investigation, compliance review, proceeding or hearing related to a HIPAA privacy violation or opposed any unlawful act or practice.
- Coordinate with the Compliance Officer regarding the development of procedures for documenting and reporting self-disclosures of any evidence of privacy violations to legal counsel, and if appropriate to the appropriate government regulatory body according to corporate policy.

- Provide strategic guidance to corporate officers and the Board regarding HIPAA privacy and the impact on the organizations information resources and technology.
- Coordinate external audit processes of business partners for the purposes of monitoring and detecting any misconduct or noncompliance with Clinic privacy policies.

Andy Popple
Executive Director

NOTICE OF HEALTH INFORMATION PRIVACY PRACTICES

Effective Date: January 1, 2003

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

Thank you for choosing the Medical Center Clinic for your healthcare needs. Each time you visit one of our providers, we create a record of the care and services you receive. We understand that this health information about you and your healthcare is personal and we want you to know that we are committed to protecting the privacy and confidentiality of that information.

In order for us to provide you with healthcare services, obtain payment for our services, and manage our healthcare operations we will need to use and disclose your protected health information. This notice explains how we may use and disclose your health information for these purposes, as well as your rights regarding the health information we maintain about you. We reserve the right to revise the terms of our notice, at any time. You may obtain a copy of the revised notice by calling your physician's office and requesting that one be sent to you by mail, by asking for one at your physician's office, or by downloading a copy from our web site at www.medicalcenterclinic.com.

Our Obligations

The law requires us to:

- Make sure that health information that identifies you is kept private;
- Provide you this notice which describes our health information privacy practices and legal duties;
- Provide you a new copy of the notice should we revise it; and
- Follow the terms of the notice that is currently in effect.

Examples of Disclosures for Treatment, Payment and Health Operations

Treatment:

We will use and disclose your health information so that our physicians, nurses, technicians, and other participants in the West Florida Healthcare System may provide, coordinate, or manage your healthcare and any related services. *For example:* Information about your past medical history, vital signs, or allergies obtained by a member of our healthcare team will be recorded in your medical record and used by your physician to determine the course of treatment that should work best for you. Your physician will then document his or her findings and prescribed medical course of action, and members of your healthcare team will record their subsequent actions and observations. In that way, the physician will know how you are responding to treatment. We may also disclose your health information to another physician or healthcare provider (e.g., a laboratory or specialist) to whom we have referred you for assistance in your diagnosis and treatment.

Payment:

Your health information will be used, as needed, to obtain payment for your healthcare services. *For example:* A bill may be sent to you or to a third-party payer. The information on or accompanying the bill may include information that identifies you, as well as your diagnosis, procedures, and supplies used.

Health Care Operations:

We may use and disclose your health information, as needed, to support our business activities. *For example:* Members of the medical staff, the risk management officer, or members of the quality improvement team may use information in your health record to assess the care and outcomes in your case and others like it. This information will then be used in an effort to continually improve the quality and effectiveness of the healthcare and service we provide.

Other Uses and Disclosures

As Required by Law:

We may disclose your health information when required to do so by federal, state, or local law.

Business Associates:

There are some services provided in our organization through contacts with business associates. Examples include transcription services, physician services in radiology, certain laboratory tests, and medical records transfer services. When these services are contracted, we may disclose your health information to our business associate so that they can perform the job we have asked them to do and bill you or your third-party payer for services rendered. To protect your health information, however, we require the business associate to appropriately safeguard your information.

Appointment Reminders:

We may use and disclose your health information to contact you as a reminder that you have a scheduled appointment. Please let us know if you do not wish us to contact you with reminders, or if you wish us to contact you at a different number.

Treatment Alternatives or Health-Related Services:

We may use or disclose health information to tell you about health-related services or to recommend possible treatment options or alternatives that may be of interest to you. Please let us know if you do not want us to contact regarding this information.

Communication with family:

Health professionals, using their best judgment, may disclose to a family member, other relative, close personal friend or any other person you identify, health information relevant to that person's involvement in your care or payment for services related to your care.

Research:

We may use and disclose information to researchers when an institutional review board has reviewed the research proposal and established protocols to ensure the privacy of your health information has approved the research.

Food and Drug Administration (FDA):

We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.

Worker's compensation:

We may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to worker's compensation or other similar programs established by law.

Military and Veterans:

If you are a member of the armed forces, or separated or discharged from the military services, we may disclose your health information as required by national military command authorities or the Department of Veterans Affairs.

Public health:

We may disclose your health information to a public health authority that is permitted by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability.

Correctional institution:

If you are an inmate of a correctional institution, we may disclose to the institution or agents thereof, health information necessary to provide you with healthcare; to protect your health and safety or the health and safety of other individuals; or for the safety and security of the correctional institution.

Law Enforcement:

We may disclose health information in response to a valid subpoena, warrant, summons or similar process. We may also release information for purposes of locating a suspect, a fugitive, a material witness, or missing person.

Health Oversight Activities:

Federal law makes provision for your health information to be released to an appropriate health oversight agency for activities such as audits, investigations, and inspections. This includes government agencies that oversee the healthcare system, government benefit programs, other government regulatory programs, and the civil rights laws.

Your Health Information Rights

You have the right to:

- obtain a paper copy of this notice upon request
- request a restriction on certain uses and disclosures of your information, but we are not required to agree to those restrictions;
- inspect and copy the information contained in your designated record set which includes your health and billing records;
- request the amendment of your health information;
- request a list of disclosures we have made of your health information for purposes other than treatment, payment or healthcare operations;
- request that we communicate with you by alternative means or at alternative locations, we will comply with all reasonable requests;
- revoke your consent to the use or disclosure of your health information for treatment, payment, or healthcare operations except to the extent that actions have already been taken based on that consent; and
- revoke your authorization to use or disclose health information except to the extent that action has already been taken based on that authorization.

Information Not Covered by This Notice

Uses and disclosures of your health information not covered by this notice or by law may only be made with your written permission (authorization).

Questions or Complaints

If you have questions about this notice, or believe that your privacy rights have been violated, please contact our Privacy Officer, Sharon Hoyle at 1-866-822-3571 or by email at privacy.officer@medicalcenterclinic.com. You have the right to file a written complaint with us or directly to the secretary of Health and Human Services. You should know that there would be no retaliation for your filing a complaint.

PRIVACY POLICIES AND PROCEDURES: PATIENT ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF HEALTH INFORMATION PRIVACY PRACTICES

Effective Date: January 1, 2003

Purpose:

To publish the policies and procedures to implement the requirements of the Final HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule with regard to obtaining the patient's acknowledgment of receipt of a copy of MCC's Notice of Health Information Privacy Practices. The Privacy Rule (as amended at section 164.520(c)(2)(ii)) states:

"Except in an emergency treatment situation, [health care providers having a direct care relationship with a patient] must make a good faith effort to obtain a patient's written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained."

Policy:

All MCC physicians and health care providers are required by HIPAA to provide each patient with a copy of MCC's Notice of Health Information Privacy Practices and to make a "good faith effort" to obtain the patient's written acknowledgment that they have been provided with a copy of the Notice.

Procedure:

Obtaining Acknowledgment of Receipt of Notice

On the occasion of the first provision of service following the implementation of this policy, all physicians and health care providers will ensure that their patient services personnel or medical staff:

1. Provides each patient with a copy of the Clinic's Notice of Health Information Privacy Practices and a copy of the Acknowledgment of Receipt of Notice form for signature.
2. Collect the signed Acknowledgment form from the patient prior to the provision of health care services at that visit.
3. If the patient does not wish to sign the acknowledgment form, the staff representative must annotate the form stating ["Patient was provided with copy of Notice on (date), but patient refuses to sign acknowledgment."], date the form, and sign it in the space provided. There will be no consequence for the patient not signing the acknowledgment.
4. Make an entry in the patient's record in Practice Point Plus (at the Patient Information, Demographics screen) to indicate that a signed acknowledgment form was received (or that the patient was provided a copy of the Notice but refused to sign the acknowledgment).
5. Forward the original signed privacy acknowledgment form via inter-office mail to the Medical Records department for filing.
6. At subsequent patient visits, each provider's office should first verify that the patient received a copy of the Notice by checking for an entry in the patient's record in Practice Point Plus (at the Patient Information, Demographics screen). If there is no entry to indicate the receipt of a signed acknowledgment (or refusal to sign), follow the procedures in steps 1–5 to provide a copy of the Notice and obtain a signed acknowledgment of receipt prior to treatment at this visit.

Upon receipt of the original signed Privacy Acknowledgment form Medical Records will:

1. Electronically scan the original signed form and store the image in the Health Information Document Imaging System where it will be retained for a period of no less than six years (the statute of limitations for the civil monetary penalties) from the date of signature.
2. Once the electronic copy is confirmed to be in the Health Information Document Imaging System, *shred* the original signed copy.

Form Attachment(s)

1. Acknowledgment of Receipt of Notice of Health Information Privacy Practices form

PRIVACY POLICIES AND PROCEDURES: ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF HEALTH INFORMATION PRIVACY PRACTICES

Effective Date: January 1, 2003

Thank you for choosing the Medical Center Clinic for your healthcare needs.

We are required by law to provide you with a copy of our Notice of Health Information Privacy Practices. To ensure that our records are accurate, please sign below to acknowledge **that you have been provided with** a copy of our Notice.

_____ Patient Name	_____ MCC#	_____ Date of Birth
_____ Signature of Patient (or Legal Representative)		
_____ Date		
_____ Signature of Staff Member	_____ Title	_____ Date

Comments:

(place label here)

PRIVACY POLICIES AND PROCEDURES: AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Purpose:

To describe the policies and procedures to be followed at the Medical Center Clinic with regard to obtaining authorization to use or disclose patient protected health information (PHI) for purposes other than treatment, payment, or healthcare operations.

Policy:

It is our policy to protect our patient's PHI from unauthorized use or disclosure. Therefore, no release of PHI will be permitted unless such release is in compliance with this document. Failure to adhere to this policy regarding use or disclosures of PHI will result in sanctions, up to and including dismissal.

The HIPAA Privacy Rule defines disclosure as follows:

"Disclosure: the release, transfer, provision of access to, or divulging in any other manner of information **outside** the entity holding the information."

Disclosure of PHI requiring an individual's authorization

The following uses or disclosures require specific approval of the patient before their PHI may be released:

1. A request made by the individual:
Where the request is made by the individual (or their authorized representative) to have their PHI released to another entity (i.e. another provider).
2. A specific request made by the Medical Center Clinic:
Where the Clinic desires to:
 - a. Use the PHI for the marketing of non-health items or services to the individual;
 - b. Disclose to a health plan or healthcare provider (prior to an individual's enrollment in a health plan) in order to make eligibility or enrollment determinations relating to the individual or for underwriting purposes;
 - c. Use the PHI to contact the individual for fund raising purposes;
 - d. Disclose to an employer for use in employment determinations;
 - e. Disclose PHI to an outside entity for sale, rent, or barter;
3. A general request made by the Medical Center Clinic:
Where the request to use or disclose PHI is made by a physician, employee, or agent of the Medical Center Clinic and the situation does not fall into the situations described above, or in the section entitled Authorization Not Required that follows.
4. A general request made by an outside entity
Where the request to use or disclose PHI is made by an entity that is not an agent of the Clinic or the patient.

Authorization Not Required

An individual's authorization to disclose their PHI is **not** required in the following situations:

1. Disclosures and Uses for **public health activities** (i.e. legal authorizations to collect health information for purposes such as reporting of disease, vital events such as birth or death, or public health investigations);
2. Disclosures and Uses for **health oversight activities** (i.e. legal authorizations to collect health information for purposes such as reporting of disease, vital events such as births or deaths, or public health information);
3. Disclosures for **judicial or administrative proceedings** (i.e. court order or individual's health history is at issue and disclosure is authorized or required by law);
4. Disclosures to **coroners and medical examiners** (i.e. for determining the cause of death of an individual);

5. Disclosures for **law enforcement purposes** (i.e. law enforcement request is supported by a court order, grand jury subpoena, or administrative request);
6. Disclosures and Uses for **governmental health data systems** (i.e. government collection of information for analysis in support of policy, planning, or other regulatory functions);
7. Disclosures for **banking and payment processes** (i.e. minimum amount necessary to complete a banking transaction);
8. Disclosures and Uses for **research purposes** (certain procedural requirements must be met)
9. Disclosures and Uses in **emergency circumstances**;
10. Disclosures and Uses in **workman's compensation**;
11. Disclosures and Uses for **certain specialized government functions** (i.e. military purposes, Department of Veterans Affairs, Intelligence community, Department of State); and
12. Disclosures and Uses **otherwise required by law**.

Procedure:

Obtaining a signed authorization

The following are examples of situations in which an authorization would be required. In such instances, a valid authorization must be obtained from the individual before any PHI is released.

1. A patient is visiting his or her regular physician at the Clinic and wants to have their records sent to a physician in a town where the patient will be vacationing. The patient services representative for the department where the patient is being seen will provide the patient with an Authorization form and have them fill it out and sign it before the patient leaves the office area. The patient services representative (PSR) will immediately forward the signed form to the manager of the Health Information Management Department (HIMD, formerly medical records). The HIMD manager will ensure that the patient's EMR is annotated at the tab marked Authorizations to indicate the receipt of the signed form and that the original form is scanned and filed in the digital storage system. The HIMD manager will then release the information in accordance with the Authorization.
2. If the Clinic desires to use a patient's health information to mail the patient marketing information about new services or products being offered at the Clinic, we must mail the patient an Authorization Form for completion and return to the HIMD manager. When the HIMD manager receives the signed authorization, he will ensure that the patient's EMR is annotated at the tab marked Authorizations to indicate the receipt of the signed form and that the form is scanned and filed in the digital storage system. The HIMD manager will then notify the requesting medical department that the Authorization has been received.
3. If the patient is not being seen, but visits the Clinic to request that we transfer their medical records to an attorney, insurance company as part of a new policy application, or a new physician's office, the PSR will give them an Authorization form to fill out and sign.
 - a. If the patient leaves the signed form with the PSR, that PSR will immediately forward the original to the HIMD manager. The HIMD manager will ensure that the patient's EMR is annotated at the tab marked Authorizations to indicate the receipt of the signed form and that the original form is scanned and filed in the digital storage system. The HIMD manager will then release the information as requested in the Authorization.
 - b. If the patient chooses to take the form with them, the PSR will provide them with a pre-addressed envelope and instruct the patient to return the signed form to the HIMD manager using the provided envelope. Upon receipt of the signed form, the HIMD manager will ensure that the patient's EMR is annotated at the tab marked Authorizations to indicate the receipt of the signed form and that the original form is scanned and filed in the digital storage system. . The HIMD manager will then release the information as requested in the Authorization.

NOTE: It is essential that these entries be made as soon as possible after the HIMD manager receives the signed Authorization form to ensure that the information is immediately available to all other providers covered under our joint Notice and authorization procedures. Failure to make a timely entry can result in violations of HIPAA and place the Clinic in jeopardy of legal action.

Revocation of Authorization to Disclose PHI

A patient may revoke their authorization at any time, except to the extent that the Clinic has already taken action in reliance thereon. If a patient elects to revoke an authorization, they must do so in writing. The PSRs in the various medical departments (or the Privacy Officer) will provide the patient with a Revocation of Authorization form upon request and ensure that the patient immediately signs, dates and returns the form. The receiving provider's office will then:

1. Immediately forward the original to the HIMD manager; and
2. Inform the patient that within twenty four hours of the date and time of the signed Revocation of Authorization, the Clinic, its physicians, employees, and agents will discontinue all disclosures of information as stipulated in the previously signed Authorization.

HIMD manager will:

1. Cause the EMR to be annotated to indicate the receipt of the revocation have the original revocation form scanned and appended to the digital storage system.

NOTE: It is essential that these entries be made as soon as possible after the HIMD manager receives the signed Authorization form to ensure that the information is immediately available to all other providers covered under our joint Notice and authorization procedures. Failure to make a timely entry can result in violations of HIPAA and place the Clinic in jeopardy of legal action.

Form Attachment(s)

1. Authorization to Disclose Protected Health Information Form
2. Revocation of Authorization Form

PRIVACY POLICIES AND PROCEDURES: AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION (PHI)

Patient Name: _____ Medical Record #: _____
Date of Birth: _____ Social Security: _____ Phone: _____

Release of PHI is for: ☐ Doctor ☐ Family ☐ Insurance ☐ Attorney ☐ Other (please specify) _____
Please complete Sections A, B and D for authorization to disclose PHI to family member or other individual:

Section A

Password for family or other individual (Either in Person or by Phone): _____

I hereby authorize the Medical Center Clinic to release the following information contained in my medical records to the following family member(s) or other individual (please attach separate sheet if necessary):

Name: _____ Relationship to Patient: _____ Date of Birth: _____

Name: _____ Relationship to Patient: _____ Date of Birth: _____

Section B – Please complete for family, other individual, and all other authorizations of PHI

☐ All PHI including confidential for the period: _____ ☐ All PHI except the confidential selected below*
for the period: _____

(*Note: While specific Confidential PHI will not be included, the information authorized for release may make reference to any confidential findings.)

Confidential: ☐ HIV Test Results ☐ Alcohol & Drug Therapy ☐ Lab Reports ☐ Mental Health Treatment Records

☐ Clinic Notes for Doctors ☐ X-ray films ☐ X-ray reports ☐ Other (please specify): _____

Section C – Please complete if PHI is to be mailed

Mail to (Name & Address): _____

Section D – Please complete for ALL AUTHORIZATIONS of Protected Health Information

I understand that I may revoke this authorization in writing at any time, except to the extent that release has been made prior to my revocation in reliance on this authorization and that such release shall not constitute a breach of my right to confidentiality. Unless I revoke this authorization prior to such, this authorization to release PHI shall expire on the following condition:

☐ This is a Single Disclosure ☐ This is a Continuing Disclosure for 12 Months

At that time no express revocation shall be needed to terminate my authorization. I hereby release the Medical Center Clinic from any legal responsibility or liability for disclosure that may arise as a result of the use of the information contained in the PHI released.

Signature of Patient

Relationship to Patient (if applicable)

Signature of Witness

Date

IF RETURNING BY U.S. MAIL, PLEASE SEND TO:

Medical Center Clinic
Attn: Record Release Dept.
8333 North Davis Highway
Pensacola, FL 32514
Facsimile 850-474-8022

PRIVACY POLICIES AND PROCEDURES: REVOCATION OF AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Patient Name: _____ Medical Record #: _____

Date of Birth: _____ Soc.Sec.#: _____ Phone#: _____

Address: _____

I hereby revoke my authorization previously given to the Medical Center Clinic to disclose PHI contained in my medical records covering the period from:

_____ to _____.

I understand that disclosures made in good faith may have already occurred in reliance upon my previously issued authorization and that this revocation cannot apply retroactively to such disclosures. I also understand that the disclosure of health information may be required by law in some instances, such as for the reporting of communicable diseases.

I hereby release the Medical Center Clinic, its employees, officers, and physicians from any legal responsibility or liability for disclosure of the information I previously authorized.

Signature

Relationship to Patient (if applicable)

Signature of Witness (if needed)

Date

For Clinic use only:

The medical department staff or official receiving this revocation must fill out the following information and forward the original revocation to the Health Information Management Department manager for processing.

Signature of Clinic employee receiving revocation Date received

PRIVACY POLICIES AND PROCEDURES: EMPLOYEE SANCTIONS FOR HIPAA PRIVACY VIOLATIONS

Effective Date: January 1, 2003

Purpose:

To implement the policies and procedures regarding employee sanctions for privacy violations as required by the HIPAA Privacy rule.

Policy:

Protected health information belonging to a Clinic patient shall be regarded as confidential and shall only be available to authorized users for approved purposes on a need-to-know basis. Access to protected health information is only permitted for activities involving direct patient care, for functions and activities involved in obtaining payment for health care rendered, or for functions or activities involving approved Clinic health care operations.

Confidential information obtained during assigned duties, or by accident, shall not be released to any person or institution except in accordance with the Clinic's Use and Disclosure policy. No Clinic employee, volunteer, vendor, or contractor shall seek access to protected health information out of curiosity, for malicious purposes, or for financial gain.

Discussions or consultations involving a patient's protected health information should be conducted in private and individuals that are not directly involved in that patient's care should not be present without the patient's permission.

Procedures:

Violations or breaches of protected health information privacy or confidentiality have been divided into three levels as described in the following paragraphs.

Level 1. Carelessness –

This level of breach occurs when a Clinic employee inadvertently discloses confidential patient health information to others or unintentionally or carelessly accesses or reviews patient information without a legitimate need to know. For example:

- an employee discusses confidential patient health information in a public area;
- an employee leaves a copy of confidential patient health information in a public area;
- an employee leaves a computer unattended in an accessible area with a medical record open and unsecured;
- an employee accesses a patient record in error, such as by entering the wrong patient ID or SSN.

Disciplinary Sanctions -

Sanctions for this level of violations are given the greatest latitude and shall be administered in a flexible manner by the immediate supervisor. Depending upon the facts involved, sanctions imposed may include counseling, verbal warning, written warning, final written warning or suspension, or termination. The more severe sanctions will be documented in writing and maintained in the employee's personnel record. If appropriate, disciplinary sanctions shall be reported to the applicable professional licensing board.

Level 2. Curiosity or Concern (no personal gain) –

This level of violation is more egregious and occurs when an employee intentionally accesses or discusses patient information for purposes other than treatment, payment, or health care operations, but for reasons unrelated to personal gain. For example:

- an employee looks up birth dates, address of friends or relatives;
- an employee accesses their own record out of curiosity or concern (violating the Clinic's policy and procedure for gaining access to personal medical records)
- an employee accesses and reviews a record of a patient (e.g. friend, family member) out of concern for their well-being or curiosity;
- an employee reviews a public personality's record out of curiosity or concern.

Disciplinary Sanctions –

Due to the more serious nature of these violations of confidentiality, the immediate supervisor must immediately notify the Privacy Officer and adhere to the following to ensure equal application of this policy.

First offense: Depending upon the facts, verbal or written warning documented and maintained in the employee's personnel record. The employee shall be required to repeat the HIPAA privacy-training module on his/her own time.

Second offense: Depending upon the facts, a final written warning, suspension for 3-30 days without pay, or termination. The sanction will be documented and maintained in the employee's personnel record and the employee shall be required to repeat the HIPAA privacy-training module on his/her own time. Disciplinary sanctions shall be reported to the applicable professional licensing board if appropriate.

Third Offense: Termination. Disciplinary sanctions shall be reported to the applicable professional licensing board if appropriate.

Level 3. Personal Gain or Malice –

This level of breach is the most egregious and can place the individual and the Clinic in jeopardy of significant legal actions. The immediate supervisor must immediately notify their Associate Administrator and the Privacy Officer. Such violations occur when an employee inappropriately accesses, reviews, or discusses patient information for personal gain or with malicious intent. For example:

- an employee reviews a patient record to obtain information with the intent to embarrass the patient;
- an employee reviews a patient record to use the information in a personal relationship;
- an employee compiles a mailing list for personal use or to be sold;
- an employee reviews a famous patient's record to sell information to a tabloid for personal gain or malice.

Disciplinary Sanctions -

Immediate termination. Such disciplinary action shall be reported to the applicable professional licensing board.

Reporting Privacy Violations:

Any employee who observes or is aware of a privacy violation or privacy breach must immediately report the violation in accordance with MCCs policy and procedure for privacy and security breaches (refer to page 56). The employee must immediately complete the Privacy/Security Incident Form located on the Employee Intranet and immediately forward the completed form to the Compliance Department. Depending on the seriousness of the violation as outlined above, the Privacy Officer will notify the responsible senior level manager, the Executive Director, and corporate counsel as required. The failure of an individual to report a violation for which they have knowledge will result in disciplinary action. Anyone making a report in bad faith or for malicious reasons shall be subject to disciplinary action.

PRIVACY POLICIES AND PROCEDURES: MINIMUM NECESSARY INFORMATION

Effective Date: January 1, 2003

Policy:

This policy is published to comply with the requirements of Health Insurance Portability and Accountability Act (HIPAA) to ensure our patient's rights with regard to the minimum necessary use and disclosure of their protected health information (PHI) in our day-to-day business operations. All physicians and staff members must understand the implications and elements of this policy.

In the event of an emergency, the strict limits to access outlined in this document may be set aside when a licensed medical professional judges that the potential benefit to the patient outweighs the potential risk to patient privacy.

Procedure:

When using or disclosing PHI, or when requesting PHI from another covered entity, every member of our workforce must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

It should be noted that the minimum necessary restriction does not apply to:

1. uses or disclosures to a direct health care provider for treatment purposes;
2. disclosures made to the individual;
3. uses or disclosures made pursuant to an authorization signed by the patient or the patient's personal representative;
4. disclosures that are required by law;
5. disclosures made to the Secretary of Health and Human Services; and
6. disclosures that are required for compliance with the privacy regulations.

To assist members of our workforce in determining who should have a specified level of access to patient information we define the following functional and access categories:

Functional Categories:

These categories are based on the different staff roles.

1. Direct Health Care Provider – a licensed health care professional who provides direct or indirect patient care or consulting services.
2. Medical Support Staff – staff that provides patient care at the request of a direct health care provider.
3. Direct Support Staff – staff who provide a variety of professional and direct administrative support that involves delivery of patient care or billing operations.
4. Indirect Support Staff – staff who do not have direct involvement in the provision of health care and provide administrative support only.

Access Categories:

1. Administrator Access – Staff in this category perform system upgrades and maintenance, create/edit/delete accounts, set PHI access levels, and create/edit/delete passwords for each end user of that particular application. This category has the highest level of access as required to the applications and computer systems (e.g. network system administrator, individual application administrators).
2. Full Information Access – Staff in this category will have full access to the PHI contained in the electronic medical and billing records to read all appropriate information as needed for treatment, payment, or health care operations (e.g., physicians, nurses, physician assistants, office managers, EMR Coordinator, Risk Manager).
3. Summary Information Access – Staff in this category will have access to summary information about a patient with treatment or diagnostic codes as needed to perform their assigned tasks (e.g., billing staff). Use of PHI by this category should be confined to the absolute minimum necessary required to complete their tasks. The EMR Coordinator and the PPM Administrator restrict their level of access to the PHI contained in the medical and billing records.

4. Minimum Information Access – Staff in this category will have access to patient demographic information with only minimal reference to the treatment or diagnostic information as needed to complete their assigned tasks (e.g., reception/scheduling staff, filing clerks, computer technicians).

Other Requests for Information:

Requests for a patient's PHI may originate within our own organization, yet fall outside the "normal" use and disclosure for treatment, payment, or health care operations. This is an area that can lead to serious breaches of patient privacy. In such instances, staff members must evaluate the request to ensure that only the minimum necessary information is released. Staff should consider the following before releasing any patient information in response to these requests:

- Who is making the request?
- What is the reason the information is being requested (is it directly related to treatment, payment, or health care operations, or is it for convenience or some non-business purpose)?
- What types of information will fulfill the stated reason for the request?
- Would restricting the information hinder or reduce the quality of care provided the patient?

Transmitting ANY patient information via our email system or by internal facsimile machines must be in accordance with the MCC policy on electronic communications.

Information requests originating from entities outside the organization must be directed to the Privacy Officer for resolution.

PRIVACY POLICIES AND PROCEDURES: HIPAA PRIVACY TRAINING

Effective Date: January 1, 2003

Purpose:

To implement the requirement of the HIPAA Privacy regulation to provide training for all Clinic employees regarding the Clinic's policies and procedures for maintaining the privacy and confidentiality of patient protected health information.

"A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart as necessary and appropriate for the members of the workforce to carry out their function within the covered entity."

Policy:

- The Privacy Officer is responsible for the content, implementation, and oversight of Privacy training for all Clinic employees and physicians.
- All members of the Clinic's workforce must complete Privacy training by April 14, 2003 (the compliance date for the HIPAA Privacy rule). This training will provide an overview of the new HIPAA Privacy regulations and the Clinic's policies and procedures that have been created to institute those regulations.
- Thereafter, all new employees must attend Privacy training during their first week of orientation and training. The Privacy training module must be completed before a new employee can attend any computer training classes and before they can be assigned any duties within their department that involves the use of patient health information.
- When a material change in the Privacy policies and procedures affects the functions of employees, Privacy training regarding these changes must be provided to each person whose functions are affected. This training must be completed within ninety days after the changes have been implementation.
- All Privacy training classes will be documented and that documentation will be retained for a period of six years from the date.

While not required, the Clinic will offer its Business Associates the opportunity to attend Privacy training sessions at the Clinic. This will help ensure that Business Associate employees are familiar with the Clinic's policies and procedures regarding the protected health information of its patients.

PRIVACY POLICIES AND PROCEDURES: DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Policy:

This policy is published to comply with the requirements of Health Insurance Portability and Accountability Act (HIPAA) to ensure our patient's rights with regard to the use and disclosure of their protected health information (PHI). We will remove individually identifiable health information for all uses and disclosures that fall outside normal treatment, payment, and health care operations. All physicians and staff members must understand the implications and elements of this policy.

Procedure:

HIPAA permits us to use PHI to create information for other uses and disclosures so long as that information can not be used to specifically identify an individual. Under HIPAA, individually identifiable health information may be de-identified in only one of two ways.

Statistical De-Identification - The first method is to have a person with appropriate knowledge and experience in statistical and scientific methods render the information in such a way that it can not be used, either by itself or in combination with other information, to identify an individual as the subject of that information.

Safe Harbor Method of De-Identification - The second method is to remove all of the elements defined in the Privacy regulation. These data elements are:

1. Names;
2. All geographic subdivisions smaller than a State, including:
 - a. Street address
 - b. City
 - c. County
 - d. Precinct
 - e. Zip code (and their equivalent geocodes), except for the initial 3 digits of a zip code
3. All elements of dates (except year) for dates related directly to an individual, including:
 - a. Birth date
 - b. Admission date
 - c. Discharge date
 - d. Date of death
 - e. All ages over 89, and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URL's);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints;
16. Full face photographic images and any comparable images; and
17. Any other unique identifying number, characteristic, or code.

If after de-identifying the information we have any reason to suspect that the individual patient could still be identified, we will take further steps to remove such information, or seek a written authorization from the patient to release the data.

All employees will be trained regarding this de-identification policy and the importance of removing individually identifiable information except for:

1. Uses and disclosures for treatment, payment, or health care operations;
2. When the disclosure is required by law or is otherwise allowable without authorization; and
3. When an authorization to release information has been obtained from the patient.

The responsibility for assuring that patient information has been sufficiently de-identified prior to release is generally that of the EMR Coordinator (or the Privacy Officer in his/her absence). This responsibility may be delegated to other management or information specialists as appropriate.

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUESTS TO ACCESS AND COPY PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Purpose:

This document delineates the Medical Center Clinic policies and procedures to implement the requirements of the HIPAA Privacy Rule with regard to affording our patients the right to request access and obtain a copy of their protected health information (PHI) maintained in the Clinic's designated record set.

Policy:

The Medical Center Clinic utilizes an electronic medical record (EMR) and billing system, which constitutes our designated record set. It is our policy to accommodate all patient requests to access and inspect the PHI contained in their electronic record set and to request a copy of that information. Such access shall be under the direct supervision of a designated medical records staff member and within the confines of the medical records office.

Definitions:

Access means that patients may request to inspect (view) their medical records and billing records under the supervision of a designated staff member.

Designated record set means the medical and billing records that we use to make health care and payment decisions about the patient.

Procedure:

1. A patient may request to view and copy their designated record set by filling out a Patient Records Access Request Form (a copy is attached to this document) and submitting it to the EMR Coordinator. These forms are available at all physician PSR desks as well as at the reception desk in the Clinic lobby.
2. After the patient has filled out the form, they may return it to a PSR representative or the lobby receptionist, or they may mail it to the medical records office themselves. If the form is left with a PSR or the lobby receptionist, the recipient should inform the patient that they would be contacted within three to five workdays to schedule their appointment to review the records. The recipient will forward the completed form via interoffice mail to the EMR Coordinator.
3. Upon receipt of the request form, the EMR Coordinator will process the patient's request for access within three to five working days of the signed request. The coordinator will:
 - a. Review the records to ensure that information that is excepted from disclosure to the patient is not accessible. (If excepted information is included in the file and it is determined that the information can not be shielded from patient view, the request for access may be denied by following the steps listed under "Rejection of Access Requests" at the end of this document.);
 - b. That the records are complete;
 - c. Set an appointment time that falls within a 30-day timeframe of the signed request (if unable to fulfill the request within the 30-day limit due to difficulties with document retrieval or other technical reasons, inform the patient in writing and state the expected timeframe, not to exceed 60 days);
 - d. Call the patient and:
 - 1.) Confirm the identity of the patient (e.g., verify social security number and birth date) and that they did in fact submit the request;
 - 2.) Confirm the appointment date and time with the patient;
 - 3.) Inform the patient that they have the right to request a copy of their records, but that we are allowed to charge them for the costs of reproducing and mailing the copies;
 - 4.) Provide instructions to the patient on how to locate the medical records office when they come for their scheduled appointment.
4. When the patient arrives for their appointment, the EMR Coordinator will:
 - a. Verify the patient's identity by checking their driver's license or another form of identification;

- b. After the patient's identity has been confirmed, either assist or designate someone in the records room to assist the patient in viewing the information contained in their designated record set and answer any questions they may have.
5. If the patient requests a copy of their medical information, the Clinic employee assisting the patient will:
 - a. Have the patient:
 - 1.) check the block on the Patient Records Access Request Form to indicate that copies are being requested,
 - 2.) include a mailing address to send the copies to in the space provided, and
 - 3.) sign the line below the address line;
 - b. Inform the patient that there is a charge for reproducing and mailing the copies, and collect the fee at that time;
 - c. Inform the patient that the copies will be sent to the address provided within 10 working days.
6. If the patient states that something in their record is incorrect or incomplete, instruct them that they may request amendment or correction by following the procedures in the Clinic's Policy and Procedures for Patient Requests to Amend PHI. Take out that procedure and go over it with them.

Rejection of Access Requests:

Under certain circumstances (detailed in the following paragraphs) the patient's request for access may be denied. Denial of access is a serious matter under the law and before the EMR Coordinator may deny a patient's request for access, the Privacy Officer must make an internal review of the proposed denial. If the denial is supported by the review, the EMR Coordinator may then deny the request, but must do so in writing.

There are two categories for denials of access: unreviewable grounds, determined by the law; and reviewable grounds, which allow a patient to request that we have our decision to deny access reviewed.

Unreviewable grounds for denial of access include:

1. When the information is psychotherapy notes, which are specially protected.
2. When the information was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
3. When the patient has agreed to the denial of access when consenting to participate in a research study we are conducting that includes treatment, for the duration of the research study.
4. When the information is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the patient would be prohibited by law or exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).
5. When a patient's access to the information contained in the medical record or billing record is subject to the Privacy Act, 5 U.S.C. Section 552a, if the denial of access under the Privacy Act would meet the requirements of that law.
6. When the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
7. When the request is from an inmate of a correctional institution, and we believe that providing a access to the information would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or the safety of any person responsible for transporting the inmate.

If access is denied for one of these unreviewable reasons, return a copy of the request form to the patient indicating that we are unable to comply with their request due to the applicable reason. Retain a copy of the request form and the denial, and have it electronically scanned and appended to the electronic medical record.

Reviewable grounds for denial of access include:

1. When a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person.
2. When the information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access is reasonably likely to cause substantial harm to such other person.

3. When the request is made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

If access is denied for one of these reviewable reasons, determine if a summary of the record or if partial access to the records would mitigate the risk that is the basis for the denial. If a summary or partial access to the information is feasible, return a copy of the request form to the patient informing them:

1. That we are unable to fully comply with their request for the stated reasons, and
2. That we can provide a summary of the records or partial access to the records, and ask them to state their preference;
3. That they have the right to request a review of our denial by checking the review box on the Request form and returning it to us.
4. That they will be informed of our final decision following further review.

All denials (and outcome of denial reviews) must be documented in the electronic record by having the originals electronically scanned and appended to the electronic medical record.

Form Attachment(s)

1. Patient Requests to Access and Copy Protected Health Information (PHI)

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUEST TO ACCESS/COPY PROTECTED HEALTH INFORMATION (PHI)

Patient Name: _____ Medical Record #: _____

Date of Birth: _____ Soc.Sec.#: _____ Phone#: _____

Address: _____

- ☐ I hereby request that I be granted access to review the protected health information contained in my medical and billing records (also known as my designated record set).

I wish to review: ☐ The entire designated record set
☐ PHI for the period _____ to _____.

I understand that you must fulfill my request for access within 30 days, unless you encounter a data retrieval or technical problem that would delay that event. If you are unable to meet the 30-day timeline you will notify me of the expected timeframe to fulfill my request, not to exceed 60 days from the original date of my request.

- ☐ I request that I be provided with a copy of the protected health information contained in my medical and billing records. Please mail the copy to me at the address above, unless I have provided an alternative address below:

Alternative address: _____

I understand that I will be charged a fee for the costs of copying and mailing my records.

Signature of patient or legal representative

Date of request

For Medical Center Clinic Use Only:

Date request received

Signature of Clinic employee receiving request

Request for PHI Access has been: ☐ Accepted ☐ Denied

Reason for denial:

Signature of EMR Coordinator

Date

Request for denial reviewed: _____ by _____
and _____. Request for denial is ☐ Approved ☐ Denied

Signature of Privacy Officer

Date

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUESTS TO AMEND PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Purpose:

This document sets forth the policies and procedures to be followed at the Medical Center Clinic to implement the requirements of the HIPAA Privacy Rule with regard to affording patients the right to request amendment to their protected health information (PHI) stored in the system of records maintained by the Clinic.

Definitions:

Amendment means to add information to an existing record which either provides additional information, clarifies or corrects existing information, or provides an alternative view with respect to information that we have compiled about the patient in the patient's designated record set.

Designated record set means the medical and billing records that we use to make health care and payment decisions about the patient.

Policy:

The Medical Center Clinic utilizes an electronic medical record (EMR), an electronic billing system, and an electronic scanning system to digitize older paper charts and documents for storage. These systems constitute the Clinic's designated record set.

It is our policy to afford our patients the right to request an amendment to the PHI contained in their designated record set if they believe that the information is incomplete or incorrect, with exceptions permitted by the law as listed below.

Rejection of Amendment Requests:

Under the Privacy rule, a patient's request to amend their PHI may be rejected for one of the following reasons:

1. The information subject to the requested amendment is not part of the designated record set.
2. The treating physician deems the information contained in the existing records accurate and complete.
3. Clinic health care providers or staff did not create the information subject to the requested amendment.
4. The information subject to the requested amendment is not available for patient access by law (e.g. it is part of psychotherapy notes which the patient is not allowed to see).

A rejection must be documented at the bottom of the Request to Amend PHI form, and signed and dated by the EMR Coordinator or the Privacy Officer.

Procedure:

1. The patient may approach the author of the entry (usually the provider or their office staff), point out the error, and ask for an amendment. The staff member receiving the request should assist the patient in filling out an amendment request form. The staff member will then forward the request form to the EMR Coordinator for action. (In some instances, the request may come in a letter written by the patient to the administrative staff or to other Clinic officials. In the case of a letter, it would be directly forwarded to the EMR Coordinator for action without further patient request information.)
2. Alternately, the patient may contact the HIM department directly.
HIM personnel will assist the patient in completing an amendment request form, and then forward the completed request form to the EMR Coordinator for action.
3. The EMR Coordinator will review the request form, notify the Privacy Officer that a request has been filed, forward a copy of the request to the provider for input, conduct any research needed to close

the action, and then fill out the bottom of the amendment request form to indicate the final disposition of the request.

4. If the amendment is accepted, the EMR Coordinator will:
Ensure that copies of the amendment request form are provided to those individuals or organizations that the patient has indicated on the amendment request form.
Ensure that copies of the amendment request form are provided to the facility's business associates who are authorized to access the information that is subject to the amendment and that may have relied on, or could rely on, that information to the detriment of the patient.
5. The EMR Coordinator will forward the processed form for scanning and inclusion in the Clinic's designated record set.
6. The EMR Coordinator will ensure that whenever a copy of the amended entry is disclosed, that HIM includes a copy of the amendment request form with the associated entry.
7. Regardless of the outcome of the patient's request to amend their PHI, the EMR Coordinator will draft a letter to the patient from the Privacy Officer, indicating the final disposition of patient's request and forward it to the Privacy Officer for signature and mailing. The Privacy Officer will ensure that a copy of the signed letter is made and provided to the EMR Coordinator so that it may be scanned and stored in the electronic imaging system under the patient's account.

Form Attachment(s)

1. Patient Requests to Amend Protected Health Information (PHI)

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUEST TO AMEND PROTECTED HEALTH INFORMATION (PHI)

Patient Name: _____ Medical Record #: _____
Date of Birth: _____ Soc.Sec.#: _____ Phone#: _____
Address: _____

I request that the following information contained in my medical records be corrected/amended:

Date of entry to be corrected or amended: _____

Type of entry to be corrected or amended: _____

I believe that the specified entry is incorrect or incomplete for the following reason(s):

What should the entry state in order to be more accurate or complete?

Would you like this amendment sent to anyone to whom we may have disclosed information in the past? If so, please specify the name and address of the organization or individual.

Signature of patient or legal representative Date of request

For Medical Center Clinic Use Only:

Date request received Signature of Clinic employee receiving request

Date EMR Coordinator received request: _____

Comments of Healthcare Practitioner:

Signature of Healthcare Practitioner Date

Amendment has been: ☐ Accepted ☐ Denied

If denied, check reason for denial:

☐ PHI was not created by this organization ☐ PHI is accurate and complete

☐ PHI is not part of patient's designated record set

☐ PHI is not available to the patient for inspection as required by federal law (e.g. psychotherapy notes)

Action Completed: _____

Signature of EMR Coordinator Date

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUEST FOR CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Purpose:

In the past, it may have been common practice to send information to a patient or call them at an alternate phone, but now HIPAA requires a specific procedure to accommodate a patient's request for this kind of communication. This document formalizes the Clinic's policy and procedures to implement the requirements of the HIPAA Privacy Rule to afford our patients the right to request confidential communication of their health information.

Policy:

It is our policy to accommodate all reasonable requests by patients for the confidential handling of PHI or other information we provide them via mail and/or telephone communications or messages.

Procedure:

1. A patient may request that for privacy, a copy of their designated record set or specified subsets thereof, be sent to them at a mailing address or location other than their home.
2. A patient may request that for privacy, a Clinic provider or other Clinic medical staff, call them or leave phone messages at a phone number other than their home phone number.
3. All patient requests for confidential communications must be made in writing and sent to the Privacy Officer for processing. The Privacy Officer will ensure that the patient's request is annotated in their EMR and that the request is forwarded to the specific provider requested by the patient within 3 workdays of receipt of the written request. Patients may obtain a confidential communications request form (see attached example) from any provider's office staff, from the lobby reception desk, or from the Privacy Officer's office.
4. If a patient no longer desires communications to be handled pursuant to a prior request, they must submit a revocation of confidential communications (see attached form) in writing to the Privacy Officer. The revocation of confidential communications form may be obtained at any provider's office staff, from the lobby reception desk, or from the Privacy Officer's office.

Form Attachment(s)

1. Patient Requests For Confidential Communication of Protected Health Information (PHI)
2. Patient Request to Revoke Confidential Communication of Protected Health Information (PHI)

**PRIVACY POLICIES AND PROCEDURES: PATIENT REQUEST FOR CONFIDENTIAL
COMMUNICATION OF PROTECTED HEALTH INFORMATION (PHI)**

Patient Name: _____ Medical Record #: _____

Date of Birth: _____ Soc.Sec.#: _____ Phone#: _____

Address: _____

☐ I request that _____ (provider) mail me information I may have requested
to the alternate address below:

Alternative address: _____

☐ I request that _____ (provider) call me, or leave phone messages, at the
alternate telephone number below:

Alternative phone number: _____

Signature of patient or legal representative

Date of request

For Medical Center Clinic Use Only:

Date request received

Signature of Privacy Officer

Date

NOTE: If you are mailing this request form to the Clinic, address it to the attention of the Privacy Officer at the address below.

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUEST TO REVOKE CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION (PHI)

Patient Name: _____ Medical Record #: _____

Date of Birth: _____ Soc.Sec.#: _____ Phone#: _____

Address: _____

- ☐ I hereby request that the confidential communications I had previously requested be terminated. All future communications may be to my home address and/or phone number.

Signature of patient or legal representative

Date of request

For Medical Center Clinic Use Only:

Date request received

Signature of Privacy Officer

Date

NOTE: If you are mailing this request form to the Clinic, address it to the attention of the Privacy Officer at the address below.

PRIVACY POLICIES AND PROCEDURES: RESTRICTING USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Purpose:

To implement the requirement of the Final Privacy regulation which establishes the general standard for the right of an individual to request restriction of the uses and disclosures of their protected health information (PHI):

"A covered entity must permit an individual to request that the covered entity restrict (A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and (B) Disclosures permitted under §164.510 (b)." [§164.510 (b) is the standard that discusses uses and disclosures for involvement in the individual's care and notification purposes.]

Policy:

It is our policy to agree to requested restrictions provided:

1. the Privacy Officer or a licensed healthcare professional has determined that the restriction will not limit our ability to manage our healthcare operations or our ability to provide quality healthcare, and
2. if our Information Services (IS) procedures and systems will permit us to comply consistently with the requested restrictions.

If the Clinic does agree to a requested restriction, all physicians, health care providers, employees, and business partners of the Clinic must honor the restriction until it is withdrawn or superceded.

If the individual terminates the restriction, the Clinic may use and disclose PHI as otherwise permitted under the rule. If the Clinic terminates the restriction without the individual's agreement, we may only terminate the restriction with respect to PHI that we create or receive subsequent to having informed the patient of the termination.

Procedures:

A patient may request restriction to the use and disclosure of their PHI by submitting a written request to the Privacy Officer. They may also present a request at some later date, provided it is in writing.

If a patient indicates that they want to request a restriction of the use and disclosure of their PHI, the medical department staff receiving the written request must:

1. Provide the patient with a copy of the request form.
2. Inform the patient that their request will be forwarded to the Privacy Officer for final disposition and that the patient will receive notification of that disposition from the Privacy Officer;
3. Forward the signed request form to the Privacy Officer. If the restriction is agreed to, the Privacy Officer will cause and entry to be placed in the patient's EMR delineating the restriction.
4. The Privacy Officer will forward the original consent form to Medical Records for scanning.
5. Medical Records will electronically scan the signed request form and append it to the digital scan system records. Once the request form has been scanned and the EMR entry is validated the original form may be shredded.

Termination of Restriction

If either party decides to terminate the restriction, it must be done in writing. There is no set format for this, but the request should state what restriction is being terminated. A copy of the patient's written request for termination will be forwarded to the Privacy Officer who will place an entry in the patient's EMR indicating the restriction has been terminated. If the Clinic initiated the termination without the patient's agreement, we may only terminate the restriction with respect to PHI that we create or receive subsequent to having informed the patient of the termination.

FORM ATTACHMENT(S)

1. Patient Request to Restrict the Use and Disclosure of Protected Health Information (PHI)

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUEST TO RESTRICT THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

Patient Name: _____ Medical Record #: _____

Date of Birth: _____ Soc.Sec.#: _____ Phone#: _____

Address: _____

☐ I request the following restrictions to the use or disclosure of my protected health information:

Signature of Patient or Legal Representative

Witness

Date

Notice Effective Date or Version

☐ Restrictions to Use or Disclosure Accepted

☐ Restrictions to Use of Disclosure Denied

Signature

Title

Date

PRIVACY POLICIES AND PROCEDURES: ACCOUNTING FOR DISCLOSURES

Effective Date: January 1, 2003

Purpose:

The Privacy Rule establishes the right of any individual to request and receive an accounting of all disclosures we make of their protected health information (PHI). This policy implements the HIPAA Privacy requirements to afford our patients a means to request such accountings.

Policy:

It is our policy to keep a record of all disclosures of PHI for purposes other than treatment, payment, or health care operations (TPO), and we will provide a full and complete accounting to patients who ask for this information. The Director of Health Information Management is responsible for maintaining the log of all uses and disclosures of PHI that fall outside normal TPO and for responding to patient requests for disclosure. Patients are entitled to one free disclosure listing in a twelve-month period. If they request a subsequent listing within the same twelve-month period, they may be charged a \$30 fee for each additional request to cover the costs for compiling the listing. Patients may withdraw their requests if they do not wish to pay the fee for subsequent disclosure lists.

Procedures:

Patients may request a list of disclosures of their PHI by submitting their request in writing to the Director of Health Information Management using our Request for Accounting of Disclosures form (see the attached example). The patient may obtain a Request for Accounting of Disclosures form from any Patient Services Representative, the receptionist in the main lobby, or directly from the medical records office. The request must state the time period for which the accounting is to be supplied and the address to which the patient wants the list mailed. The time period that a request covers may not be longer than a period of six years prior to the date of the request and may not include dates prior to April 14, 2003 (the effective date of the Privacy Rule).

Upon receipt of a request for disclosure, the Director of Health Information Management will:

1. Ensure that the patient has signed their request form, if not call the patient to validate that they made the request (obtain their signature as soon thereafter as possible).
2. Record the date of the request, details of the request, and the requestor's name, address and phone number in a disclosure request log (or make a copy of the request form and place it into the log).
3. Notify the Privacy Officer (sharon.hoyle@medmgtservices.com) or call extension 8246) that a request for disclosure has been filed.
4. Review the patient's record to determine if it contains a written statement from a health care agency or law enforcement official that suspends any accountings so as not to interfere with the agency's activities. If such a statement exists and the suspension exceeds the 60-day period from the date of the request, notify the patient that you are unable to process their request due to a suspension by law, but will comply within 30 days after the suspension is lifted. State the expected date on which the suspension is to be lifted.
5. If there is no suspension statement, or if a suspension period has expired, initiate the process to gather the disclosure information and compile the list using the Accounting for Disclosures form (see the attached example).
6. Scan the original Accounting for Disclosures form and append it to the digital scan system, then send it to the patient within 60 days of the date of the request. If unable to fulfill the request within the 60-day period, we may extend the period 30 days but must notify the patient. Our extension notice must state the new date, the reason for the delay, and indicate that we will forward the list by the new date.

FORM ATTACHMENT(S)

1. Patient Request for Accounting of Disclosures
2. Accounting of Disclosures

PRIVACY POLICIES AND PROCEDURES: PATIENT REQUEST FOR ACCOUNTING OF DISCLOSURES

Effective Date: January 1, 2003

Name of requestor: _____

Address/City/State: _____

Phone number: _____

I request a listing of the disclosure of my protected health information (made for other than treatment, payment, or health care operations) for the period:

_____ to _____

I understand that I am not entitled to request information about disclosures that occurred prior to April 14, 2003, and that the maximum period for any requested information may not exceed six years. I also understand that this accounting will not include information about disclosures made to myself, to persons involved in my care, to national security or intelligence agencies, or to law enforcement officials (as stated in your Notice of Privacy Practices).

_____ I understand that I may receive the first accounting for disclosures within a 12-month period at no charge.

_____ I understand that I am requesting a second or subsequent accounting within a 12-month period and that I must pay a charge of \$30.00 for this accounting (payable before release).

Signature: _____

Date: _____

For Clinic Use Only:

Name of person receiving request: _____

Phone extension: _____ Date: _____

Comments: _____

Date action closed: _____

PRIVACY POLICIES AND PROCEDURES: ACCOUNTING OF DISCLOSURES FORM

Effective Date: January 1, 2003

____ There were no applicable disclosures made of your protected health information during the period you specified.

____ We are temporarily unable to process your request due to:

____ a suspension required by law.

____ other: _____

but we will fulfill your request by: _____

____ The Medical Center Clinic made the following disclosures of your protected health information during the period specified:

Date of Disclosure	Name and Address to Whom Disclosed	Description of the Information Disclosed	Purpose of the Disclosure

Signature: _____

Date: _____

For Clinic Use Only:

Name of person processing request: _____

Phone extension: _____ Date: _____

Date disclosure sent to patient: _____

PRIVACY POLICIES AND PROCEDURES: PATIENT OR OTHER INDIVIDUAL PRIVACY COMPLAINT PROCESS

Effective Date: January 1, 2003

Purpose:

The Privacy Rule establishes the right of any individual to file a complaint with the Medical Center Clinic or directly to the Secretary of Health and Human Services (HHS) regarding the privacy practices of the Medical Center Clinic. This policy implements the HIPAA Privacy requirements to afford our patients a means to complain about privacy issues. If a complaint to HHS results in an investigation, the Clinic must fully cooperate with the Secretary's investigative team, permitting access to all information requested by the investigators.

Policy:

As required by the Administrative Requirements section of the HIPAA Privacy Rule, the Medical Center Clinic has designated a HIPAA Privacy Officer. The Privacy Officer's extension is 2199. The Privacy Officer's title and phone number must be included in the Clinic's Notice of Health Information Privacy Practices.

The Clinic's HIPAA Privacy Officer is responsible for receiving all complaints regarding the Clinic's medical privacy practices.

It is our policy to keep a record of all health privacy complaints and to investigate all valid complaints to determine the circumstances giving rise to a complaint. If it is determined that our staff or business associates did not adhere to the privacy standards or our published policies and procedures, we will take appropriate disciplinary action. If it is determined that existing policies and procedures did not address the situation under investigation, the policies and procedures will be revised to prevent further occurrences. The Medical Center Clinic, its providers, employees, or agents, may not threaten, intimidate or retaliate against any individual filing a privacy complaint.

Procedures:

Privacy complaints are considered part of Health Care Operations and as such the use or disclosure of patient protected health information (PHI) in resolving complaints.

If a patient expresses a desire to file a health privacy complaint with the Clinic, the patient shall be directed to the HIPAA Privacy Officer for assistance. Other individuals may contact the Privacy Officer at their own discretion.

Upon notice of a patient's desire to make a complaint, the Privacy Officer will

1. Record the date of the occurrence, details of the complaint (inappropriate handling of PHI and how/ why, inadequate policies and procedures), and the complainant's name, address and phone number on a Health Privacy Complaint Form for inclusion in a complaint log (see attached example form);
2. Have the patient sign their complaint form;
3. Notify the Executive Director that a complaint has been filed;
4. Initiate an investigation to determine the circumstances surrounding the complaint (is the complaint valid or is it a misunderstanding of the requirements or of our policies);
5. Report the findings and the resolution(s) to the Executive Director and record the completion of the action in the complaint log.

If a complaint is determined to be the result of a misunderstanding of the privacy rules or of our privacy policies and procedures, the Privacy Officer will clarify the misunderstanding with the patient and determine if any further action is required. If the complaint is closed at that time, the Privacy Officer will annotate the Complaint Form and the case will be closed after management has been advised.

While the Clinic may wish to provide a response to the patient on all other complaints, there is no requirement of law to do so. If management determines that a response to the patient should be sent, the Privacy Officer will draft a letter and forward it for review by management and/or legal counsel prior to release. The Privacy Officer must ensure that patient privacy complaints and their disposition are fully documented. Beginning on April 14, 2003, these records must be retained for a period not less than six years from the date of complaint (the statute of limitations for civil penalties).

If a patient expresses a desire to file a health privacy complaint directly with the Secretary of HHS, they should be directed to the Privacy Officer. The Privacy Officer will instruct the patient that their complaint:

1. Must be made in writing;
2. Must name the entity against whom the complaint is lodged;
3. Must describe the acts or omissions; and
4. Must be filed within 180 days of the time the individual became aware or should have been aware of the violation.

Other Circumstances that May Give Rise to Complaints:

Denial of Access

Under the Privacy Rule, the Clinic has the right to deny an individual access to his/her PHI under special circumstances. In its denial, the Clinic must fully explain the reason for denial and describe how the individual may complain directly to the Secretary of HHS or to the Clinic's HIPAA Privacy Officer. The description of the process must include the Privacy Officer's name and telephone number.

Denial of Amendment

Under the Privacy Rule, the Clinic has the right to deny an individual's request to amend or correct a medical record for certain reasons. In its denial, the Clinic must fully explain the reason for the denial and describe how the individual may complain directly to the Secretary of HHS or to the Clinic's HIPAA Privacy Officer. The description of the process must include the Privacy Officer's name and telephone number.

FORM ATTACHMENT(S)

1. Patient or Other Individual Privacy Complaint

PRIVACY POLICIES AND PROCEDURES: PATIENT OR OTHER INDIVIDUAL PRIVACY COMPLAINT FORM

Date: _____

Name of complainant: _____

Phone number: _____

Specifics of the complaint: _____

Date Executive Director notified: _____

Findings: _____

Date action closed: _____

PRIVACY POLICIES AND PROCEDURES: DISPOSAL OF DOCUMENTS CONTAINING PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Purpose:

To implement procedures for the proper disposal of documents containing patient protected health information.

Policy:

Clinic employees produce documents on a daily basis containing health information that can be used to identify individual patients, their medical histories, and/or treatments. Such information is classified as protected health information and must be safeguarded just as we protect the patient's medical records. When these documents are no longer needed, they must be disposed of in a way that ensures that the information contained therein is not released to unauthorized individuals. Disposing of sensitive documents in the regular trash or in locked dumpsters does not meet this criterion.

Therefore, all members of the Clinic staff are required to dispose of documents containing individually identifiable health information by:

1. placing such documents in one of the locked MCC certified shredding service boxes;
or
2. by personally shredding the document (if a shredding machine is available in the workspace).

A list of such documents might include:

- Charge tickets
- EMR printouts
- Appointment slips or schedules
- Billing summary reports
- Lab data reports
- Screen printouts
- Nurse note printouts
- Hospital system printouts
- Hand written notes made during discussions with patients (if they identify the patient)

While this list is not all-inclusive, the premise is "if you think that the document can be used to identify a patient then shred it." Our goal is to prevent an inadvertent release of PHI and to protect our patient's rights to privacy.

PRIVACY POLICIES AND PROCEDURES: E-MAILING OF PROTECTED HEALTH INFORMATION

Effective Date: January 1, 2003

Purpose:

The advent of electronic mail has made day-to-day business functions much easier. However, this “benefit” also poses a serious threat to the confidentiality of patient protected health information. This document provides guidance for the appropriate use of e-mail at the Medical Center Clinic to ensure the privacy and confidentiality of protected health information.

Policy:

It is the policy of the Medical Center Clinic that no patient health information shall be transmitted using electronic mail without the express permission of the Privacy Officer. When such permission has been granted, communicating protected health information via e-mail is limited to the specific conditions delineated by this policy.

Procedure:

1. E-mailing confidential patient health information between Clinic employees using the Clinic’s e-mail system is only permitted when:
 - a. Permission has been obtained from the Privacy Officer; and
 - b. such information is necessary for treatment, payment, or healthcare operations; and
 - c. “time is of the essence” and no other more secure method is available that will satisfy the time requirement (e.g. a file placed on a shared network drive with controlled access; interoffice mail using a sealed envelope marked as Confidential); and
 - d. SMIME compatible encryption is used to encode the e-mail. (contact the Network Administrator for information on how to obtain and use encryption with the Clinic’s e-mail system); or
 - e. Only the MCC patient ID and a date of service is used to identify the patient.
2. Transmitting confidential patient health information via e-mail to non-Clinic personnel or to Clinic personnel outside the Clinic network is only permitted when:
 - a. Permission has been obtained from the Privacy Officer; and
 - b. The patient has signed a valid authorization specifically permitting such communication (see attached form) and has been informed of all potential security risks.

or

 - c. The communication to an authorized recipient is accomplished in such a way that it would be impossible to determine the identity of the patient if it was illegitimately intercepted (de-identification).

or

 - d. The communication to an authorized recipient is accomplished using secure communication methods provided or approved by the IS department and which are, for all practical purposes, impossible to intercept and interpret.
3. Communicating directly with patients via e-mail requires the exercise of great care to insure that confidential patient health information is not inadvertently disclosed or lost and that the intended recipient receives the information in a timely fashion. E-mail communications with patients must therefore adhere to the following:
 - a. A patient must be informed of the potential security risks associated with e-mail, including the risk of technical failure, and must sign an authorization permitting e-mail communications by the provider (see attached form). A copy of the signed authorization must be filed in the patient’s EMR as delineated in the Clinic’s Authorization for Disclosure policy.
 - b. Patients must be provided with specific instructions on how to use e-mail to communicate with their providers or authorized staff (e.g. patients must put their name and patient identification number in the first line of the body of the message; patients must put the category of transaction in the subject line: appointment, scheduling, medical advice, etc.).
 - c. Patient and provider (or authorized staff) must agree on a turnaround time for messages (e.g. provider will reply to e-mail within 3 workdays; patient will reply to e-mail within 3 workdays) and include that information on the signed authorization form in the space provided.
 - d. Patients must be informed that only information about prescription refills, appointments, and scheduling will be transmitted via e-mail. Sensitivity information such as laboratory results, HIV, or mental health information will never be transmitted.

- e. Patients must acknowledge receipt of all e-mail communications from provider.
- f. Provider must acknowledge receipt of e-mail communications from patient.
- g. If it is believed that an e-mail containing patient confidential information has been sent to the wrong recipient in error, the recipient must be contacted by the sender and instructed to destroy the message. A note should be filed in the patient's chart detailing those events, and the Privacy Officer must be informed of the incident.
- h. E-mail should never be used for emergency communications.

FORM ATTACHMENT(S)

1. Authorization to E-mail Protected Health Information (PHI)

PRIVACY POLICIES AND PROCEDURES: AUTHORIZATION TO E-MAIL PROTECTED HEALTH INFORMATION (PHI)

Patient Name: _____ Medical Record #: _____
Date of Birth: _____ Soc.Sec.#: _____ Phone#: _____

I hereby authorize Medical Center Clinic and it's authorized representatives to transmit to me or my authorized representative via email communication the following information:

Medical Center Clinic and it's authorized representatives may transmit information about me via e-mail communication to the following individuals:

Name: _____ Date of Birth: _____
E-Mail Address: _____ Relationship to Patient: _____

Name: _____ Date of Birth: _____
E-Mail Address: _____ Relationship to Patient: _____

My e-mail address is:

This is: ☐ A Single Communication ☐ A Continuing Authorization for 12 Months

I understand e-mail is a non-secure means of communication. Furthermore, I understand that there is a possibility that such communication could be intercepted and interpreted by another. By signing this authorization I accept those risks and release Medical Center Clinic from any legal responsibility or liability for disclosures that may occur as a result of eavesdropping or interception by others of the subject e-mail communications.

I understand that I may revoke this authorization in writing at any time, except to the extent that communications have been made prior to my revocation in reliance on this authorization and that such communications shall not constitute a breach of my right to confidentiality. Unless I revoke this authorization prior to such, this authorization to communicate via e-mail shall expire on the following date, event, or condition: _____.

Communicating patient information via e-mail requires the exercise of great care to insure that confidential patient health information is not inadvertently disclosed or lost and that the intended recipient receives the information in a timely fashion. E-mail communications between a provider and patient must therefore adhere to the following:

- a. The patient's name and medical record number must appear in the first line of the body of the message.
- b. The category of transaction must appear in the subject line (i.e., appointment, scheduling, prescription refill).
- c. Patient and provider (or authorized staff) agrees to acknowledge receipt and respond to email communications within _____ business days.
- d. The patient and patient's authorized representative understands that only information about prescription refills, appointments, and scheduling will be transmitted via e-mail.
- e. The patient or other authorized individual must acknowledge receipt of all e-mail communications from the provider or other authorized representative.
- f. The provider or other authorized individual must acknowledge receipt of e-mail communications from patient or other authorized individual.
- g. E-mail may never be used for emergency communications.

I understand that if I refuse to sign this authorization I may not be denied treatment by Medical Center Clinic. I acknowledge receipt of a copy of this authorization.

Signature of Patient or Patient's Legal Representative

Date

Signature of Witness (if needed)

Relationship to Patient (if applicable)

PRIVACY POLICIES AND PROCEDURES: FACSIMILE TRANSMISSION OF PROTECTED HEALTH INFORMATION (PHI)

Effective Date: January 1, 2003

Purpose

This document provides guidance for the appropriate use of facsimile (FAX) machines when transmitting protected health information. FAX machines are now used regularly to transmit medical information to facilitate the medical billing process, and occasionally to communicate health information to patients. Without proper safeguards to ensure that medical information is faxed in accordance with strict protocols, there is significant risk that the confidentiality of those records will be compromised.

Policy

It is policy of the Medical Center Clinic to ensure that PHI sent or received by FAX are handled in a manner that protects against unauthorized disclosure of such information to third parties. When practicable, MCC employees are encouraged to send and receive PHI by interoffice mail or the regular U.S. Mail service to lessen the risk of compromise. Transmission of PHI by FAX should be limited to the minimum amount necessary to accomplish the intended purpose. Whenever it is necessary to FAX patient health information, employees must comply with the procedures set forth in this policy.

Procedures

1. FAX machines will be located in non-public, controlled access areas.
2. FAX machines shall be checked periodically to ensure that PHI is not left sitting in the receive slot or on the desk next to the machine. Incoming faxes shall be routed to their intended recipients as soon as possible after receipt. A folder to contain the received faxes until the recipient can pick them up is acceptable so long as this information is not left unattended for a long period of time.
3. Only designated staff members within a medical unit are authorized to transmit PHI using FAX equipment. Such designations shall be in writing by the medical unit supervisor and held in the supervisor's file on the employee.
4. Each FAX transmittal of PHI requires that a valid authorization be obtained from the patient prior to the transmission.
5. FAX machine must be set to print transmission confirmation sheets.
6. A log of FAX transmissions of PHI shall be maintained within the sending department. These records shall be retained for a period of six years from date of entry.
7. Highly sensitive medical information (such as that dealing with mental health, chemical dependency, sexually transmitted diseases, or HIV) shall not be transmitted by FAX unless a licensed health care provider has determined that such transmission is necessary to assist in the treatment of an emergency medical condition. A record of the provider's determination must be kept in the transmission log.

When MCC staff sends a FAX:

1. Where possible, FAX numbers that are used on a regular basis shall be preprogrammed and keyed to a speed dial button. These preprogrammed numbers must be tested and verified (by calling the receiving party to confirm the receipt of the test file) before the preprogrammed numbers can be used to transmit PHI. The section supervisor shall ensure that a record of the verification test (date, recipient and sender) is recorded in a log, should that information be needed for a future investigation. Re-verification of the numbers must be accomplished at least semi-annually and documented.
2. In cases where a number can not be preprogrammed (e.g. the number is not frequently dialed, all speed dial buttons are already in use; the machine does not have preprogrammed button capability) the sender must:
 - a. Call the intended recipient to obtain their FAX number and inform them that PHI is being Faxed;
 - b. Create a cover sheet containing the following:
 - 1.) MCC Department Identification, Sender's Name, Phone #, FAX #
 - 2.) Date of Transmission
 - 3.) Number of Pages Transmitted
 - 4.) Recipient Name, Phone #, FAX #;

- 5.) Remarks or Special Instructions (if required);
- 6.) Confidentiality Statement, for example:

THIS FAX IS INTENDED ONLY FOR THE USE OF THE PERSON OR OFFICE TO WHOM IT IS ADDRESSED, AND CONTAINS PRIVILEGED OR CONFIDENTIAL INFORMATION PROTECTED BY LAW. ALL RECIPIENTS ARE HERBY NOTIFIED THAT INADVERTENT OR UNAUTHORIZED RECEIPT DOES NOT WAIVE SUCH PRIVILEGE, AND THAT UNAUTHORIZED DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION IS PROHIBITED. IF YOU HAVE RECEIVED THIS FAX IN ERROR, PLEASE DESTROY THE ATTACHED DOCUMENT (S) AND NOTIFY THE SENDER OF THE ERROR BY CALLING

- c. Reconfirm that the destination FAX number keyed and displayed on the FAX machine screen is correct before pressing the Send button;
- d. Compare the printed confirmation sheet against the number dialed to confirm valid transmission.
- e. If sender becomes aware that the FAX was erroneously sent to the wrong FAX number, the sender must immediately contact the erroneous recipient and request that they destroy the FAX, then notify their MCC section supervisor. (Supervisors in turn will notify the Privacy Officer.) The erroneous transmission incident and follow-up action should be recorded in the supervisor's log as a permanent record of the event.

When MCC staff is notified that they will be receiving a FAX containing PHI, they will:

1. Remove the fax containing the PHI from the FAX machine as soon as possible after receipt;
2. Count the number of pages received and compare that number to the number on the transmitted FAX cover page. If pages are missing, immediately notify the sender and request that they retransmit the missing pages.
3. Read the FAX cover page for any "Special Instructions";
4. Notify the recipient that the FAX has been received.

When MCC staff receives a FAX containing PHI that was obviously sent in error they will:

1. Call the sending party and inform them of the erroneous transmission;
2. Destroy the FAX by shredding.

PRIVACY POLICIES AND PROCEDURES: BUSINESS ASSOCIATES AND CONTRACT REQUIREMENTS

Effective Date: January 1, 2003

Purpose

To implement the requirement of the Privacy rule regarding placing written contracts with Business Associates who perform a function or activity on behalf of the Medical Center Clinic that involves the use or disclosure of protected health information (e.g. claims processing, data analysis, utilization review, quality assurance, billing, benefit management, practice management services, legal services, consulting services, accounting or financial services).

Policy

It is our policy to ensure that all contracts with individuals or entities that perform a function or activity on our behalf involving the use or disclosure of our patient's protected health information shall include language to address the Privacy requirements as stipulated in the Privacy rule at Section 164.502(e) and as required under the Health Information Technology for Economic and Clinical Act (HITECH).

Procedures

1. The Privacy Officer will review, or cause to have reviewed, all contracts with individuals or companies that provide a function or activity that involves the use or disclosure of our patient's protected health information to perform their tasks.
2. The Privacy Officer shall create a list of these individuals and vendors and maintain that list for review at any time by an investigating official.
3. The Privacy Officer shall cause all contracts that are in force prior to and continuing past April 14, 2003 to be modified at their renewal date to incorporate the required language of the Privacy rule regarding the safeguarding of patient protected health information.
4. The Privacy Officer will ensure that all new contracts taking effect after April 14, 2003 incorporate the required language of the Privacy rule regarding the safeguarding of patient protected health information.

SECTION TWO

SECURITY POLICIES AND PROCEDURES

DESIGNATION OF HIPAA INFORMATION SECURITY OFFICER

Effective Date: January 1, 2003

From: Andy Popple, Executive Director
To: Hank Falacienski, Director of Information Services
Subject: Designation as the MCC HIPAA Information Security Officer

The "Security and Electronic Signature Standards" promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), requires that, "...security responsibility be designated to a specific individual or organization, and that the assignment be documented. These responsibilities include the management and supervision of use of security measures to protect data, and the conduct of personnel in relation to the protection of data. This assignment is important in providing an organizational focus and importance to security and to pinpoint responsibility."

Accordingly, you are hereby designated as the HIPAA Information Security Officer for the Medical Center Clinic. Your duties and responsibilities are detailed in the paragraphs that follow.

Information Security Officer Duties and Responsibilities:

- Coordinate with the HIPAA Privacy Officer and the Compliance Committee to oversee the establishment, implementation and adherence to policies and procedures to support the provision of information security services.
- Conduct periodic risk assessments and analyses to help the Clinic develop security standards and procedures that support strategic and operational objectives on a cost-effective basis.
- Makes recommendations on appropriate physical and technical security controls.
- Manage the HIPAA Information Security Incident Reporting program to ensure the prevention, detection, containment and correction of security breaches.
- Participate in the resolution of security violations.
- Responsible for the content of information security seminars and training classes.
- Coordinate the communication of information security awareness to all members of the organization.
- Coordinate steps to certify that IT systems meet predetermined security requirements.
- Strive to maintain high system availability.
- Work with vendors, IT associates, and end-user departments to enhance information security processes and procedures.

Andy Popple
Executive Director

SECURITY POLICIES AND PROCEDURES: SECURITY MANAGEMENT PROCESS

Effective Date: January 1, 2005

Background:

45 CFR §164.308(a)(1) of the Security standards states “a covered entity must establish a formal Security Management process which implements policies and procedures to prevent, detect, contain, and correct security violations.”

Purpose:

To establish the Medical Center Clinic's (MCC's) security management process, including the required subordinate implementation specifications of risk analysis, risk management, sanction policies, and information system activity reviews.

Policy:

MCC is committed to implementing a security management process to minimize or eliminate potential risks to the electronic protected health information (ePHI) stored in, processed, or transmitted by its computer network systems. The following policies apply to all ePHI in use by MCC and are the responsibility of the Information Systems (IS) department with guidance from the Security Officer.

Risk Analysis

Section 164.308(a)(1)(ii)(A) of the rule states: “Covered entities will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held or processed by their computer systems.” The following procedures are implemented to ensure MCC's compliance with the rule and are the responsibility of the IS Director or a designated alternate:

- The IS Department will identify all MCC computer and network systems hardware, operating system software, application software, and data sets, and determine the criticality of each asset to daily operations.
- The IS Department will identify all “reasonably anticipated risks” and vulnerabilities of the above assets to various natural disasters or to disasters resulting from manmade causes (e.g. fire, terrorist attacks).
- The Security Officer will ensure that an estimate of the likelihood of occurrence for each identified threat is prepared and included in MCC's overall Security Compliance Program documentation.
- The IS Department, in conjunction with the Security Officer or a designated alternate, will prepare a list of possible mediations to all identified risks and identify those most likely to occur given the MCC environment. This list will be included in MCC's overall Security Compliance Program documentation.

Risk Management

Section §164.308(a)(1)(ii)(B) of the rule states, “Covered entities will implement security measures sufficient to reduce potential risks and vulnerabilities to a reasonable and appropriate level.” The following procedures implement MCC's approach to these requirements:

- All MCC supervisors are responsible for ensuring that all MCC employees currently under their direction are adequately trained with respect to the security policies and procedures implemented by MCC, and will periodically review the policies and procedures with their staff to ensure they stay current with the policies.
- All supervisors, in conjunction with the Human Resources department, will ensure that all new employees attend the privacy and security awareness training during their New Employee Orientation Week.
- The IS Director, in conjunction with the Security Officer or a designated alternate, will ensure that processes and procedures are implemented to minimize or eliminate the possibility of occurrence for each threat identified by the risk analysis.
- The IS Director, in conjunction with the Security Officer or a designated alternate, will ensure that a process for the continual assessment of potential risks is instituted and followed, and that policies and procedures are updated as necessary to address new or continuing risks or changes to the regulations. This may be accomplished using internal assets, or a third party contractor.

Sanction Policy

Section §164.308(a)(1)(ii)(C) of the rule states: “Covered entities will apply appropriate sanctions against employees who fail to comply with the policies and procedures of the covered entity”. MCC has implemented the following policies to address these requirements, which augment and compliment the sanctions implemented under the privacy policies:

Unintentional violations (Level 1) –

This level of breach occurs when an employee unintentionally or carelessly performs an action that violates the security policies and jeopardizes the confidentiality, integrity, or availability of the ePHI maintained or processed by MCC computer systems. For example:

- an employee leaves a computer unattended in an accessible area while still logged into the network and/or a patient record (e.g. while taking a patient to a treatment room, or while at lunch or attending a meeting);
- an employee fails to log out of their computer when leaving at the end of their normal shift potentially allowing access to the network and confidential patient data via their account;
- an employee places confidential patient information on a diskette and misplaces that diskette.

Disciplinary Sanctions –

Sanctions for this type of violation will be given the greatest latitude and will be administered in a flexible manner by the immediate supervisors. Depending upon the facts involved, sanctions that can be imposed may include unofficial counseling, verbal warning, formal written warning, final written warning, or suspension or termination. The more severe violations in this category, and the subsequent sanctions applied, will be documented in writing and maintained in the employee's personnel record. All violations must be reported to the Security Officer as soon as they are discovered. When appropriate, disciplinary sanctions shall be reported to the applicable professional licensing board. If an employee commits an unintentionally violation, they are responsible for reporting that violation to their immediate supervisor. An employee's failure to report such a violation will escalate the incident to a Level 2 sanction.

Follow-up to a reported violation –

- Immediate supervisors will review the procedures used by the employee to ensure that the cause of the violation was not a lack of policy or clarity of guidance in this area.
- If this was a first time occurrence, immediate supervisors will counsel the employee and provide re-fresher policy and procedure training as deemed necessary.
- For a second violation of this type, supervisors should consider making the counseling a formal written warning, and place a copy of the warning in the employee's personnel file.
- If the same employee commits a third violation of this type, the IS department will suspend the user's access until they complete retraining in security policies. Depending on the seriousness of the violation, termination of employment may also be considered.

Intentional violations (Level 2)-

This level of violation is more egregious and occurs when an employee intentionally violates one of the Privacy or Security policies. For example:

- an employee knows that they are not supposed to share their network access with others, but logs into the network and allows another individual to access ePHI on MCC's network through their account (e.g. family members or a visiting physician);
- an employee shares their network and/or application password with another individual;
- an employee knowingly fails to report a security violation to their supervisor or to the Security Officer.

Disciplinary Sanctions –

Because violations of this type are of a more serious nature, the immediate supervisor must immediately notify the Security Officer and adhere to the following to ensure equal application of this policy.

First offense: The user's network account will be disabled and, depending upon the facts, a verbal or written warning will be documented and maintained in the employee's personnel record. The employee shall be required to repeat HIPAA privacy and security training in the next regularly scheduled class before their network account is re-enabled.

Second offense: The user's network account will be disabled and, depending upon the facts, they may be given a final written warning, a suspension for 3-30 days without pay, or they may be terminated. The sanction will

be documented and maintained in the employee's personnel record and, if the employee is not terminated, they shall be required to repeat HIPAA privacy and security training on his/her own time before their network account is re-enabled. If appropriate for the violation committed, disciplinary sanctions shall be reported to the applicable professional licensing board.

Third Offense: The user's network account will be disabled and the employee will be terminated. If appropriate for the violation committed, disciplinary sanctions shall be reported to the applicable professional licensing board.

Follow-up to a reported violation –

Immediate supervisors will review the procedures used by the employee to ensure that the cause of the violation was not a lack of policy or clarity of guidance in this area. The supervisor will report their findings to the Security Officer as soon as possible.

***Intentional violations for personal gain or for malice* (Level 3) –**

This level of breach is the most egregious, and places the individual and MCC in jeopardy of significant legal actions. The immediate supervisor must immediately notify the Privacy and Security Officers. Such violations occur when an employee inappropriately accesses, reviews, or discusses patient information for personal gain or with malicious intent. For example:

- an employee intentionally downloads a file containing a virus to willfully infect the MCC network systems and cause an interruption of normal processing;
- an employee intentionally damages one or more components of the MCC network causing an interruption of normal processing;
- an employee compiles a list of patient data with the intent of selling it to a third party for personal gain.

Disciplinary Sanctions –

The employee will be immediately terminated for cause and the disciplinary action shall be reported to the applicable professional licensing board.

A violation of this magnitude is the most serious type, and under the regulations is a misdemeanor subject to criminal and/or civil penalties. Violations of this type will result in immediate termination for cause, and may result in legal action by MCC against the employee directly. MCC must notify a patient if it is determined that a violation of this type directly involved the patient's ePHI. The patient may well take his or her own legal action against the violator.

Information System Activity Review

Section 164.308(a)(1)(ii)(D) of the rule states: "Covered entities will implement procedures to regularly review records of the information systems activity, such as audit logs, access reports, and security incident tracking reports". MCC has implemented the following procedures to address these requirements:

- The IS Director will ensure that information system activity logs are implemented and maintained for all applications that process ePHI on MCC computers.
- The IS Director will assign a person(s) to conduct quarterly reviews of the MCC information systems' activity logs, this activity may entail the use of an outside entity if desired. Selected reviewer(s) must have the appropriate technical skills and authorized access to enable them to interpret the audit logs correctly.
- The designated reviewer(s) will prepare reports to summarize their reviews. The report will include the reviewer's name, date and time of the review, application or process reviewed, and any significant findings, and describing any events that require additional action (incident reporting).
- Reviewers will look at system/application logs to identify events such as multiple failed login attempts, patient file accesses, and unauthorized access attempts.
- Based on the periodic reviews, the IS Director may implement new procedures or technologies to improve the security management process.
- As necessary, the Security Officer, in conjunction with the IS Director, will make modifications or additions to the policies implemented to protect ePHI on MCC computer systems.

SECURITY POLICIES AND PROCEDURES: WORKFORCE SECURITY

Effective Date: January 1, 2005

Background:

45 CFR §164.308(a)(3) of the Security standards states “a covered entity must implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section [Information Access Management], and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.”

Purpose:

To establish the Medical Center Clinic's (MCC) Workforce Security policies, including the required subordinate implementation specifications of authorization and/or supervision, workforce clearance procedures, and termination procedures.

Policy:

MCC is committed to maintaining formal procedures to ensure that all workforce members whose jobs require access to electronic protected health information (ePHI) have the appropriate level of access and to preventing unauthorized personnel from obtaining access to that information. MCC will continually assess potential risks and vulnerabilities to the ePHI in its possession and develop and implement appropriate security measures in accordance with 45 CFR §164.308 [Administrative Safeguards].

Authorization and/or Supervision

Section 164.308(a)(3)(ii)(A) of the Security Rule states: “Covered entities will implement procedures for the authorization and/or supervision of employees who work with ePHI or in locations where it might be accessed”.

MCC has implemented the following procedures to address these requirements:

- Senior managers are responsible for ensuring that the extent of authorization and/or supervision required for each employee position within their department(s) when accessing ePHI on MCC computer systems is identified, and that such requirements are included in each employee's job description.
- Senior managers are responsible for ensuring that current employees have attended the appropriate training classes necessary to qualify for the level of access required in their job description.
- Senior managers are responsible for ensuring that the training needs of employees who are changing jobs or being promoted are reviewed, and that they are assigned to the appropriate training classes for the level of access required by their new job requirements.
- All new employees must be assigned to the appropriate levels of training during New Employee Orientation week based on the requirements of their job descriptions, as provided to Human Resources by the senior managers.
- Senior managers are responsible for ensuring that periodic reviews are conducted of the information access requirements of the employees under their supervision, and for making appropriate changes to the training requirements and job descriptions.

Workforce Clearance Procedure

Section 164.308(a)(3)(ii)(B) of the Security Rule states: “Covered entities will implement procedures to determine that an employee's access level to ePHI is appropriate”. MCC has implemented the following procedures to address these requirements:

- Employees may only attend training classes to which they have been assigned by their supervisor (based on the access requirements of their job description).
- The network trainer will have each new employee fill out their password request form and confidentiality agreement form at the end of the class.
- The trainer will then sign and immediately forward the completed network password request forms to the Network Administrator who will set up the new user's account in the network server no later than Friday of the week in which the training took place.
- Application trainers (EMR, billing, and scheduling) will have each employee fill out and sign a Training Completion form at the end of each class completed, and then the trainer will sign the completed form to certify that the training was completed.

- Application managers (e.g. EMR, Context, billing, and scheduling) will set up accounts in the appropriate application for the newly trained employees then forward copies to the Network Administrator who will then provide the user with the appropriate application icons in their network applications manager screen.

Termination Procedures

Section 164.308(a)(3)(ii)(C) of the Security Rule states: "Covered entities will implement procedures for terminating access to ePHI when an individual's employment ends or their access requirements under paragraph (a)(3)(ii)(B) above are removed". MCC has implemented the following procedures to address these requirements:

- Supervisors are responsible for immediately notifying the Network Administrator when it is first known that an employee is leaving the Clinic or is no longer filling a position that requires network account access. In the case of a terminating employee, supervisors shall provide the employee's prospective termination date, if known, as part of that notification.
- The Network Administrator will immediately suspend the network account access for the terminated employee(s).
- In the case of disciplinary action that results in an employee's immediate termination, whether initiated by the Human Resources department or the employee's department, supervisors must immediately notify the Network Administrator so the employee's network access can be terminated as soon as possible to prevent possible malicious destruction or alteration of ePHI by that employee.

SECURITY POLICIES AND PROCEDURES: INFORMATION ACCESS MANAGEMENT

Effective Date: January 1, 2005

Background:

45 CFR §164.308(a)(4) of the Security standards states that a covered entity “must implement policies and procedures for authorizing access to electronic protected health information (ePHI) that are consistent with the requirements of subpart E [the Privacy Rule] of this part.”

Purpose:

To establish the Medical Center Clinic’s (MCC) information access management process, including the required and addressable subordinate implementation specifications of: Isolating Healthcare Clearinghouse functions (R), Access Authorization (A), and Access Establishment and Modification (A).

Policy:

MCC is committed to implementing an information access management process to ensure that only employees with a determined need are granted access to the ePHI maintained in MCC’s computer systems. The following policies apply to all MCC’s ePHI and are the responsibility of the IS Director.

1. Isolating Healthcare Clearinghouse Function (Required)

Section 164.308(a)(4)(ii)(A) of the Security Rule states: “If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.” MCC has implemented the following procedures to address this requirement, and they are the responsibility of the IS Director.

- (a) Separate and specific accounts will be established for each of MedPro Solutions’ billing customers.
- (b) Access rights to MedPro Solutions billing client information shall be restricted to MedPro Solutions employees and designated IS Department technicians who must process the various data processing jobs and reports, and manage the electronic transmission of the data to and from the client organizations to preclude unauthorized access to the information. Access to MedPro billing client’s information by any other MCC employee shall be blocked.

2. Access Authorization (Addressable)

Section 164.308(a)(4)(ii)(A) of the Security Rule states: “Covered entities will implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.” MCC has implemented the following procedures to address this requirement, and they are the responsibility of the IS Director and the senior managers.

- (a) As addressed in the Workforce Security policy, all network users must have their access requirements specified as a part of their job descriptions, and each user must attend the appropriate training classes necessary to qualify for varying levels of access to ePHI within the network, as determined by the application managers and the Network Manager.
- (b) The IS Director will ensure user access requirements are periodically reviewed and that appropriate changes to user access are made as job requirements change.

3. Access Establishment and Modification (Addressable)

Section 164.308(a)(4)(ii)(A) of the Security Rule states: “Covered entities will implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.” MCC has implemented the following procedures to address this requirement, and are the responsibility of the IS Director and the senior managers.

- (a) As addressed in the Workforce Security policy, all network users must have their access requirements specified as a part of their job descriptions, and each user must attend the appropriate training classes necessary to qualify for varying levels of access to ePHI within the network, as determined by the application managers and the Network Manager. If employees are given greater responsibilities requiring an increased level of access, the senior managers must ensure that the employee’s job description is modified and that the employee is scheduled for further training to qualify for the increased access.
- (b) The IS Director, through the senior managers, will ensure that user access requirements are periodically reviewed and that appropriate changes to user access are made as job requirements change.

SECURITY POLICIES AND PROCEDURES: SECURITY AWARENESS AND TRAINING

Effective Date: January 1, 2005

Background:

45 CFR §164.308(a)(5)(i) of the Security standards states that covered entities must “implement a security awareness and training program for all members of its workforce (including management).”

Purpose:

To implement the Medical Center Clinic’s (MCC’s) Security Awareness and Training policies and the policies for the subordinate implementation specifications: Security Reminders, Protection From Malicious Software, Log-in Monitoring, and Password Management.

Policy:

MCC has implemented its Security Awareness and Training program to educate its workforce about security requirements and their obligations to protect the ePHI stored on and processed by the MCC network systems. The IS Director, in his role as the Security Officer, is responsible for implementing these policies and for ensuring that all MCC personnel comply.

1. Security Reminders: (Addressable)

Section §164.308(a)(5)(ii)(A) of the standard states that covered entities will “implement periodic security reminders.”

As an integral part of the overall security training plan, MCC has implemented the use of periodic security awareness reminders to educate the staff about the security requirements and their roles in complying with the standards. The initial series of awareness reminders will be distributed with pay stubs to all physicians and employees. Following the initial series, a routing distribution will occur on the last payday of each month to continue the information flow to all employees. The IS Director, in his capacity as Security Officer, is responsible for ensuring that this requirement is met.

2. Protection From Malicious Software: (Addressable)

Section §164.308(a)(5)(ii)(B) of the standard states that covered entities will “implement procedures for guarding against, detecting, and reporting malicious software.”

MCC has installed an enterprise level anti-virus solution to meet this requirement. Each workstation has had a client application installed to scan the local machine’s hard drive for malicious software and eliminate it. All MCC email is screened as it is sent or received and there is also special software installed to prevent “spyware” applications from being installed over Internet connections. The IS Director will assign responsibility within his department for monitoring and updating the technology used to comply with this standard.

All MCC network users are hereby notified that they must exercise due caution with regard to using the email and Internet connections provided to them by MCC. Downloading software from the Internet and installing it on local workstations without prior approval is prohibited. Forwarding of “chain letters” or other similar files via email is prohibited. Violation of this policy may result in the loss of privileges.

3. Log-in Monitoring: (Addressable)

Section §164.308(a)(5)(ii)(C) of the standard states that covered entities will “implement procedures for monitoring log-in attempts and reporting discrepancies.”

MCC has implemented a network management software solution to meet the requirements of this standard. All user log-ins are verified against confidential information tables before a login is allowed. If a user makes 3 unsuccessful attempts to login, the network management software temporarily disables that account until the user contacts the network administrator and explains the nature of the error. This prevents unauthorized persons from attempting to use repetitive guessing to break into the network. The network administrator is responsible for periodically reviewing the logs created by the monitoring software to ensure that it is functioning properly and to identify any problems or unauthorized attempts to access the network.

4. Password Management: (Addressable)

Section §164.308(a)(5)(ii)(D) of the standard states that covered entities will “implement procedures for creating, changing, and safeguarding passwords.”

MCC has established the following process for creating new network user accounts and for maintaining the password protections for those accounts.

- a) Each new network user will be assigned to training classes by their supervisor (via the HR department for new employees) based on the information access requirements established for their job. This training will take place as part of the new employee’s initial orientation training.
- b) At the completion of the network training class, each user fills out a form to establish their initial account username and password. This form is sent to the network administrator who ensures that the account is established no later than Friday of the training week, and that the various network application icons are available to the user based on the training classes completed.
- c) A user may attend further training to gain access to additional applications, or to gain a greater level of access to information within an application (e.g. for the EMR system, or for the billing system). The user’s supervisor must submit an authorization for training to the appropriate application trainer before the employee will be allowed to attend further training. At the completion of each new training class, the application instructor must forward a signed training completion form to the network administrator certifying that the required training has been completed, before the new access is granted.
- d) Supervisors are responsible for immediately notifying the network administrator as soon as it is known that an employee’s access requirements have changed (e.g. a job change to a position that no longer requires the same level of access to ePHI the employee had previously), or if the employee has resigned or has been terminated.
- e) The network administrator will disable the accounts of employees who have resigned or have been terminated as soon as the notification is received from the supervisor. Permanent account deletion will occur when formal notification is received from the HR department regarding employee terminations or resignations.

All users are hereby notified that the sharing of network usernames and/or passwords with another individual is prohibited and can result in sanctions. Knowingly violating this policy can result in termination for cause.

SECURITY POLICIES AND PROCEDURES: PRIVACY/SECURITY INCIDENT PROCEDURES

Effective Date: September 1, 2009

BACKGROUND:

Federal law requires that health care providers take measures to protect patient health information (PHI) and ensure that it is not used or disclosed except as authorized by the patient, or as permitted or required by law. Health care providers are also required to develop and implement policies and procedures to address security incidents.

PURPOSE AND SCOPE:

The purpose of this policy is to implement administrative and physical safeguards to ensure the confidentiality, integrity and availability of PHI that is maintained by the Medical Center Clinic ("MCC") and to protect PHI against unauthorized uses or disclosures. This policy statement establishes MCC's policies and procedures for reporting and responding to privacy and security incidents. It also serves to strengthen our privacy policies and procedures by including the reporting and mitigation of privacy incidents within the scope of this policy.

The scope of this policy covers the response to and reporting of privacy and security incidents, including the identification of and response to suspected or known incidents, and the documentation of security incidents and their outcomes. This policy applies to all staff, physicians, volunteers, students, contractors and subcontractors of MCC.

POLICY:

This policy is an action plan for addressing privacy and security incidents at MCC. All MCC personnel are required to comply with the following policies and procedures regarding the reporting and investigation of privacy and security incidents. The VP of Information Systems and Technology, in his role as the Security Officer, and the Corporate Compliance and Privacy Officer are responsible for implementing these policies to ensure that all MCC personnel comply.

1. Definitions

- **HIPAA:** The Health Insurance Portability and Accountability Act of 1996 limits the use and disclosure of patient health information that could associate an individual's identity with his or her health information and lays out the three types of security safeguards required for compliance: administrative, physical, and technical.
- **Protected Health Information:** PHI includes oral, written or otherwise recorded information that is created or received by MCC. PHI may relate to a patient's physical or mental health, payment, or the health care services provided to a patient.
- **Security or privacy incident:** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. This definition includes, but is not limited to, thefts, power failures, data loss and non-routine requests for patient information.
- **Security/Privacy Officer:** The MCC official(s) designated as the person(s) responsible for PHI security, the development of policy and procedures and the methods for facilitating those policies and procedures.

2. Identification

Health care providers are required to identify suspected or known security incidents. All MCC employees must be vigilant for suspicious activities or security vulnerabilities.

- Be aware of who has access to workstations within your designated work area to significantly reduce attempts by unauthorized users to access electronic protected health information ("ePHI").
- If an unauthorized disclosure or acquisition of private data occurs, or is suspected to have occurred, take proactive steps to correct the situation, if possible. Such actions may include rescuing and removing the document left in a public place; shutting down the affected computer or server; or locking an area with access to private data.

3. Response and Reporting

Health care providers are required to report suspected or known security incidents.

If you observe or become aware of any activity that seems suspicious or out of the ordinary:

- Immediately contact and report that activity to your supervisor.
- Complete a Privacy/Security Incident Form. The form is available, along with all other HIPAA forms, on the Employee Intranet. The Privacy/Security Incident Form must be completed no later than the end of the shift or workday and immediately forwarded to the Privacy Officer.
- The completed Privacy/Security Incident Form must include the details of the incident and the reporting employee's contact information. It must also include the date, time and location of the incident, including, if appropriate, the location of found documents. It should include a clear description of what happened and, if known, how the breach occurred, the type of private data involved (for example, paper records, electronic records, or other type of data). If other persons involved are known, their names, titles, contact information, and how they were involved should be included.
- Supervisors shall contact and report incidents to the Privacy Officer.

4. Documentation & Mitigation

Health care providers are required to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes.

- A. Documentation:** The Privacy rule requires that inappropriate uses and disclosures be reported and mitigated.
- Supervisors will immediately forward all Privacy/Security Incident Forms to the Privacy Officer, along with as much supporting information possible to assist in the investigation of the incident.
 - Supervisors must ensure that Privacy/Security Incident Forms include: the name of the employee making the report; the date and time of the incident being reported; details of the circumstances surrounding the event; and any observed behaviors that led to the incident being suspected.
- B. Risk Assessment:** The Privacy rule requires that a risk assessment be performed to determine whether the impermissible acquisition, access, use, or disclosure of PHI presents a significant risk of harm to the individual as a result of the impermissible activity and therefore requires notification of the breach to the affected individual and federal authorities. The Risk Assessment shall be performed and documented by the Privacy Officer.
- C. Follow Up and Mitigation:** The Privacy rule requires that steps be taken to mitigate inappropriate uses and disclosures and diminish any harmful effects of a breach.
- If the incident involved the actual penetration of the network via a network workstation, the Security or Privacy Officer will immediately have that workstation secured and disconnected from the network until a thorough investigation of the equipment can be completed to ensure that it has not been compromised.
 - The Privacy Officer will launch an investigation of the reported incident and record all findings for future reference. The incident report and the resulting investigation report shall be retained for a minimum of 6 years from the date of the incident. As part of the investigation, the Privacy Officer will attempt to determine if the incident occurred because of a lack of procedure, or failure to adhere to procedure. Once the investigation is completed, the Privacy Officer will create an Incident Outcome Report.
 - When warranted, the Privacy Officer or another individual designated by the Privacy Officer will contact local law enforcement officials and seek their assistance in resolving the incident.
 - The Privacy Officer will update procedures or new develop new procedures, depending on the outcomes of the investigation.
 - Incidents resulting from an employee inappropriately accessing or disclosing PHI may result in sanctions being taken against the employee as outlined in MCC's Employee Sanctions policy.

- After the risk assessment and investigation, if notification of affected persons or mitigation is required, departments and/or individuals involved in the privacy breach may be asked to assist with the notification process and/or in mitigating the harmful effects.

FORM ATTACHMENT(S)

1. Privacy and Security Incident Report

PRIVACY AND SECURITY INCIDENT REPORT

Legibly Print All Information

IMMEDIATELY FAX COMPLETED AND SIGNED FORMS TO 850-474-8275 ATTN: SHARON HOYLE

Incident Date:		Incident Time:		Incident Location:	
Patient Name Whose PHI Is Involved <i>(if more than one, list on back of this form, or provide list)</i>				Patient MCC#	
Phone Number Where Patient Can Be Reached:					
Nature of Incident:					
Describe any harm to patient or negative outcome:					Is the patient aware of the incident? <input type="checkbox"/> YES <input type="checkbox"/> NO
Persons Involved In This Incident Are <i>(include individual(s) and or entity who received PHI)</i> :					
Name		Title/Position		Can Be Reached At:	
How was this person involved?					
Name		Title/Position		Can Be Reached At:	
How was this person involved?					
Name		Title/Position		Can Be Reached At:	
How was this person involved?					
Patient Information Involved: <input type="checkbox"/> Electronic Record <input type="checkbox"/> Paper Record <input type="checkbox"/> Other		Describe the Patient Information involved in as much detail as possible: <i>(Check all that apply)</i> <input type="checkbox"/> Patient Name <input type="checkbox"/> Patient Address <input type="checkbox"/> Medical Record # <input type="checkbox"/> Diagnosis <input type="checkbox"/> Social Security # <input type="checkbox"/> Financial Information Other Information – Please Describe <i>(attach separate sheet if necessary)</i> :			
Who Was Notified of This Incident? <i>(Provide Names and Titles)</i>					
Describe Any Immediate Remedial Actions/Interventions, if any:					
Report Completed By <i>(print legibly)</i> :			Title		Extension
Signature				Date	

SECURITY POLICIES AND PROCEDURES: CONTINGENCY PLAN

Effective Date: January 1, 2005

Background:

45 CFR §164.308(a)(7)(i) of the Security standards states that covered entities must “establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.”

Purpose:

To implement the Medical Center Clinic’s (MCC’s) Contingency Plan and its subordinate implementation specifications: the Data Backup Plan, the Disaster Recovery Plan, the Emergency Mode Operations Plan, the Testing and Revision Plan, and the Applications and Criticality Analysis.

Policy:

MCC has implemented its Contingency Plan in the form of an Information Security Standards and Practices Manual (ISSPM). This manual defines the specific plans and procedures to follow in the event of an emergency or other type of disaster that damages, or threatens to damage, the MCC network system and the ePHI maintained on that system. The IS Director is responsible for ensuring that all IS personnel follow the policies contained in this manual and that the manual is periodically reviewed and updated to ensure its compliance with the rule.

1. Data Backup Plan: (Required)

Section §164.308(a)(7)(i)(A) of the standard requires that covered entities “establish and maintain procedures to create and maintain exact copies of protected health information.”

MCC has implemented and maintains a Data Backup Plan, as detailed in the ISSPM, to meet the requirement of this implementation specification. The plan assigns responsibilities to designated IS personnel (as shown in Appendix A of the ISSPM) for creating and storing the data backups in a designated safe storage location, which will protect the media from fire and/or water damage. Daily rotation of the backup media is required under the plan. The IS Director is responsible for ensuring that all IS personnel follow the guidance set forth in the published procedures.

2. Disaster Recovery Plan: (Required)

Section §164.308(a)(7)(i)(B) of the standard requires that covered entities “establish (and implement as needed) procedures to restore any loss of data.”

MCC has implemented and maintains a Data Backup Plan, as detailed in the ISSPM, to meet the requirement of this implementation specification. The IS Director is responsible for assigning responsibilities to all IS personnel during an emergency and for ensuring that they follow the guidance set forth in the published procedures. The IS Director will also ensure that the Disaster Recovery Plan is periodically tested, reviewed, and updated to reflect the most current requirements of the Security standards.

3. Emergency Mode Operation Plan: (Required)

Section §164.308(a)(7)(i)(C) of the standard requires that covered entities “establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.”

MCC has implemented and maintains an Emergency Mode Operation Plan, as detailed in the ISSPM, to meet the requirement of this implementation specification. The IS Director is responsible for ensuring that all IS personnel follow the guidance set forth in the published procedures, and for updating the plan following any actual emergency situation.

4. Testing and Revision Procedures: (Addressable)

Section §164.308(a)(7)(i)(D) of the standard states that covered entities will “implement procedures for periodic testing and revision of contingency plans.”

As detailed in the ISSPM, the IS Director is responsible for establishing a process to periodically review, test, and update the Contingency Plan and its subcomponents to ensure that they meet the most current requirements of the standard. The revision process will also allow for updating the technologies used to comply with the standard.

5. Applications and Data Criticality Analysis: (Addressable)

Section §164.308(a)(7)(i)(E) of the standard states that covered entities will “assess the relative criticality of specific applications and data in support of other contingency plan components.”

MCC has conducted an application and data criticality assessment, the most current version of which is maintained as an appendix to the ISSPM. The IS Director is responsible for ensuring that this analysis is updated as part of the periodic review of the Contingency Plan.

SECURITY POLICIES AND PROCEDURES: EVALUATION

Effective Date: January 1, 2005

Background:

45 CFR §164.308(a)(8) of the Security standards requires that covered entities “perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.”

Purpose:

To implement the Medical Center Clinic’s (MCC’s) policies and procedures for the management of the process for periodically reviewing and evaluating MCC’s security policies and procedures for compliance with the rule.

Policy:

MCC shall periodically (at least annually as a minimum) conduct a technical and a non-technical review of its security safeguards to determine if they appropriately meet the compliance standards of the Security Rule given the MCC environment in which they have been implemented. These evaluations may be conducted by an internal IS department employee, or MCC may use the services of an outside contractor. The IS Director, in his role as the Security Officer, is responsible for implementing this policy and for ensuring that the evaluations are completed.

Prior to the evaluations taking place, the IS Director will have a current diagram and listing of the network systems prepared, as well as an up-to-date inventory of all computer and network equipment and software. The evaluations will include (as a minimum):

- Review of the security policies and procedures for correctness and completeness;
- Review of all training, incident reporting, and log-in monitoring logs for completeness and proper use;
- Interviews with employees to determine level of knowledge and awareness as well as compliance with policies and procedures;
- After-hours walkthrough inspections to assess physical security and employee compliance with policies;
- Review of the network control procedures to determine adequacy and completeness;
- Review of automated monitoring systems to determine effectiveness and use;
- Functionality and correctness of security controls and anti-virus software; and
- Testing of Contingency Plan elements to determine their adequacy and completeness.

The evaluator(s) will prepare a final written report detailing the results of the evaluations and submit it to the Security Officer. The evaluation report will be retained for a period of six years from the date of the report. The Security Officer will follow-up on any deficiencies identified to ensure that procedures are modified or new ones implemented to mitigate the deficiencies.

SECURITY POLICIES AND PROCEDURES: BUSINESS ASSOCIATE CONTRACTS OR OTHER ARRANGEMENTS

Effective Date: January 1, 2005

Background:

45 CFR §164.308(b)(1) of the Security standards states that “a covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information.”

Purpose:

To implement the Medical Center Clinic’s (MCC) policy regarding business associate contracts and other arrangements.

Policy:

MCC is committed to protecting the ePHI that it maintains, and has implemented the use of business associate contracts or other arrangements that are compliant with the requirements of the Privacy and the Security rule standards and implementation specifications.

1. Written Contract or Other Arrangement (Required)

Section 164.308(b)(4) contains the implementation specification for this requirement and states that a covered entity “must document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).”

Section 164.314(a) requires that such contracts provide that the business associate will:

- “Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, maintains, or transmits on behalf of the covered entity as required by this subpart;”
- “Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;”
- “Report to the covered entity any security incident of which it becomes aware;”
- “Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.”

MCC has reviewed the language of its business associate contracts and other arrangements to ensure that the requirements of the above, as well as those of the Privacy Rule, have been incorporated.

SECURITY POLICIES AND PROCEDURES: FACILITY ACCESS CONTROLS

Effective Date: January 1, 2005

Background:

45 CFR §164.310(a)(1) of the Security standards states that covered entities “must, in accordance with §164.306, implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”

Purpose:

To implement the Medical Center Clinic’s policies regarding the HIPAA Security standard for Facility Access Controls and the its subordinate implementation specifications: Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, and Maintenance Records.

Policy:

MCC has implemented its policies to comply with the standard for Facility Access Controls as part of an Information Security Standards and Practices Manual (ISSPM). The IS Director is responsible for ensuring that all IS personnel follow the policies contained in this manual and that the manual is periodically reviewed and updated to ensure its compliance with the rule.

1. Contingency Operations: (Addressable)

Section §164.310(a)(2)(i) of the standard states that covered entities must “establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.”

The specific policies and procedures implemented to comply with this section can be found at pages 23 and 24 of the ISSPM.

2. Facility Security Plan: (Addressable)

Section §164.310(a)(2)(ii) of the standard states that covered entities must “implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.”

- A. First element
- B. Second element
- C. Third element.

3. Access Control and Validation Procedures: (Addressable)

Section §164.310(a)(2)(iii) of the standard states that covered entities must “implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.”

The specific policies and procedures implemented to comply with this section can be found at pages 23 and 24 of the ISSPM.

4. Maintenance Records: (Addressable)

Section §164.310(a)(2)(iv) of the standard states that covered entities must “implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).”

The specific policies and procedures implemented to comply with this section can be found at pages 23 and 24 of the ISSPM.

SECURITY POLICIES AND PROCEDURES: WORK STATION USE

Effective Date: January 1, 2005

Background:

45 CFR §164.310(b) of the Security standards requires that covered entities “implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected health information.”

Purpose:

To implement the Medical Center Clinic’s (MCC’s) policies and procedures regarding the proper use of workstations.

Policy:

This policy applies to all physicians, employees, contractors, consultants, temporaries, and other workers who are granted access to the MCC network system. Inappropriate use of workstations and the MCC network can expose the Clinic to unacceptable risks including compromise of network systems and services, virus attacks, and legal issues.

1. Physical Attributes of Workstation Surroundings –

- a. Workstations shall be placed in controlled access areas where their use can be constantly monitored by MCC employees at all times;
- b. Workstations that are in public access areas must have a visual block from the area immediately behind the workstation so unauthorized personnel can not view the monitor screen, and the authorized users who access these workstations must use screensavers and lock the workstation when they are not present;
- c. Nurse’s workstations that are located in hallways must located where access can be monitored by other staff members when the authorized users is not present;
- d. Workstation screens at PSR check-in desks and other staff positions must not be visible to patients or others who approach the desks from the front;
- e. Staff must prevent unauthorized individuals from lingering near workstations that are in use.

2. Proper Use – Workstations are provided to authorized network users for the following purposes:

- a. To access patient electronic medical records, billing accounts, scheduling information, and laboratory and imaging results;
- b. To enhance the communications capabilities between staff members by providing email services for sending and receiving work related email;
- c. To access the Internet to search for educational information, to research work related issues, to look up federal or state regulations or statutes that govern health care and related services, to search for commercial solutions to work related issues.

3. Improper Use – The following are considered to be improper uses of workstations provided to MCC employees:

- a. Revealing your account username and password to others or allowing the use of your account by others;
- b. Accessing data that the employee is not authorized to access;
- c. Introducing malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
- d. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of copyrighted software for which MCC does not have an active license;
- e. Downloading and installation of games, screensavers, cursor files;
- f. Creating or forwarding of “chain letters”, “Ponzi” or other “pyramid” schemes, “junk mail”, or other materials that may be offensive in nature (e.g. sexually explicit pictures or text, crude language, racially oriented, etc.);
- g. Posting of non-business-related messages or solicitations;

h. Messages intended to communicate political or religious beliefs to others.

MCC reserves the right to monitor all user network activity to ensure compliance with this policy and to protect the confidentiality of the ePHI maintained on the network. Employees who choose not to comply with this policy will be subject to disciplinary actions up to and including termination.

SECURITY POLICIES AND PROCEDURES: WORK STATION SECURITY

Effective Date: January 1, 2005

Background:

45 CFR §164.310(c) of the Security standards requires that covered entities “implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.”

Purpose:

To implement the Medical Center Clinic’s (MCC’s) policies and procedures regarding workstation security.

Policy:

This policy applies to all physicians, employees, contractors, consultants, temporaries, and other workers who are granted access to the MCC network system. All users must exercise due diligence to guard the integrity, confidentiality, and availability of the ePHI maintained on the MCC.

1. Only those individuals who have been approved for and have completed the required training will be granted access rights to the MCC network and other applications maintained on the system.
2. Authorized users are not permitted to share their user password or account with other individuals.
3. All workstations have had anti-virus software loaded, which performs an automatic update and scan each time the workstation is started. Users are not permitted to alter or otherwise interfere with the operation of this software.
4. As of January 1, 2005 all users will be required to change their network password every 120 days.
5. All workstations have been placed in areas where members of MCC’s staff can monitor their use at all times during the workday. MCC staff will ensure that the suspicious individuals are asked to leave the area of a workstation or to stop any suspicious activity immediately, and report such suspicious individuals or activity to their supervisor as soon as possible. Supervisors will document the incident and report it to the Security Officer as soon as possible.
6. Users who must leave their workstation unattended and logged into the network must lock the workstation by pressing Ctrl+Alt+Del and selecting Lock Workstation from the options menu before leaving the workstation.
7. All workstations must be logged out of the network before users leave at the end of their shift. If no other individual will be using the workstation following their shift, users should turn off the workstation.
8. Physical access to the computer room is restricted to authorized IS personnel, or to individuals who are escorted at all times by an IS department member while in the facility.
9. Electronic key fobs have been issued to IS personnel to access the computer facility. These fobs may not be shared with others.
10. The IS Director, or the designated alternate, will collect electronic key fobs and or pass keys from personnel who are terminated, upon notification of such action by the Human Resources Department.

SECURITY POLICIES AND PROCEDURES: DEVICE AND MEDIA CONTROLS

Effective Date: January 1, 2005

Background:

45 CFR §164.310(d)(1) of the Security standards states that covered entities “must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.”

Purpose:

To implement the Medical Center Clinic’s policies regarding the standard for Device and Media Controls and the its subordinate implementation specifications: Media Disposal, Media Re-use, Media Accountability, and Data Backup and Storage (during transfer).

Policy:

The following policies are applicable to all MCC employees, physicians, volunteers, and Business Associates. Supervisors are responsible for ensuring that their employees adhere to these policies. The IS Director/Security Officer is responsible for ensuring that all IS personnel follow these policies and that the policies are periodically reviewed and updated to ensure its compliance with the rule.

1. Media Disposal: (Required)

Section §164.310(d)(2)(i) of the standard states that covered entities must “implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.”

Reusable Media: Reusable media (e.g., floppy diskettes, DAT tapes, rewriteable CDs and DVDs, USB flash cards or sticks, internal hard disks) must have all ePHI completely removed prior to disposal or reuse.

To ensure that this policy is followed, all MCC computer users must return reusable media to the IS Department for disposal. Supervisors shall provide a container (e.g., a small empty box) for their employees to place such media into, and shall notify the IS Help Desk when the container needs to be emptied. The collection container must be located in an area that is under constant surveillance by employees during work hours and secured after hours. Once the IS Department picks up the returned media, it will take the necessary steps to completely wipe the reusable media of any ePHI before disposing of it and will record those actions in a log which will be maintained for a period of six years from the date of the entry.

Computer equipment: All computer equipment must be returned to the IS Department for disposal to ensure that no ePHI is inadvertently released from the Clinic.

Supervisors will notify the IS Help Desk when computer equipment is to be removed from service. The IS Department will pick up the equipment and take the necessary steps to remove and completely wipe any reusable internal hard drives of ePHI before disposal of the computer equipment. Hard drives removed and deemed non-reusable shall be electronically degaussed prior to disposal. The computer inventory will be updated to reflect the change in the equipment at the source location and a record of computer and hard drive disposals (by serial number) shall be maintained for a period of six years from the date of the entry for future reference.

2. Media Re-use: (Required)

Section §164.310(d)(2)(ii) of the standard states that covered entities must “implement procedures for the removal of electronic protected health information from electronic media before the media are made available for re-use.”

All reusable media must be cleansed of any ePHI before it can be reused. To ensure that this policy is followed, all MCC computer users must return reusable media to the IS Department for erasure. Supervisors will instruct their employees to place such media into the collection box provided in their area and shall notify the IS Help Desk when the container needs to be emptied. The collection container must be located in an area that is under constant surveillance by employees during work hours and secured after hours. Once the IS Department picks up the returned media, it will take the necessary steps to completely wipe the reusable media of any ePHI before recycling it for reuse.

3. Accountability: (Addressable)

Section §164.310(d)(2)(iii) of the standard states that covered entities must “maintain a record of the movements of hardware and electronic media and any person responsible therefore.”

The IS Director/Security Officer will ensure that a formal method of inventorying computer and network equipment is implemented. Inventory logbooks will be used, and each logbook will have an “opened” and “closed” date record inside the front cover. Logbooks will be maintained for a minimum of six years from the “closed” date.

No computer or network equipment may be moved except by IS personnel. Supervisors are responsible for providing IS with a minimum of 5 workdays advanced notice of required moves. The technician performing the move will provide the Network Manager with the serial numbers of the equipment moved, as well as the “from point” and the “end point” locations. The Network Manager will make the appropriate entries in the inventory logs.

4. Data Backup and Storage: (Addressable)

Section §164.310(d)(2)(iv) of the standard states that covered entities must “create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.”

The assigned responsibilities and specific back-up procedures are detailed in the Backup Plan contained in the MCC Information Security Standards and Practices Manual (ISSPM).

SECURITY POLICIES AND PROCEDURES: ACCESS CONTROL

Effective Date: January 1, 2005

Background:

45 CFR §164.312(a)(1) of the Security standards states that covered entities “must implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).”

Purpose:

To implement the Medical Center Clinic’s policies regarding the standard for Access Control and the its subordinate implementation specifications: Unique User Identification, Emergency Access Procedures, Automatic Logoff, and Encryption and Decryption (for data at rest).

Policy:

All authorized users of the MCC network shall adhere to the policies and procedures set forth in this document. The Security Officer is responsible for ensuring that the policies contained in this document are periodically reviewed and updated to ensure continued compliance with the rule.

1. Unique User Identification: (Required)

Section §164.312(a)(2)(i) of the standard states that covered entities must “assign a unique name and/or number for identifying and tracking user identity.”

As outlined in the MCC Information Security Standards and Practices Manual (ISSPM), each network user is granted a level of access based on their job function (as defined in the user’s job description by their supervisor) and must complete the required training classes for the defined level of access.

At the completion of the network training class, each user signs a confidentiality agreement and fills out a user name/password request form indicating the username and password they want to have initially set up for their account. Passwords must be at least 6 characters long, containing letters and numbers, and may not contain any of the non-alphanumeric characters on a standard keyboard (!@#\$%^&*()_+~[]{}|<>^`~). The original form is forwarded to the Network Administrator, who sets up the user’s account in the network, and a copy is sent to the designated application manager responsible for setting up user accounts for the billing, scheduling, or EMR applications (each has a designated application manager).

Supervisors are responsible for identifying new access requirements for network users, and for scheduling the user for the appropriate training to achieve the new access level. Supervisors shall ensure that users are not given access to information requiring a higher access level before they have completed the required training. Such “unauthorized” access would violate the Privacy Rule’s Minimum Information Necessary requirement.

2. Emergency Access Procedure: (Required)

Section §164.312(a)(2)(ii) of the standard states that covered entities must “establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.”

MCC has implemented its policies to comply with the standard for Emergency Access Procedures as part of its comprehensive Information Security Standards and Practices Manual (ISSPM). Within the IS department, specific individuals have been designated to act as alternates to the regular data managers in case of an emergency and procedures for emergency access to ePHI have been outlined.

3. Automatic Logoff: (Addressable)

Section §164.312(a)(2)(iii) of the standard states that covered entities must “maintain implement procedures that terminate an electronic session after a predetermined time of inactivity.”

MCC has set the network user account access to automatically terminate after 30 minutes of system inactivity. All system users are provided training regarding this feature when they attend the training sessions required before their account access is granted. Additionally, a password protected screen saver will display to hide any screen information after 15 minutes of system inactivity.

4. Encryption and Decryption (data at rest): (Addressable)

Section §164.312(a)(2)(iv) of the standard states that covered entities must “implement a mechanism to encrypt and decrypt electronic protected health information.”

MCC does not use an encryption scheme for its stored application data. Rather, it utilizes proprietary database structures to store the information on the various servers. The information cannot be accessed without using the database application that created the data, and access to those applications is controlled by the username and password settings as described above. As further protection, access to the data storage area on MCC's servers is tightly controlled and limited to the designated database administrators (refer to the MCC ISSPM for the current list) to prevent unauthorized access. Database managers are responsible for verifying data integrity via their software logs on a daily basis.

SECURITY POLICIES AND PROCEDURES: AUDIT CONTROL

Effective Date: January 1, 2005

Background:

45 CFR §164.312(b) of the Security standards states that covered entities “must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”

Purpose:

To implement the Medical Center Clinic’s policies regarding the standard for Audit Control.

Policy:

All Medical Center Clinic network user activity will be recorded in electronic logs that are periodically reviewed to ensure that users are adhering to the policies that govern the use of ePHI stored and processed on the Clinic’s network.

Logs of network user activity will track all network log-ins and log-outs. Failed log-in attempts will be flagged as potential attempts at unauthorized access and followed up in a manner outlined by the Security Officer at the time. Investigations that reveal a true unauthorized login attempt will be summarized in an incident report and kept on file for 6 years from the date of. The incident report will state if any employee sanctions were applied as outlined in the MCC Security Management Process policy.

Individual application usage logs will track the EMR, digital filing, and billing systems that are accessed and which records are opened. The logs will match file access to the user access level authorization on file. The network administrator (or designated alternate), in conjunction with the Security Officer, will periodically review the activity logs to identify inconsistencies and possible unauthorized accesses. Reports of activity log reviews will be maintained for a period of 6 years from the date of the review and will include information about any employee sanctions applied, if applicable.

The Security Officer is responsible for ensuring that the procedures enacted to comply with this policy are periodically reviewed and updated to ensure continued compliance with the rule. This may be conducted by a third party or by a designated MCC employee. A summary report of such reviews will be maintained for a period of 6 years from the filing date.

SECURITY POLICIES AND PROCEDURES: DATA AUTHENTICATION

Effective Date: January 1, 2005

Background:

45 CFR §164.312(c)(1) of the Security standards states that covered entities “must implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”

Purpose:

To implement the Medical Center Clinic’s policies regarding the standard for Data Authentication.

Policy:

The following policies have been implemented to protect the ePHI stored and processed on the MCC network.

1. Mechanism to Authenticate ePHI: (Addressable)

Section §164.312(c)(2) of the implementation specification states that covered entities must “implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”

Database managers utilize a series of SQL system tools, programs, and logs to verify the integrity of ePHI that is stored and processed on the EMR (Oracle), Context, and Great Plains servers. Daily reviews of these tools are conducted to ensure that data is not inadvertently altered or destroyed.

The vendor (McKesson) for the main billing system application monitors that application’s data under a maintenance/support contract, and they also process the electronic claims generated by the system. The data structures used are proprietary to McKesson and are protected from access by others. This monitoring ensures the integrity of the billing information processed.

The Security Officer is responsible for ensuring that the procedures enacted to comply with this policy are periodically reviewed and updated to ensure continued compliance with the rule.

SECURITY POLICIES AND PROCEDURES: PERSON OR ENTITY AUTHENTICATION

Effective Date: January 1, 2005

Background:

45 CFR §164.312(d)(1) of the Security standards states that covered entities “must implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”

Purpose:

To implement the Medical Center Clinic’s policies regarding the Security standard of Person or Entity Authentication.

Policy:

All MCC employees seeking access to the MCC network and the applications that it supports must satisfy a user authentication mechanism before they will be granted login authorization. MCC has implemented the use of unique user identification and passwords to satisfy this requirement. The MCC policy on Access Control and the MCC Information Security and Standards and Practices Manual (ISSMP) detail the process for issuing and maintaining network user names and passwords, as well as individual levels of access authorization.

All MCC network users seeking access to the network and the applications that it supports must not misrepresent themselves by using another user’s ID and password.

MCC network users are not permitted to allow other persons or entities to use their unique user ID and password to access the network and the applications that it supports.

The Security Officer is responsible for ensuring that the procedures enacted to comply with this policy are periodically reviewed and updated to ensure continued compliance with the rule.

SECURITY POLICIES AND PROCEDURES: TRANSMISSION SECURITY

Effective Date: January 1, 2005

Background:

45 CFR §164.312(e)(1) of the Security standards states that covered entities “must implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”

Purpose:

To implement the Medical Center Clinic’s policies regarding Transmission Security and its subordinate implementation specifications: Integrity Controls (Addressable) and Encryption (Addressable).

Policy:

MCC has implemented its policies to comply with the standards for Integrity Controls and Encryption. The IS Director is responsible for ensuring that all IS personnel follow these policies and that the policy is periodically reviewed and updated to ensure its compliance with the rule.

1. Integrity Controls: (Addressable)

Section §164.314(e)(2)(i) of the standard states that covered entities must “establish implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.”

The only data routinely transmitted by MCC involves billing data submitted to our clearinghouse for processing and submission. This transmission is conducted via an FTP dial-up link utilizing the built-in integrity controls of the McKesson software. As the stream is processed, the software checks packet integrity. If a problem is encountered, the process automatically resends the data under McKesson controls.

2. Encryption: (Addressable)

Section §164.314(e)(2)(ii) of the standard states that covered entities must “implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”

MCC physicians and remote satellite offices can connect to the MCC network via Microsoft Citrix Server links. This process establishes a virtual private network (VPN) connection for each user that is protected by 128-bit encryption. Additionally, because the processing takes place behind the firewall, unauthorized access or monitoring is prevented. As new remote users are identified, accounts are established and the users are trained on how to make the connections. All remote connections are pre-verified to ensure that they are authorized to make such access.

“At-Home” transcriptionists connect to the MCC network via PC Anywhere dial-up connections. These connections make use of the built-in 128-bit encryption of the PC Anywhere software. Each new “at home” transcriptionist account is requested by the transcription manager via the EMR coordinator/Privacy Officer to ensure that only authorized users are setup.

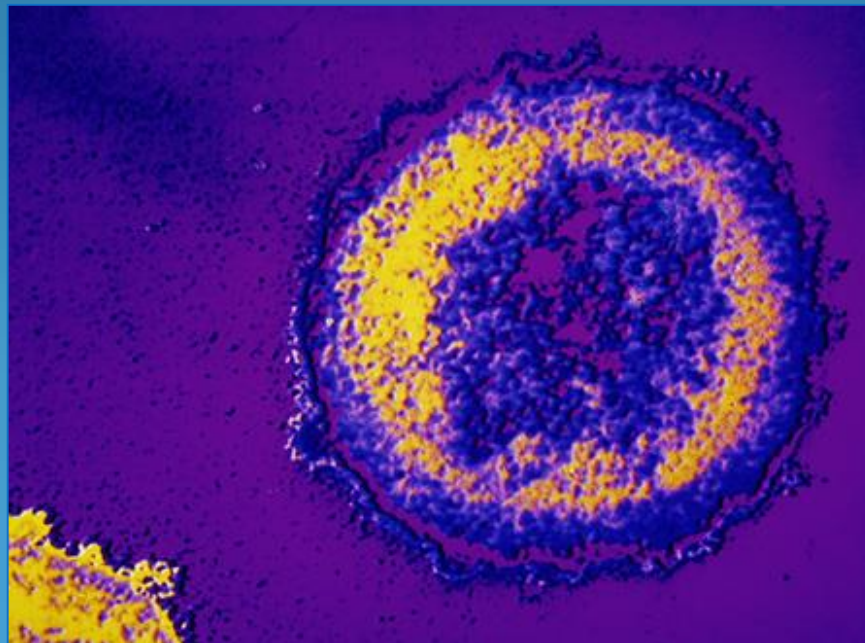
Medical Training Consultants Safety Training for Medical Center Clinic

Bloodborne Pathogens 29 CFR 1910.1030

Hazardous Communications (HCS/GHS 2012) 29 CFR 1910.1200

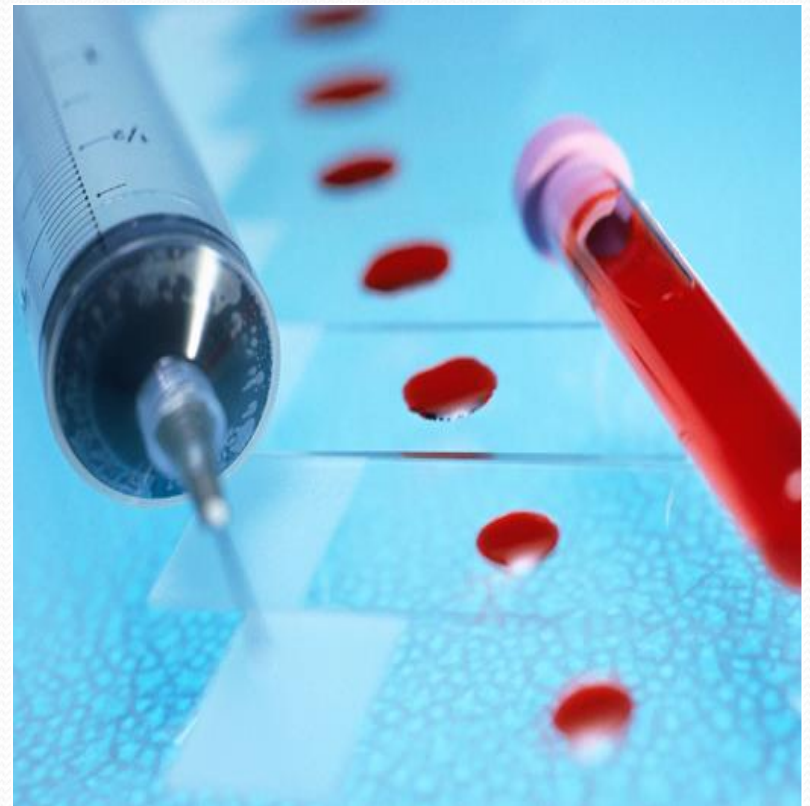
Biomedical Waste Florida 64E-16

Fire and Emergency 29 CFR 1910.38,157



Bloodborne Pathogens

- Are pathogenic micro-organisms present in human blood that can lead to diseases.
- Examples of such diseases, but not limited to just these, are:
 - Human immuno-deficiency virus (HIV)
 - Hepatitis B (HBV)
 - Hepatitis C (HCV)



Potentially Infectious Bodily Fluids

- Blood
- Saliva, vomit, urine
- Semen or vaginal secretions
- Skin, tissue, cell cultures
- Other body fluids, except sweat and tears

Important Elements of the Exposure Control Plan

- Be aware of your exposure potential
- Use safe work practices
- Know how to properly decontaminate equipment and surfaces
- Select and use proper PPE (gowns, gloves, goggles)
- Know how to properly handle biomedical waste
- Be aware of biohazard labels and signs
- Complete all training requirements (OSHA training before starting your job and then annually thereafter)
- Recordkeeping requirements (keep for three years)
- HBV

Personal Protective Equipment

- Ensure you have access to and are trained on the proper use of PPE
- If respirators are required they must fit properly and must be fit tested annually (with documentation)
- Change gloves after each patient
- Use proper technique when removing gloves
- Follow with hand washing (with soap and water)
- CDC hand hygiene procedures (wash for 20 seconds with soap and running water)
 - *alcohol gel can be used if not visibly contaminated
- Know where the eye wash station is located in your department and how to use it properly

Safe Work Practices

- Remove contaminated PPE or clothing as soon as possible
- Thoroughly wash immediately after exposure with soap and running water
- Clean and disinfect contaminated equipment and work surfaces
- Properly dispose of contaminated items in biohazard container
- Document incident

HBV Vaccination

- Strongly endorsed by medical communities
- Shown to be safe for infants,
- children, and adults
- Offered to all potentially exposed **employees**
 - * (externs and students must bring in proof of vaccinations to MCC prior to starting work)
- Provided at no cost to **employees**
- A Declination Form must be completed if vaccination is refused and kept on file



Exposure Incident

- An exposure incident is a specific incident of contact with potentially infectious blood or body fluids
- If there is no infiltration of mucous membranes or open skin surfaces, it is not considered an occupational exposure
- Report all accidents involving blood or bodily fluids immediately to your department manager and HR
- Post-exposure medical evaluations are offered

Post-exposure Evaluation

- Includes a confidential medical evaluation
- Documents route of the exposure
- Identifies the source individual
- Tests source individual's blood with individual's consent
(May use blood obtained for other testing without patient consent.)
- Provide results to exposed employee/student



Hazard Communication

HCS/GHS 2012

- You have the right to know and to have the knowledge to know what hazardous chemicals you will be working with
- Know where the Medical Center Clinic's OSHA Compliance Manual for the department to which you are assigned is located (ask the department supervisor to show it to you)
- You must read the MSDS/SDS (material safety data sheets/ safety data sheets) for the chemicals you will be working with
- Know the dangers of chemicals in your work area
- Ask if you have questions

Handling Medical Waste

- Regulated Medical Waste (RMW) can produce infectious diseases in humans and must be handled appropriately
- RMW includes, but is not limited to:
 - Blood, semen, vaginal secretions, cerebrospinal fluid
 - Synovial fluid, pleural fluid, peritoneal fluid
 - Pericardial fluid and amniotic fluid
 - Unfixed tissues or organs, cell or tissue and organ tissues

Handling Medical Waste

(cont)

- Cultures and stocks of microorganisms
- Animal carcasses
- Body parts infected for research
- Waste from a patient in isolation
- Products contaminated with body fluids
 - RMW must be placed in red labeled bags
 - Needles must be placed in puncture-resistant, leak-proof sharps containers

Fire Safety

- Know the exits and emergency routes out of the building
- Know where you are to meet for your department's head count
- RACE to safety
 - Rescue patients
 - Activate alarm
 - Confine blaze
 - Extinguish if possible or evacuate

Fire Safety

(cont)

- Never open a hot door
- Stay low to the floor to avoid smoke
- PASS to use extinguisher
 - Pull the pin
 - Aim at base of fire
 - Squeeze the trigger
 - Sweep side to side

Questions while at an MCC Facility?

Contact the Department Manager

Or

Debbie Ray Kings, RN,
Risk Manager, at 474-8625

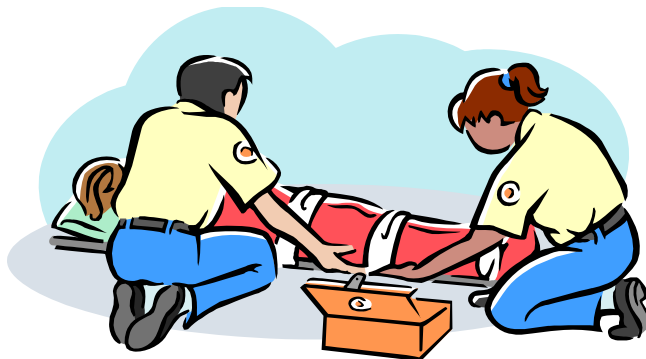
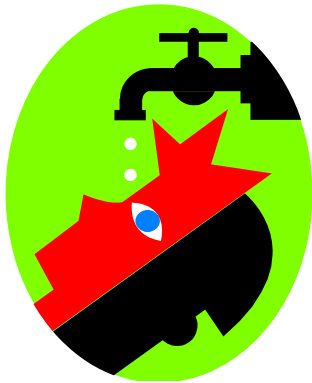
Or

Sommer Hall
Employee Health, at 474-8023





RISK MANAGEMENT



What is Risk Management?

The process of *making and carrying out decisions* that will assist in *prevention of adverse consequences* and *minimize the adverse effects* of accidental losses upon an organization.

What is a Risk Manager?

A professional working in either healthcare or law to focus on the *prevention of adverse consequences* &/or *minimize the adverse effects* of accidental losses upon the organization.

Who Is Responsible for Risk Management?

Everyone!!!

(It takes all of us working together to have an effective risk management program –
All departments, services and personnel, including volunteers & students)

Risk Management Staff

Debbie Ray Kings, RN-BC, CPHRM, Risk Management Coordinator

Office: 850-474-8625

Cell: 850-777-7620

James D. Frost, M.D., Medical Director

Office: 850-474-8217

Cell: 850-390-2138

General Liability

Negligence for Hazards in the Environment
& Non-Professional Judgments/Actions

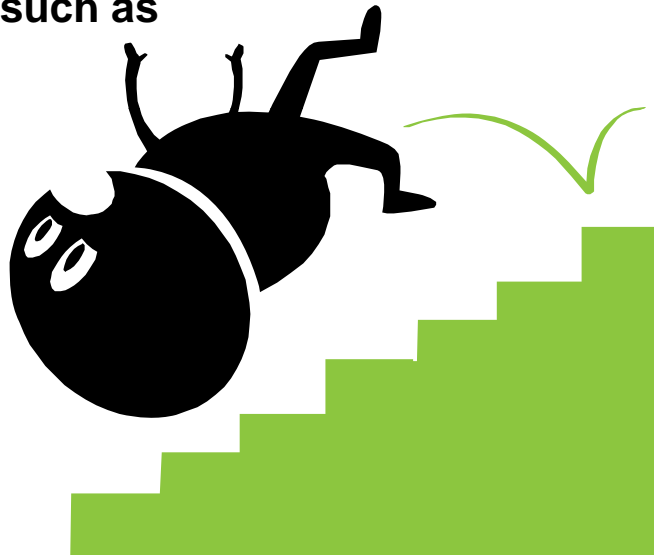
Negligent acts and/or omissions result in
bodily injury and/or property damage on the premises of a business,
when someone is injured as the result of using the product
manufactured or distributed by a business,
or when someone is injured in the general operation of a business.

Includes such concerns as:
Maintenance of the Premises
Defamation
Employment Issues
Slander

General Liability Insurance excludes coverage for losses related to war,
terrorism, or nuclear events.

Ways to Avoid General Liability Claims

- **Set a high standard for customer service and product quality control;**
- **Make sure all company records are complete and up-to-date;**
- **Be sure employees are properly trained;**
- **Pay attention to safety concerns such as**
 - hidden steps
 - loose, irregular surfaces
 - slick surfaces
 - wet spots
 - oil and grease
 - unsafe chairs
 - moving too fast
 - obstructed aisles
 - bad lighting
 - improper shoes
 - standards of care
- **Have a Safety Committee that routinely reviews and addresses potential problem areas**





Medical Liability



Malpractice

Improper professional actions or
the failure to exercise proper professional skills
by a professional advisor,
such as a physician, dentist, or healthcare entity.

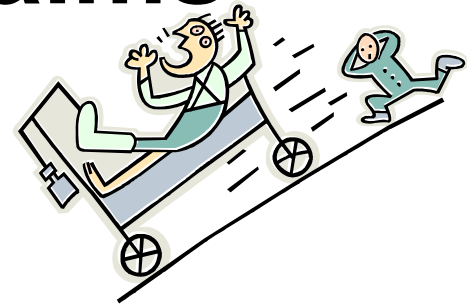
Also, professional misconduct,
improper discharge of professional duties, or
failure to meet the
standards of care of a professional,
resulting in harm to another.

Neglect

Failure to provide goods and services necessary to
avoid physical harm, mental anguish, or mental illness.

Ways to Avoid Medical Liability Claims

Risk Management Do's & Don'ts



- Do practice good patient care
- Don't try to practice legalese.
- Don't clam up when an accident occurs.
- Do see that the proper person discusses an event with the patient or family if possible.
- Don't put critical remarks in the patient's chart.
- Don't comment beyond the necessary in the chart. Only relevant patient information should be included.
- Do report any observed deviation from accepted patient care standards to the person in charge.
- Do indicate in the progress notes if the patient's condition has changed and that the physician has been notified.
- Don't change progress notes or other record entries by erasure or other means – use approved “error” technique.
- Don't label a progress note as a “late entry”. Enter the current date & time and refer to the specific information in the narrative data.
- Do notify the next physician in line if the first physician called in a patient emergency fails to respond.
- Do communicate openly with co-workers regarding patient care.
- Don't use the progress note entry just to cover yourself or to pass a problem along to someone else.
- Don't comment about patients in elevators, cafeterias, or other areas where non-direct care staff may be present.
- Don't answer personal questions about patients over the telephone without verifying who you're speaking to (and that you have authorization to discuss the patient with that person).
- Do be courteous and professional.
- Don't fail to give prescribed patient care.
- Don't fail to report adverse events.
- Do know how to monitor or operate all equipment necessary for patient care in your area.
- Do include full identification of equipment involved in incidents including serial numbers, manufacturer, etc.
- Don't refer to an incident report in the patient's medical record.

Remember: A patient is less likely to take adverse action against a staff member they like!

“Incident”

Any happening not consistent with the routine or desired operation of MCC, including patient care

Incidents include all significant and/or unusual or unexpected complications of treatment

An incident is an accident (or a situation which might result in an injury or damages) if not assessed, controlled, or corrected

Report any incident (including near misses) to Risk Management, regardless of whether there is a known injury or not

Incidents involving injury must be immediately called to Risk Management at 474-8625



The system is rendered totally ineffective when a claim is made or lawsuit filed and there has been no incident report filed

Risk Management Incidents Include (But are NOT Limited To):

- **Falls**
- **Injuries to patients or visitors**
- **Vehicle accidents**
- **Theft**
- **Fraud**
- **Inappropriate handling of prescriptions or medications**
- **Delayed diagnosis**
- **Wrong site surgery**
- **Poor clinical outcome**
- **Transfers to the ER or hospital**
- **Threatening or aggressive patient**

Incident Report



An early warning system intended to identify risk situations or adverse events in a timely manner

An incident report triggers prompt investigation from a claim management perspective
as well as
initiating corrective actions to prevent similar future events

The report should be an objective and factual written statement about the event and should be specific to the
time,
location,
all involved persons (including witnesses and titles as appropriate),
and
nature of the event with a description of any injuries

The report is not a medical record form and should not be referred to (or placed in) a medical record.

The original incident report is considered privileged and confidential and should not be copied for any reason

Details, Details, Details

Writing Tips:

Only use black or dark blue ink to complete the report.
Do not erase, use white out or black out on any part of the report.

Correct errors per Clinic policy.

Incident reports should contain the following information:

The person's name, locating information, date of birth, age and sex;

A clear and concise description of the incident, Including time, date, exact location;

Whether or not the person was seen by a physician; and if so, a brief statement of said physician's recommendations as to medical treatment, if known;

A listing of all persons then known to be involved directly in the incident, including witnesses, along with locating information for each;

The name, signature, extension, and position of the person completing the report, along with date and time that the report was completed



Incident Reports Should Be Prepared By:

The employee having knowledge of the facts; or

The employee who observed the incident; or

The employee who received the complaint; or

The supervisor (if the supervisor is present and is knowledgeable of the facts)

Keep Administrative Processes Separate from Medical Care:

Visitors or patients should not review or sign the incident report

References to the Incident Report or Risk Management should not be made to the patient nor documented in the medical record

Notifying Risk Management:

Phone Call (x8625): For all incidents involving patients or visitors where injury is suspected. Arrangements will be made for the person to be seen by a physician, Urgent Care, or the West Florida Hospital Emergency Department, as indicated.

Written Report: Submit within 1 working day of the event.
Do NOT make copies of the Incident Report for any reason.

Don't accept blame.

Communicate care and concern but not commitment.

Documenting Incident Reports: DETAIL Documentation Model

Document in as much detail as possible

Eliminate unnecessary commentary

Trace the steps that led up to the event including who, what, when, where, why, & how

Align the facts in chronological order

Include full names, dates, times, & all other pertinent facts required by the organization's incident report form

Log all copies with the appropriate person

Documenting Incident Reports: Common Errors

- Consciously or unconsciously directing the report through selection or omission of facts
- Guessing at what took place
- Discussing the report with unauthorized persons
- Using connotative words, i.e. victim, suspect, or accident
- White-outs or scratch-outs





PATIENT/VISITOR INCIDENT REPORT FORM

This is privileged communication to legal counsel.
This document is subject to confidentiality requirements and should be treated accordingly.

Submit Reports to Risk Management Within 1 Working Day of the Event (In An Envelope Via Interoffice Mail)

Call Risk Management at 474-8625 For Serious Injury

DO NOT COPY

PATIENT ID LABEL IF AVAILABLE

Main Participant:

Address:

Phone #:

DOB:

Age:

MCC#:

Patient / Visitor / Employee

Participant / Witness

Type of Injury:

(1st Aid UC ER No Injury)

EVENT	Date:	Time: a.m./p.m.	Location:
DETAILS	Reporting Employee:	Dept:	Ext:
DESCRIPTION (Describe What Happened, How, When, Where, By & To Whom. Use Quotes When Possible.)			
OF EVENT Please Print. Use Plain Paper If Additional Space is Needed and Attach to This Form.			
(MRT	Code 3-Code G	Security	N/A)
			(ASC Patient: Yes/No)

Environmental Conditions / Contributing Factors:

Names of All Patients, Visitors, & Employees Participants & Witnesses	Address (Work Location for Employees)	Phone Number(s) (Work Extension for Employees)	M F	Patients Only
(Pt Visitor Employee) (Participant Witness) Type of Injury: _____ 1 st Aid Urgent Care ER No Injury		Home: Work: Cell:	M F	MCC #: DOB: Age:
(Pt Visitor Employee) (Participant Witness) Type of Injury: _____ 1 st Aid Urgent Care ER No Injury		Home: Work: Cell:	M F	MCC #: DOB: Age:
(Pt Visitor Employee) (Participant Witness) Type of Injury: _____ 1 st Aid Urgent Care ER No Injury		Home: Work: Cell:	M F	MCC #: DOB: Age:

Risk Management	Printed Signature	Date	Time	Comments
Received by Risk Mgmt				
Logged In	Faxed	Scanned		Rev. 02/08

Got a Problem? Here's Help!!!

Computer Problems	8010
Telephone Problems	8477
Patient Transport	5051
Patient Parking Lot Shuttle Service	291-2646
Immediate Help After Hours/Weekends (Ask for Administrator on Call)	8001
Identification of a Particular Provider or Department	8001
Medical Equipment Maintenance Needs	2107
Urgent Maintenance or Housekeeping Need (Ask Operator to page maintenance or housekeeping personnel)	8001

Non-Urgent Maintenance Repair:

Each department has one person designated to submit electronic maintenance work orders:

Departmental Contact Person: _____

Non-Urgent Housekeeping Need:

Contact your department supervisor.

Manned Response Needed:

All Emergency Codes	3333
Risk Management	8625
Employee Services Specialist	8023
Sr VP, Human Resources	8544










MCC Emergency Line

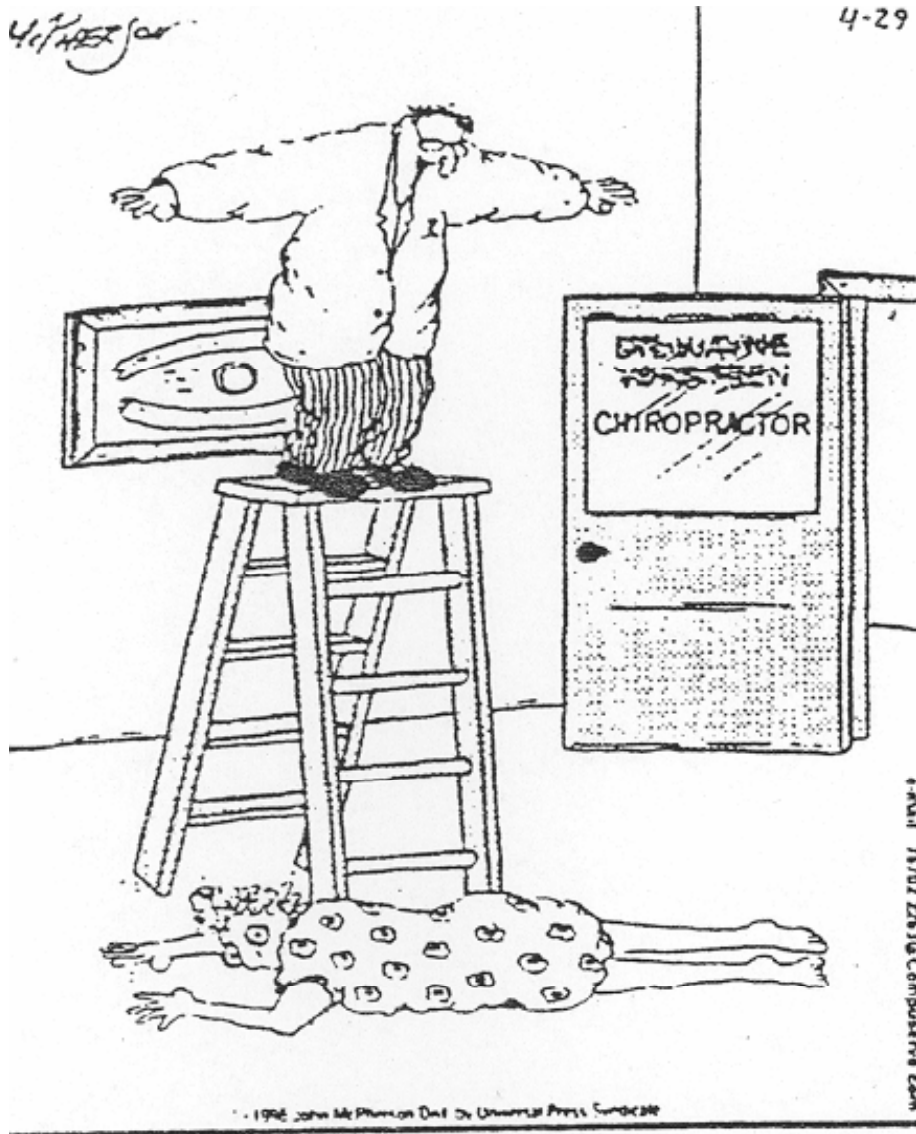
850-474-8788

This information line is activated to inform employees of work status during hurricanes and other emergencies or disasters.

Emergency Code Designations

For All Codes Unless Otherwise Specified: Call x3333

MRT (No Color Designation)	Manned Response Team: Injured/Medically Compromised <u>or</u> Missing Person (Responsive Patient)	
Blue (Also Known as "Code 3") On-Campus: Call x3333 to be Connected Off-Campus: Call 911	Cardiac / Respiratory Arrest (Unresponsive Patient)	
Red On-Campus: Call x3333 to be Connected Off-Campus: Call 911	Fire	
Gray/Silver On-Campus: Call x3333 to be Connected Off-Campus: Call 911	Security / Violence	
Black	Bomb / Explosion Threat	
Green	Mass Casualty/Disaster	
Orange	Toxic Atmosphere / <u>Hazmat</u> or <u>Bioterrorism</u>	
Pink (Hospital Alert)	Baby Abduction	
Brown 474-8788 Information Line Regarding Job Responsibilities	Severe Weather	



Questions?

Contact

Debbie Ray Kings, RN
Risk Manager

474-8625

June 2013



EMERGENCY PROCEDURE QUICK RESPONSE CHART

QUICK RESPONSE CHART

Got a Problem? Here's Help!!!.....3

Emergency Code Designations:

- Code Chart4
- MRT (No Color Designation)5-9
- Cardiopulmonary Arrest / Code 3 (Blue)10-11
- Fire (Red)12-13
- Security / Violence (Gray/Silver)14-15
- Bomb / Explosion Threat (Black)16-18
- Mass Casualty / Disaster (Green)19
- Toxic Atmosphere/Hazmat or Bioterrorism (Orange)20
- Baby Abduction (Pink)21
- Severe Weather (Brown)22

Non-Code Situations:

- Acute Reactions.....23/24
- Infection Control: Biomedical/Biohazardous Waste.....25
- Infection Control: Exposure Precautions.....26
- Infection Control: Blood/Body Fluid Spills.....27/28
- Chemical Exposures/Spills (MSDS Sheets and Chemical Spills).....29
- Employee Injuries/Exposure to Blood/Body Fluids.....30/31
- Incident Reporting.....32

Got a Problem? Here's Help!!!

Computer Problems	8010
Telephone Problems	8477
Patient Transport	5051
Patient Parking Lot Shuttle Service.....	291-2646
Immediate Help After Hours/Weekends	8001
(Ask for Administrator on Call)	
Identification of a Particular Provider or Department	8001
Medical Equipment Maintenance Needs	2107
Urgent Maintenance or Housekeeping Need	8001
(Ask Operator to page maintenance or housekeeping personnel)	

Non-Urgent Maintenance Repair:

Each department has one person designated to submit electronic maintenance work orders:

Departmental Contact Person: _____

Non-Urgent Housekeeping Need:

Contact your department supervisor.

Manned Response Needed:










All Emergency Codes.....	3333
Risk Management	8625
Employee Services Specialist	8023
Sr VP, Human Resources	8544

MCC Emergency Line..... 850-474-8788

This information line is activated to inform employees of work status during hurricanes and other emergencies or disasters.

Emergency Code Designations

For All Codes Unless Otherwise Specified: Call x3333

MRT (No Color Designation)	Manned Response Team: Injured/Medically Compromised or Missing Person (Responsive Patient)		Pg 5-9
Blue (Also Known as "Code 3") On-Campus: Call x3333 to be Connected Off-Campus: Call 911	Cardiac / Respiratory Arrest (Unresponsive Patient)		Pg 10-11
Red On-Campus: Call x3333 to be Connected Off-Campus: Call 911	Fire		Pg 12-13
Gray/Silver On-Campus: Call x3333 to be Connected Off-Campus: Call 911	Security / Violence		Pg 14-15
Black	Bomb / Explosion Threat		Pg 16-18
Green	Mass Casualty/Disaster		Pg 19
Orange	Toxic Atmosphere / <u>Hazmat</u> or <u>Bioterrorism</u>		Pg 20
Pink (Hospital Alert)	Baby Abduction		Pg 21
Brown 474-8788 Information Line Regarding Job Responsibilities	Severe Weather		Pg 22

MANNED RESPONSE TEAM

There are 2 types of MRT calls utilized at the Medical Center Clinic:
Medical Response and Missing Person

Medical Manned Response

Patient is responsive, is in the building, and needs emergency transport

Tower, ASC Building, & Grounds:

1. ACTIVATE MRT CODE RESPONSE:

- Dial x3333, state “MEDICAL MRT CODE” and give location of incident. Be specific!
- Identify special equipment needs, i.e. stretcher, AED (defibrillator), or Acute Reaction Emergency Kit.
- MRT members coordinate a response to the need for rapid transport to the Emergency Department or Urgent Care.

2. UPON ACTIVATION OF THE CODE MRT the following should take place:

- Manned Response Team will respond to that location with a stretcher or wheelchair, and medical bag. Other items will be provided as requested.
- Security will lock off the elevator as needed and hold in standby.
- The Team Captain will determine the appropriate referral location - Emergency Department or Urgent Care. Patients being transported via stretcher should be transported to the Emergency Department.
- The Team Captain will accompany the patient to the referral location.
- The Ambulatory Surgical Center manages their own emergency situations. All other departments within the ASC building may utilize the MRT service.

MANNED RESPONSE TEAM (continued)

Off-Site Locations: Cancer Institute, Allergy, & MedPro

All off-site locations must call 911 for emergency transport needs.

Refer to the Manned Response Team (MRT) policy located in the Patient Care section of the MCC Policy and Procedure Manual for more information.

MANNED RESPONSE TEAM (continued)

Missing Person Emergency

A patient or visitor is reported as missing from one of the MCC main campus locations, including the Cancer Center and MedPro.

This process is only available during normal business hours.

Call the Doctor's Call Center at x3333 and request that an "MRT – Missing Person" call be announced. Be sure to identify the specific department from where the call is originating.

The Doctor's Call Center will send out the announcement stating "Missing Person MRT" and the location of the call.

All available MRT staff will report promptly to the specified department.

A "Missing Person Questionnaire" should be completed as thoroughly as possible to facilitate sharing information with each of the search team members.

- Copies may be distributed to the team members as needed but must be promptly placed in the confidential trash at the conclusion of the event.
- Exception: Questionnaires may be returned to Risk Management for incident reporting purposes and disposal as needed.

Only the portions of the form that actually apply to the situation needs to be complete. Do not delay searching for missing person due to omitted information on the form.

Assignments will be made to promote a comprehensive search of the buildings and grounds.

Community contacts (including the Sherriff's office) may be made as requested by the family member, friend, or caregiver.

The staff member identifying the missing person situation is responsible for initiating the Incident Report and forwarding it to Risk Management.

Refer to the Manned Response Team (MRT) policy located in the Patient Care section of the MCC Policy and Procedure Manual for more information.

Missing Person MRT Questionnaire

Missing Person	Name	Nickname	Age
Phone #s of Missing Person	Cell Phone #	Home #	
Last Seen	Time:	a.m. / p.m.	Place:
Appearance	Ht / Wt	Height	Weight
	Hair	Brown Black Blond Red Gray Salt & Pepper Bald Thinning Long Short Shoulder-Length _____	
	Eyes	Black Blue Brown Gray Green Hazel Glasses / No Glasses	
	Prosthesis	Hearing Aid Cane Walker Wheelchair Prosthesis _____	
	Other	Tattoo(s) Piercing(s) Scars Amputation Distinguishing Marks or Characteristics: _____	
	Clothes	Shirt _____ Long/Short Sleeve Button-Up/Pullover T-Shirt Pants / Shorts _____ Jeans Khakis Sweats Dress Jacket / Sweater _____ Shoes _____ Tennis Shoes/Sandals/Lace Ups/Slip Ons Hat _____ Ball Cap	
	Picture	Available (See Attached) Not Available	
Possible Actions of the Missing Person At This Time			
Vehicle (If Applicable)	Description	Color	
	Year	Make	Model
	Tag (State, County, & #)		
Other Physicians & Services Utilized at MCC / WFH			
Other Pertinent Notes			
Contact Person (Family, Friend, or Caretaker)	Contact	Name	
		Home #	Cell #

Person	Activity
Risk Management (or Designee)	Coordinate All Activities Serve as Main Contact Person (Risk Manager's Cell # 777-7620) If Not Available, Designate Another Contact: Name _____ Phone #: _____
Departmental Representative (If Possible)	Make Phone Calls As Indicated _____ Sherriff's Department (436-9350) to File a Report _____ Missing Person's Cell or Home Phone _____ Family, Friends, or Others as Requested _____ Local ERs If Indicated WFH (494-6565) SHH (416-7000) Baptist (434-4811) Baptist GB (934-2020) Santa Rosa (626-5150) _____ WFH Security (494-4000) _____ Other
IT Staff	Connect the Friend/Family Member with IT staff to review videos (969-2599)
Guest Services & Facilities	Use Shuttles to Check Parking Lots _____ Lot A . . . _____ WFH Parking (East Side / Davis Hwy & Johnson) _____ Lot B . . . _____ Check Woods & Maintenance Area _____ Lot C . . . _____ WFH Parking (West Side / Univ Pkwy & Johnson)
Risk Management & All Other Available Staff	Begin a Building Search (Including Restrooms) _____ ASC Bldg (All 3 Floors; Identify Specific Service Providers) _____ Towers (Designate Floors; Identify Specific Service Providers) _____ WFH (Start With 1 st Floor & Cafeteria Unless Otherwise Specified)
Other Available Staff	Initiate Other Activities as Indicated:
	Additional Notes:

CODE BLUE (aka “Code 3”)

Person Is Unresponsive in any MCC Building or Property And Needs Emergency Transport

1. ACTIVATE THE CODE RESPONSE:

Dial 3333, state “CODE 3” and give location of incident.

- Be specific!
- Stay on the line to answer any further questions from EMS

2. UPON ACTIVATION OF THE “CODE 3” the following should take place:

- Doctor’s Call Center activates EMS first by calling 911 & then alerts the Manned Response Team.
- Manned Response Team will respond to that location with a stretcher, and a medical bag with an Automated External Defibrillator.

3. FIRST RESPONDER ON SCENE SHOULD:

- Briefly assess for responsiveness while simultaneously assessing for normal breathing & the presence of an obvious pulse (<10 second total).

- Initiate the C-A-B sequence: Circulation, Airway, Breathing,

Circulation If pulse is absent, give 30 compressions immediately

Airway After the first cycle of compressions, open the airway with the head-tilt, chin-lift

Breathing Provide 2 rescue ventilations.

Use Pocket Mask for resuscitation.

NO MOUTH TO MOUTH RESUSCITATION

Continue this 30:2 ratio until an AED or EMS arrives.

CODE BLUE (continued)

- CPR: **Adult and Older Child (Puberty and Older)**
1-and 2-rescuer CPR: 30 Compressions to 2 Ventilations

Child (1 y/o to Puberty) Or Infant (Less Than 1 y/o)
1-rescuer CPR: 30 Compressions to 2 Ventilations
2-rescuer CPR: 15 Compressions to 2 Ventilations
- The AED will automatically instruct on proper use of device.

4. WHEN EMS ARRIVES:

- Notify EMS what procedures you have performed.
- If possible notify patient's primary physician.
- Assist EMS as necessary.

Refer to the Manned Response Team (MRT) policy located in the Patient Care section of the MCC Policy and Procedure Manual for more information.

CODE RED

Fire Or Smoke In Your Area

1. Do Not Shout “Fire”; state “Code Red”

2. R - A - C - E:

RESCUE people from the vicinity. Close all doors.

ACTIVATE the alarm.

Pull the fire alarm box located _____.

Pick up the telephone and dial x3333 (Off-Campus Call 911)

Report type and exact location of the fire/smoke. Be specific!

CONTAIN the fire.

Close all doors.

Check to see that fire exits are clear.

EXTINGUISH if you can do so safely.

Go to the area with a fire extinguisher and attempt to put the fire out.

Spray the fire with the extinguisher, sweeping it side-to-side at the base of the fire.

Do Not Use More Than Two Extinguishers . . .
Get Out If Not Extinguished at This Point!

Closest fire extinguisher is located:_____.

3. EVACUATE:

Evacuation Instructions On The Following Page

EVACUATION INSTRUCTIONS

11 STORY TOWER		
<u>Location</u>	<u>Exit</u>	<u>Meeting Area</u>
Floors 8 to 11	Use both stairwells to 7 th floor. Exit to Hospital via the ancillary hallway. Use Hospital elevator to 1 st floor.	Grassy area by flagpole, in front of ancillary building.
Floors 2 to 7	Exit Clinic via ancillary building to elevator to 1 st floor.	Parking lot in front of flagpole, in front of ancillary building.
1st Floor	Exit via hallway toward switch-board or exit by glass elevator, if closer.	Doctor's parking lot or grassy area by flagpole in front of ancillary building.
EYE INSTITUTE/ AMBULATORY SURGICAL CENTER		
1st Floor	Exit via front entrance.	Parking lot in front of pond.
Lower Level and 2nd floor	Use both stairways to ground level.	Doctor's parking lot or nearest parking lot.
OFF-SITE LOCATIONS		
All Areas	Leave building by nearest exit.	Nearest parking lot.
MEDPRO SOLUTIONS		
All Areas	Leave building by nearest exit.	Nearest parking lot.

Do Not Leave the Meeting Area Until Authorized to do so by a Supervisor

**Refer to the Fire Management policy located in the
Emergency Action Plans of the MCC Policy and Procedure Manual for more information.**

CODE GRAY/SILVER

NEED MANPOWER: Assistance needed for Security or Violence Issue

1. ACTIVATE THE CODE RESPONSE:

- Dial x3333 and state the need for Manpower.
- Give location of incident. Be specific!
- Give number and gender of aggressors involved.
- State if any types of weapons are present.

2. UPON ACTIVATION OF THE CODE “GRAY/SILVER”:

- If indicated (i.e. presence of weapons), Doctor’s Call Center will contact law enforcement
- Doctor’s Call Center will page the Facilities/Security staff
- Doctor’s Call Center will provide a courtesy notification to West Florida Hospital, advising them of situation and location.

3. EVACUATE IF ORDERED TO DO SO: See Page 13/Evacuation Procedures

4. GUN THREATS

Quickly determine the most reasonable way to protect your own life.

Responses from most preferable to least preferable (Run. Hide. Fight.):

Get Out (Run/Evacuate)

- Evacuate regardless of whether others agree to follow.
- Leave belongings behind.
- Help others to escape if possible.
- Prevent individuals from entering an area where an active shooter may be.
- Do not attempt to move wounded people.

CODE GRAY/SILVER (continued)

Hide Out (Hide/Move to a Safe Place)

- If you are in an office, stay there and secure the door.
- If you are in a hallway or open area, get into a room and secure the door.
- Try to find a place that will provide protection (i.e. an office with a closed & locked door) and will not trap you or restrict your options for movement.
- Use heavy furniture to blockade the door.
- Silence any cell phones or pagers that may give away your location. Also turn off any source of noise (i.e. radios or televisions).
- Hide behind large items.
- Remain quiet.

Take Out (Fight/Take measures to incapacitate the active shooter)

- Physical intervention is always utilized as a last resort (i.e. when your life is in imminent danger).
- Attempt to disrupt &/or incapacitate the active shooter by acting as aggressively as possible against the person, throwing items, improvising weapons, & yelling.
- Be committed to your actions.

At all times:

- Remain calm.
- If you cannot speak, dial 911 and leave the line open to allow the dispatcher to listen.
- Do not leave the grounds until law enforcement authorities have authorized you to do so.

Refer to the Emergency Action Plan and Gun Threat policies located in the Emergency Action Plans of the MCC Policy and Procedure Manual for more information.

CODE BLACK

BOMB THREAT

1. RECEIPT OF WARNING:

- If letter or note is received, handle as little as possible.
- If telephone call – Refer to *Bomb Threat Script*.

Get as much information about the caller as possible.

Keep the caller on the telephone as long as possible.

Delay as Much as Possible – ask the caller to repeat statements.

2. ACTIVITE THE CODE RESPONSE:

- Dial x3333 and advise of threat. If on the telephone with a person issuing a bomb threat, try to get a co-worker's attention so that they can dial x3333.
- Doctor's Call Center will contact the Escambia County Sheriff's Department first and then page the Facilities/Security staff.
- Facilities/Security staff will maintain communications with law enforcement as the situation develops.
- If a bomb is found a Code Black will be called.

3. PROTOCOLS:

- Remain calm. Do not discuss the threat in public.
- Do not touch suspicious packages, letter or objects.
- Do not start or repeat rumors.

CODE BLACK (continued)

4. SEARCH PROCEDURES:

- Public areas such as lobbies, storerooms, restrooms, etc. should be searched. **Do not touch** the bomb or any suspicious-looking packages.
- Notify the police/fire officials in the building if any suspicious item is found.
- Evacuate patients and personnel in the immediate area as directed by Executive Director or his designee.

5. IF CODE BLACK IS CALLED

- Close all fire and smoke doors.
- Leave all lights on.
- Turn off all gases (O₂, nitrous oxide, etc.).

Refer to the Bomb & Explosion Threats policy located in the Emergency Action Plans of the MCC Policy and Procedure Manual for more information.

BOMB THREAT SCRIPT

Remember: Remain Calm



Time of Call a.m./p.m.	Date of Call / /	#Call received at () -	Person receiving call
---------------------------	---------------------	----------------------------	-----------------------

Exact Words of Caller: _____

Voice Type (Check all that apply)

<input type="checkbox"/> Male	<input type="checkbox"/> Excited	<input type="checkbox"/> Calm	<input type="checkbox"/> Stutter	<input type="checkbox"/> Normal
<input type="checkbox"/> Female	<input type="checkbox"/> Accent	<input type="checkbox"/> Giggling	<input type="checkbox"/> Stressed	<input type="checkbox"/> Rapid
<input type="checkbox"/> Child	<input type="checkbox"/> Disguised	<input type="checkbox"/> Slow	<input type="checkbox"/> Nasal	<input type="checkbox"/> Lisp
<input type="checkbox"/> Angry	<input type="checkbox"/> Broken Speech	<input type="checkbox"/> Slurred	<input type="checkbox"/> Deep	

Approx. age of caller: _____ If voice is familiar, who does it sound like? _____

Background Noise (Check if heard):

<input type="checkbox"/> Music	<input type="checkbox"/> Water	<input type="checkbox"/> Typing	<input type="checkbox"/> Cars
<input type="checkbox"/> Children/Babies	<input type="checkbox"/> Birds	<input type="checkbox"/> PA System	<input type="checkbox"/> Trucks
<input type="checkbox"/> People Talking	<input type="checkbox"/> Machine Noise	<input type="checkbox"/> Airplanes	<input type="checkbox"/> Other _____

Describe all background noises. Be Specific: _____

Ask Caller:

When is the bomb going to explode? _____

Where is the bomb? _____

What does it look like? _____

What kind of bomb is it? _____

What makes it explode? _____

How can we stop it from going off? _____

Did you place the bomb? ☐ Yes ☐ No When? _____

Why? _____

Who do you represent? _____

Will you call again? ☐ Yes ☐ No

Where are you calling from? _____

What is your address? _____

What is your name? _____

Call reported to: ☐ Administration ☐ Physician ☐ Police ☐ Fire Department ☐ FBI

CODE GREEN

Mass Casualty/Disaster

- Upon notification of a mass casualty or disaster in the immediate area, the Medical Center Clinic Command Center will be activated.

As needed, alert providers & administrative/management staff to the event.

- Directions to staff will be given in accordance with guidelines from law enforcement and the local Health Department.

Activate staffing for Urgent Care, Facilities, & other departments as needed.

- Follow Evacuation Procedures (page 12) **IF** evacuation is ordered.

Refer to the Emergency Action Plan policy located in the Emergency Action Plans of the MCC Policy and Procedure Manual for more information.

CODE ORANGE

Toxic External Atmosphere/Hazmat or Bioterrorism

Toxic External Atmosphere – atmosphere contaminated by a chemical cloud, smoke, or other pollutants to the extent that it becomes a significant threat to life or health. A chemical spill in the immediate outside area of Medical Center Clinic would indicate a toxic atmosphere by this definition.

- The objective is to stay indoors until the air has cleared or evacuation is ordered. All doors to the outside are secured and are to be kept closed.
- All persons within MCC will be directed to each department's designated receiving area.
- An announcement will be made that no one leave the building or open doors to the outside.
- Follow Evacuation Procedures (page 12) IF evacuation is ordered.

Refer to the Emergency Action Plan policy located in the Emergency Action Plans of the MCC Policy and Procedure Manual for more information.

CODE PINK

West Florida Hospital Alert

- “Code Pink” is a West Florida Hospital alert indicating that a baby has been abducted from the nursery.
- Doctor’s Call Center will announce “Code Pink” three times with the location, e.g. “Code Pink, 3rd floor, NE stairwell”.
- Facilities/Security staff and transporters will be dispatched to monitor MCC exits.
- Anyone suspected of being the perpetrator will be detained until MCC Facilities/Security and/or West Florida Hospital Security or the Escambia County Sheriff’s Office arrives.

Refer to the Emergency Action Plan policy located in the Emergency Action Plans of the MCC Policy and Procedure Manual for more information.

CODE BROWN

Inclement Weather (Hurricane, Tornado, etc.)

- Unplug all unnecessary equipment and appliances.
- Store all equipment in safe areas away from window.
- Cover all equipment in rooms near outside windows with plastic (supplied by maintenance or housekeeping).
- Close, but do not lock, all doors in rooms with outside windows.
- Leave all lights on.
- Assure that all equipment and supplies are removed from hallways.
- In imminent situations, insure that all people are gathered:
 - In the department designated receiving area.
 - Away from windows and external doors.
 - If possible, at the lowest level available.
- Assist where needed or as may become necessary as directed by your supervisor.

MCC EMERGENCY LINE 850-474-8788

Refer to the Emergency Action Plan & Disaster Preparedness policies located in the Emergency Action Plans of the MCC Policy and Procedure Manual for more information.

ACUTE REACTIONS

Medical Center Clinic clinical staff can access the acute reaction supplies if a patient appears to be having an adverse response to medications.

Emergency Kit Locations:

In the Tower	In a locked cabinet on each odd numbered floor (1, 3, 5, 7, 9) outside of the doctor's elevator
In the ASC Building	In a locked cabinet across from the freight elevator located on the 1 st floor
Off-Campus Medical Buildings	The department will identify (& communicate to staff) a specific storage area for the supplies

The Tower/ASC Building cabinet keys will be retained by Risk Management, the Purchasing Director, and (1) available at Doctor's Call Center. If necessary, the door can be popped open to access the supplies.

An incident report should be completed any time the cabinet is entered for a medical emergency.

The following drugs, supplies, and equipment are stocked by Risk Management and are available in each cabinet:

Medications:

Claritin or Zyrtec 10 mg (1)
Benadryl (Diphenhydramine) Elixir (4)
Decadron (Dexamethasone) or Solumedrol 4mg vial (2)
Epinephrine Injection (1:1000: 1mg/ml) ampule (2)

Medication Supplies:

TB 1cc syringe/safety needle (3)
6cc safety syringes (2)
Needles 22g 1½ inch (2)
Alcohol wipes
Positive pressure ventilation device (ambu bag)

Other Supplies:

Nasal cannula
Oxygen tank

ACUTE REACTIONS (continued)

The written Acute Reaction Protocol should be followed explicitly in utilizing these items. A current copy of the protocol is kept with the kit in the cabinet.

The protocol includes the following specifications:

Adult (Mild Reaction and Moderate to Severe Reaction)

Pediatric (Mild Reaction and Moderate to Severe Reaction)

Refer to the Acute Reaction policy located in the Patient Care section of the MCC Policy and Procedure Manual for more information.

BIOMEDICAL OR BIOHAZARDOUS WASTE INFECTION CONTROL

- The Exposure Control Plan is located in the Department's OSHA Manual, which is located_____.
- Personal Protection Equipment for this department is located
_____.

Personal Protection items include, but are not limited to:

Gloves
Masks

Eye Protection
Red Bags

Gowns

- Additional red bags for this location are located
_____.
- Red bagged waste is placed in the following location for collection by housekeeping
_____.
- Employee exposures (See Employee Exposure to Blood and Body Fluids Section and Employee Work Related Injury/Illness Section).
- Sharps (needles, scalpels, etc.) must be separated from other waste and disposed of in designated sharps containers.

Sharps containers must be changed out when 2/3 full (and not allowed to overfill), they should be taped securely closed (to prevent spillage or protrusion of contents during handling, storage, transport or shipping) and labeled with name of department and address.

**FOR YOUR PROTECTION, DO NOT EAT OR DRINK
IN BIOHAZARDOUS WORK AREAS!**

PRECAUTIONS AGAINST EXPOSURE TO BLOOD/BODY FLUIDS

- Exposure Precautions should be used with every patient.
- ALL healthcare workers must use the appropriate Personal Protection Equipment as barrier precautions when contact with blood/body fluids is anticipated.
- Hand-washing must be done before and after contact with patients, each procedure in patient care, and handling of contaminated materials.
- Techniques for Hand Hygiene with soap and water:
When hands are visibly dirty, they should be washed with soap and water when available. Use friction; remember to wash hands for a full 20 seconds.
- Techniques for Hand Hygiene with Alcohol-Based Products:
If soap and water are not readily available, use an alcohol-based product to clean your hands. When using an alcohol-based hand rub, apply product to palm of one hand and rub hands together, covering all surfaces of hands and fingers, until hands are dry. Note that the volume needed to reduce the number of bacteria on hands varies by product. Alcohol-based hand rubs significantly reduce the number of germs on skin and are fast acting.
- Refer to the Exposure Precautions section of the MCC Policy and Procedure Manual located in the Resources section of the MCC Employee Intranet for more information.

BLOOD/BODY FLUID SPILLS RESPONSE

Hard Surface Spill

DURING NORMAL BUSINESS HOURS:

Notify Housekeeping by dialing the Doctor's Call Center at x8001.

Ask an operator to page a member of Housekeeping.

Be prepared to advise Housekeeping on the type of spill.

AFTER HOURS/WEEKENDS:

- Secure the area.
- Apply two pairs of gloves.
- Saturate area with an approved cleaner from housekeeping (HDQ-10) or a 1:10 solution of household bleach and water. Bleach and water solution must be prepared fresh daily.
- Place paper towels over the area and remove spill.
- Clean area well with the approved cleaner from housekeeping (HDQ-10) or 1:10 solution of household bleach and water.
- Wipe area dry with paper towels and place all used paper towels in a red plastic biohazardous waste bag.
- When the spill is removed and area has been cleaned, reapply disinfectant to clean area and allow to dry.
- Remove ONE pair of gloves and place them in the red plastic biohazardous bag.
- Securely tie the red plastic biohazardous bag closed.
- Place the red plastic biohazardous bag in the appropriate location for collection by Housekeeping (see Biomedical or Biohazardous Waste Infection Control, page 20).
- Enter the closest restroom, remove the remaining pair of gloves and place them in a regular trash receptacle.
- Wash hands thoroughly.

**PLEASE NOTE IF BLEACH AND WATER 1:10 SOLUTION IS USED:
BLEACH IS CORROSIVE TO METAL
AND
CAN BE IRRITATING TO SKIN AND MUCOUS MEMBRANES**

BLOOD/BODY FLUID SPILLS RESPONSE (continued)

Carpet Or Upholstery Spill

During Normal Business Hours:

Notify Housekeeping by dialing the Doctor's Call Center at ext 8001. Ask an operator to page a member of Housekeeping. Be prepared to advise Housekeeping on the type of spill.

After Hours/Weekends:

- Secure the area, or remove the item from the area in a red plastic biohazardous bag AFTER putting on two pairs of gloves.
- Put on two pairs of gloves.
- If scrubbing may be required to remove spill, apply a gown, splash goggles, and a mask to cover mucous membranes in case of spattering.
- Saturate area with PR Spot Remover (available from Housekeeping).
- Place paper towels or absorbent cloths over the area and remove the spill and spot remover.
- Clean the area well with PR Spot Remover.
- Blot the area dry with paper towels and/or absorbent cloths, and place all used paper towels and cloths in a red plastic biohazardous bag.
- When the spill is removed and area has been cleaned, reapply disinfectant to clean area and allow to dry.
- Remove ONE pair of gloves and place them in the red plastic biohazardous bag.
- Securely tie the red plastic biohazardous bag closed.
- Place the red plastic biohazardous bag in the appropriate location for collection by Housekeeping (see Biomedical or BioHazardous Waste Infection Control, page 20).
- Enter the closest restroom, remove the remaining pair of gloves and place them in a regular trash receptacle.
- Wash hands thoroughly.

CHEMICAL EXPOSURE

MSDS and Chemical Spills

MSDS (Material Safety Data Sheets)

- As an employee, you have the right to know what hazards you face on the job and how to protect yourself against them.
 - The MSDS for this department are located
-
- The MSDS give details on physical danger, safety procedures and spill clean-up of chemicals in your department.
 - When you are working with chemicals, read the container label and follow any instructions and warnings.

CHEMICAL SPILLS

Mercury, Cidex, etc.

- Secure the area.
- Refer to MSDS.
- During Normal Business Hours: Notify Housekeeping by dialing the Doctor's Call Center at ext 8001. Ask an operator to page a member of Housekeeping. Be prepared to advise Housekeeping on the type of spill.
- After Hours/Weekends: Refer to MSDS for emergency procedures. Use gloves and any other Personal Protection Equipment recommended on MSDS, and avoid direct contact.

EMPLOYEE EXPOSURE TO BLOOD/BODY FLUIDS

Needlestick Or Skin And Mucous Membrane Exposure

During The Hours Human Resources Is Open:

1. Wash hands or any exposed skin with soap and hot water.
2. Flush mucous membranes with water.
3. If it is a NEEDLESTICK encourage the wound to bleed freely and clean wound well with soap and water.
4. Immediately notify your supervisor, then notify the Employee Services Specialist at 474-8023. If you cannot reach her via phone, contact another member of the HR Department at ext 5308. TIME IS OF THE ESSENCE.
5. It is important you receive treatment immediately following an exposure, and that proper testing of the source person can be completed before the source person leaves MCC.
6. Fill out an Employee Incident Report Form, which is located on the Employee Intranet in the Forms section.
7. Follow up with the Employee Services Specialist within 72 hours for follow up on the HCV, HIV, and HBV test results.

During The Hours Human Resources Is Closed:

Follow the steps above, under “During The Hours Human Resources Is Open” and report to the Emergency Room at West Florida Hospital or the nearest available Emergency Room.

TIME IS OF THE ESSENCE.

Immediately make ER staff aware that:

- You are an employee of MCC
- It is a work related incident
- It is an exposure to blood/body fluids

EMPLOYEE WORK RELATED INJURY/ILLNESS

During The Hours Human Resources Is Open:

1. Immediately notify your Supervisor.
2. Fill out an "Employee Incident Report Form". Incident Report Forms are located on the Employee Intranet in the Forms section.
3. Report to the Employee Services Specialist if evaluation and/or treatment are medically indicated. Take the completed Employee Incident Report with you.
4. If evaluation and/or treatment are not medically indicated, forward the completed Employee Incident Report Form to the Employee Services Specialist in a sealed envelope marked confidential.

During The Hours Human Resources Is Closed:

1. Immediately notify your Supervisor.
2. If medical evaluation and/or treatment is medically indicated, report to the Urgent Care Department (Urgent Care is open Monday through Friday from 8:00am – 6:00pm; Saturday, Sunday and Holidays from 9:00am – 4:00pm), the Emergency Room at West Florida Hospital, or the nearest available Emergency Room. Make them aware you are an employee of MCC and this is a work related injury/illness.
3. Fill out an "Employee Incident Report Form". Incident Report Forms are located on the Employee Intranet in the Forms section.
4. Forward the completed Employee Incident Report Form to the Employee Services Specialist in a sealed envelope marked confidential.
5. Notify the Employee Services Specialist about the incident by leaving a voice message at 474-8023. You will be contacted as soon as possible on the next regular business day.

Refer to MCC Employee Handbook, Employee Responsibilities Section, for further information about Employee Work Related Injury/Illness. The MCC Employee Handbook is located on the Employee Intranet in the Resources section.

INCIDENT REPORTING

- An incident is defined as any event that is not consistent with the routine operation of MCC, the routine care of a patient, or the expected result of the care administered to a patient. This includes incidents with or without injury, involving patients, visitors, employees, and occurrences that could evidence employee/physician negligence/incompetence.
 - “Incident” shall include all significant and/or unusual or unexpected complications of treatment.
 - “Incident Report” means a factual written statement about a particular incident detailing particulars as to time, locations, all persons directly involved including functional titles, and the nature of event including description of injuries. The report should contain a listing of witnesses to the event.
- If an incident occurs, immediately complete an MCC Incident Report Form.
- Be sure to complete the correct MCC Incident Report Form.
 - **Patient/Visitor Incident** – Complete the MCC Incident Report Form for Risk Management. This form is located on the Employee Intranet in the Forms Section, and in the Resources Section in the Policies and Procedures Manual.

CONFIDENTIALITY: The MCC Incident Report represents a significant component of the confidential communication between healthcare personnel and their legal counsel, risk manager, or insurer. **DO NOT COPY THE REPORT.**

The report should be completed immediately by the individual most closely associated with the event and sent to the Risk Management Department upon completion of the report in a sealed envelope marked confidential. (The injured party cannot complete the form).

See the MCC Policy and Procedures Manual (located on the Employee Intranet) or Ambulatory Surgery Center Manual for further information.

- **Employee Incident**, including work related injury or illness – Complete the MCC Employee Incident Report Form for Human Resources. This form is located on the Employee Intranet in the Forms section. The report should be completed immediately & sent to the HR Employee Services Specialist.

Refer to the Incident Reporting policy located in the Risk Management section of the MCC Policy and Procedure Manual for more information.