



**NEW EMPLOYEE
COMPLIANCE AND PRIVACY
MANUAL**

TABLE OF CONTENTS

MESSAGE FROM THE SENIOR MANAGEMENT OF THE HEALTH SYSTEM

INTRODUCTION	3
SECTION I VCU HEALTH SYSTEM COMPLIANCE PROGRAM POLICY.....	4
Philosophy	4
Code of Ethics	4
Standards of Professional conduct	5
Compliance Standards	6
• Patient Care	6
• Work Place Responsibilities	6
• Business Information and Records	6
• Conflicts of Interest	7
• Competitive Behavior	7
• Coding and Billing of Patient Services and Cost Reporting.....	7
• Cost Reporting to Government and Other Third Party Payers ..	8
• Contact with External Entities	8
• Compliance	8
SECTION II COMPLIANCE PROGRAM.....	9
Purpose of the Compliance Plan	9
Legal and Ethical Obligations	10
False Claims Act	11
Penalties for Violation	12
Training.....	13
Chief Compliance and Privacy Officer	14
Reporting Concerns	14
Where to Find Help	14
SECTION III HIPAA AND PRIVACY	15
HIPAA - It's the Law	15
Protected Health Information	15
The Importance of PHI	16
Treatment, Payment and Health Care Operations (TPO)	16
Minimum Necessary Information	16
Reasonable Safeguards for PHI	16
Notice of Privacy Practices	17
Written Authorization for Non-TPO Uses and Disclosures	17
Patient Rights Under HIPAA	18
Patients Rights – Exceptions under HIPAA.....	18
De-Identified and Limited Data Sets	18
HIPAA Privacy Rule and State Privacy	19
SECTION IV HIPAA AND SECURITY	19
Security of Electronic Protected Health Information	19
Administrative Safeguards	19
Physical Safeguards.....	20
Technical Safeguards	20
User Responsibilities	20
Accepted Uses of Electronic Resources	21
NON-Acceptable Uses of Electronic Resources	21
Where to Find Help	22
SECTION V HIPAA DEFINITIONS.....	23

VIRGINIA COMMONWEALTH UNIVERSITY HEALTH SYSTEM INTEGRITY AGREEMENT

VCU HEALTH SYSTEM COMPLIANCE PLAN

VCU Memo

V i r g i n i a C o m m o n w e a l t h U n i v e r s i t y

Health System MCV Hospitals and Physicians

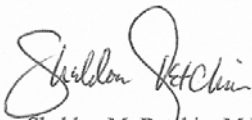
A Message from the Senior Management of the Health System

Welcome to Virginia Commonwealth University Health System. As an academic medical center we are united by a common mission of superior patient care, education, and research. The VCU Health System is committed to improving the quality of and access to patient care in Central Virginia and throughout the Commonwealth. With dedicated physicians, nurses, and clinical care and administrative staff, the VCU Health System has gained an excellent reputation for patient satisfaction and is nationally recognized for quality and innovation.

The 7,000 members of our Health System demonstrate dedication and passion for our mission, vision, and values on a daily basis. As new employees, it is essential to make this same commitment in reviewing and adhering to the standards outlined in the VCU Health System's policies and procedures as well as the accepted standards of your professions. Compliance with the laws and regulations that govern our industry is the responsibility of every member of the VCU Health System.

Our mission articulates the values and priorities that serve as the foundation for the VCU Health System's Code of Ethics, Code of Conduct, Compliance Program, and Privacy Policy. The New Employee Compliance and Privacy Manual should assist you in fulfilling your responsibilities in a manner consistent with our mission, vision, and core values.

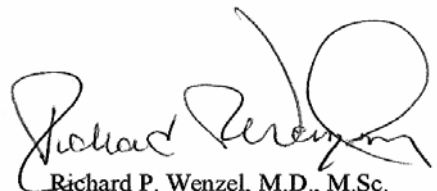
We wish you much success in your new role with the VCU Health System, and we appreciate your efforts in support of our compliance program.



Sheldon M. Retchin, M.D., M.S.P.H.
CEO
VCU Health System



John F. Duval
CEO
MCV Hospitals



Richard P. Wenzel, M.D., M.Sc.
President
MCV Physicians



The VCU Health System (VCUHS) and all of its component companies are committed to conducting business in accordance with all applicable laws, regulations, policies, and procedures. The purpose of the Compliance and Privacy Plans is to articulate for all employees and other affiliated individuals our commitment to ethical standards and our responsibilities for compliance with regulatory and privacy policies.

This New Employee Compliance and Privacy Manual is a summary of the VCU Health System's "Compliance Program," "Code of Conduct," and "Privacy Policies." It describes the legal and ethical obligations of each VCU Health System employee

and requires each employee to maintain compliance with the laws and regulations governing our businesses. This manual provides you with information concerning the process behind making the VCU Health System Compliance and Privacy Programs work and how they apply to you.

VCU Health System Mission and Vision and Core Values

Mission

The VCU Health System is committed to improving the quality of and access to patient care in Central Virginia and throughout the Commonwealth by:

- Providing superior, compassionate, and innovative patient care to improve the health of all members of the communities we serve.
- Educating the health-care professionals of tomorrow, health-care providers of today and the community at large.
- Advancing the generation, dissemination, and application of biomedical research.

Vision

Improving the health of all people as the preeminent academic health center in the region with national recognition for specialty care, innovative research and workforce development.

Values

Service

We will execute every customer interaction with a caring attitude, honesty and respect, putting our customer's needs first to yield exceptional customer service.

Trust

Through our integrity, respect of individual and diversity and commitment to privacy and safety, we achieve trust from those we serve and from those with whom we work.

Attitude

Our attitude is that in the pursuit of excellence, we display kindness, concern, compassion and appropriate charity to those in our care.

Respect

We respect the dignity of each individual and the collective diversity of the communities we serve.

VCU HEALTH SYSTEM COMPLIANCE PROGRAM POLICY

Philosophy

VCU Health System is committed to conducting all facets of its operations in compliance with relevant laws, regulations, policies, and procedures. The foundation for that approach is a zero tolerance for fraud and abuse with every effort being made to eliminate waste. The VCU Health System compliance plan and policies are designed to be a continuous process of education, monitoring, detection, correction, and reeducation where needed.

The benefits of this plan are to establish a structure to:

- Maintain operations in compliance with laws and regulations;
- Provide information to the VCU Health System Board of Directors and the Health System Compliance Committee on the status of organizational compliance;
- Make legal and policy changes quickly in response to identified compliance needs;
- Increase organization-wide vigilance of legal and regulatory requirements;
- Respond appropriately to investigations, audits, and other compliance issues that may arise; and
- Decrease the likelihood of civil liability.

VCU HEALTH SYSTEM CODE OF ETHICS

The Virginia Commonwealth University Health System is committed to an environment of uncompromising integrity and ethical conduct. Our ethical standards are the foundation for our decisions and actions. As employees of the Virginia Commonwealth University Health System our actions will be guided by these principles and values:

- **Respect:** We will respect individuals, diversity, and the rights of others.
- **Honesty:** We will act and communicate honestly and candidly. We will not mislead others.
- **Excellence:** We will strive for excellence in all that we do.
- **Responsibility and Accountability:** We will be responsible and accountable for our decisions and actions and will comply with the laws, regulations, policies, and procedures that govern our Health System activities.
- **Stewardship:** We will be good stewards of the resources entrusted to the Health System.
- **Compliance:** We will understand and comply with the codes, laws, regulations, policies, and procedures that govern our Health System activities.

We recognize that our decisions and actions reflect not only upon our individual reputations but also upon the reputation of the Health System. Our actions will be guided by these ethical principles and values even when confronted by personal, professional, social, or economic pressures.



VCU HEALTH SYSTEM STANDARDS OF PROFESSIONAL CONDUCT

The Virginia Commonwealth University Health System Authority Board of Directors approved Standards of Professional Conduct (the "Standards") is designed to provide guidance to all staff in carrying out their daily responsibilities. The Standards is based upon four principles that are the core of our mission and reflect the values of our organization. These are areas that are the highest priorities for us as health care providers and require our most careful attention and oversight.

The standards and guidelines set forth describe expectations for professional conduct and give further direction in carrying out the principles of The Standards. However, the standards may not provide easy instruction in all situations, given the complex nature of the health care environment and the difficult issues we often confront. You are encouraged to seek advice from your supervisor, the hospital policy and procedure manual, Human Resources, General Counsel, or other campus resources when dealing with conduct-related matters.



Principles:

The following principles are the legal and ethical foundations of The Standards:

- ***Dignified Patient Care*** - Treat all patients with dignity and respect recognizing the diverse cultures and communities served by the Health System.
- ***Compliance with Laws and Regulations*** - Adhere to all applicable standards of professional practice, all applicable federal and state laws and regulations, and demonstrate ethical behavior in all aspects of business.
- ***Responsibility for Actions and Behaviors*** - Report any concern you may have that a patient's care may be at risk or that staff are not meeting ethical or legal standards.
- ***Accuracy and Accountability*** - Provide and maintain accurate and reliable financial records and raise any questions or concerns related to compensation, expenses, or patient billing and reimbursement to your supervisor or other members in the chain of command.

VCU HEALTH SYSTEM COMPLIANCE STANDARDS

Standard 1 - Patient Care

VCUHS will provide health care in a manner that is of the highest quality, clinically appropriate, cost efficient, and takes into account a patient's right to be involved in their choice of care.

All care given to patients must be consistent with accepted standards of care and based upon medical necessity not the patient's ability to pay.

Providing an appropriate level of quality care involves informing the patient about the alternatives and risks associated with the care they may receive and obtaining consent of the patient, legal representative or family for the performance of all procedures. The VCUHS focus on patient centered care also requires health care providers, to the extent possible and appropriate, to involve patients and family members in the clinical decision-making and plan of care process.



Standard 2 - Workplace Responsibilities

VCUHS is committed to providing a work environment of fairness, dignity, and respect for all employees.

VCUHS is an equal opportunity employer and is committed to providing a work environment that is free from unlawful discrimination and/or harassment and workplace violence. If an employee or affiliated individual believes they are being subjected to discriminatory, harassing, or violent behavior, or observe or receive a complaint regarding such behavior, they have an obligation to report it to their supervisor, Human Resources, or other members of the chain of command. Retaliation against individuals for raising claims of discrimination, harassment, or workplace violence is prohibited. Retaliation violations can result in disciplinary action up to and including termination of employment.

Employees must not engage in actions, which create a threat to the health, safety, or security of our patients and other employees. Therefore, reporting to work or being at work under the influence of alcohol or illegal drugs is strictly prohibited and is considered cause for termination.

Standard 3 - Business Information and Records

Reasonable efforts will be made to protect personal and confidential information of VCUHS, its patients, and employees. All patient care and institutional records are the property of VCUHS. Staff responsible for the preparation and retention of the records shall ensure that records are accurately prepared and maintained in a confidential manner and location as prescribed by law and Health System policy.

While working at or with VCUHS, employees may learn or have access to confidential or proprietary information. This information entrusted to you by VCUHS, our patients, and customers must be maintained with the highest level of discretion and confidentiality.

Confidential and/or proprietary information includes, but is not limited to:

- Patient information, including information in electronic medical records;
- Employee information that would be considered confidential without prior authorization;
- Information about VCUHS financial or other performance or existing and/or potential contracts;
- Sign-on codes, usernames, and passwords;
- VCUHS systems and software;
- Other sensitive information.

Standard 4 - Conflicts of Interest

All VCUHS staff shall conduct clinical and personal business in a manner that avoids perceived conflicts of interest.

Employees and individuals affiliated with VCUHS must avoid gaining business or financial interest or participating in activities or services that would, or would appear to:

- Create an excessive demand upon their time and attention while scheduled to be at VCUHS;
- Use their position within the Health System to influence a VCUHS decision in which an employee has a financial interest;
- Use the VCUHS name and/or logo to promote or sell non-VCUHS products or services;
- Promote or receive an improper financial or other benefit, either directly or indirectly, to you, another employee, family member, a VCUHS customer or patient, partner, contractor, or service provider.

The above are limited examples of potential conflicts of interest, inquiries regarding potential or perceived conflicts of interest and transactions constituting a conflict of interest must be directed to the General Counsel's office.

Standard 5- Competitive Behavior

VCUHS and its staff will comply with all applicable antitrust laws.

Antitrust laws protect patients and providers by promoting competition and ensuring that patients have health care choices that reflect an open market. Staff should be knowledgeable about activities that may be in violation of antitrust laws. Examples of forbidden activities include, but are not limited to the following:

- Agreements, or attempts to agree, with a competitor to artificially set prices or salaries, to divide markets, to restrict productivity, or to restrain new competitors from the market;
- Disclosure of pricing information to competitors that is not normally available to the public; and
- Unfair business practices, boycotts (including agreements to deal or not to deal with certain patients, providers, or payors) deception, intimidation, misappropriation of business information, and similar unfair practices.

Standard 6 - Coding and Billing of Patient Services and Cost Reporting

Staff responsible for the charging, coding, billing, documentation, and accounting for patient care services for the purpose of billing governmental, private or individual payors must comply with all applicable state and federal regulations, payor contracts, and specific policies and procedures.

VCUHS will bill only for services actually provided and will collect only the amount to which it is entitled. VCUHS will not tolerate any instance in which billing misrepresents the actual services performed. The following are guidelines to assist in the performance of coding and billing activities:

- All claims for services provided must be accurately and completely coded and submitted to the appropriate payor in accordance with applicable laws, regulations, contractual obligations, and VCUHS policies and procedures.
- All documentation of orders and services must be complete, legible, and accurately reflect the services or items provided.
- All patients will be consistently and uniformly charged. Discounts will be appropriately reported. Items and services will be consistently described so that comparability can be established among payors.
- Credit balances on patient accounts must be processed in a timely manner and in accordance with applicable rules and regulations.
- All claims submitted to any payor for payment must *only* be for those services or items that are medically necessary and consistent with generally accepted clinical standards for the diagnosis and treatment of disease and/or injury. Services requested by a patient that do not meet the medical necessity criteria may be provided if in accordance with VCUHS policies and procedures.

Standard 7 - Cost Reporting to the Government and Other Third Party Payors

Staff responsible for the preparation and submission of cost reports must ensure that all cost reports submitted to government and other third party payors are properly prepared and documented in accordance with all applicable federal and state laws and regulations.

All VCUHS staff responsible for preparation of cost reports must ensure that all costs are properly classified, allocated to the correct cost centers, and supported by verifiable data. Any errors identified in the preparation or submission of cost reports must be corrected in a timely and accurate manner and documented according to applicable regulations and Health System procedures.

Standard 8- Contact with External Entities

VCUHS is committed to maintaining open and accurate communication with respect to third party inquiries for information and on-site visits and providing privacy and security to our employees, patients, and visitors.

University News Services is the spokesperson for the Health System. Any inquiries or requests from the media or a third party involving VCUHS business, patients, documents or interview requests should be directed to your supervisor, the General Counsel's office, when appropriate, or other appropriately designated individuals.

Any government requests for information in conjunction with a federal inquiry or investigation should first be directed to your immediate supervisor, the General Counsel, Risk Management, or Compliance Services. Staff must obtain positive identification of the investigator and identify the subject of the request and information requested before consenting to interviews or providing an investigator with confidential patient, employee, or other VCUHS records, either in written or verbal form.

You have a legal right to consult with your supervisor, the General Counsel, Compliance Services, or where appropriate, University Counsel before answering questions surrounding an investigation.

Staff are expected to: cooperate with any government, internal, or external investigation; must never alter or destroy VCUHS records in anticipation of an investigation. Staff should also never attempt to persuade other employees to make false or misleading statements to an investigator or to alter or destroy records.

Standard 9 - Compliance

The Standards apply to all VCUHS staff, including but not limited to administration, faculty, physicians, fellows, residents, and students. Moreover, The Standards are applicable to all persons not employed by VCUHS but serving as the Health System's staff, contractors, vendors, and consultants.



What resources are available if I have a question?

You should direct questions and concerns to your immediate supervisor for clarification and/or direction.

The following resources are also available to assist you:

- The VCUHS policy and procedure manual
- The Department of Human Resources
- The Hospital Ethics Committee
- The Office of the General Counsel
- Compliance Services

*If there is a concern or issue that you do not feel comfortable discussing with your supervisor and would like to make a report without revealing your identity, the Compliance Services Helpline, 1-800-620-1438, exists for that purpose.

COMPLIANCE PROGRAM

Purpose of the Compliance Program

The VCU Health System Compliance Program was developed to define our ethical standards, principles and values and to provide guidance in complying with the laws that govern our businesses. We want to ensure compliance not only with these laws, but also with the ethical standards that are an integral part of the VCU Health System.

An effective compliance program is vital to preventing ethical and legal infractions. The adoption of a compliance program, with nothing more, does not give us an *effective* compliance plan. We must incorporate the high ideals and practices of this program into the daily routine of our business practices. The role of the Compliance Program is to offer us guidance in understanding our legal and ethical obligations; it is *our* role to make the Compliance Program effective—by participating in compliance training sessions, reporting compliance concerns appropriately, and making a personal commitment to the standard of integrity promoted by the Compliance Program.

We are each responsible for continually considering the ethical and legal merits of our business activities; the Compliance Program provides us with the guidance to do so effectively. Consult the Compliance Program policies if you question the appropriateness of your business activities or those of other VCU Health System employees, or if you are unsure of the correct procedures to follow. Access the Compliance Services Helpline to verify your understanding of the policies as they apply to you.

In addition to promoting our goal of meeting high ethical standards, the VCU Health System Compliance Program could protect us if a legal violation were to occur. More specifically, a company with an effective compliance program in place at the time of a violation can avoid the more severe penalties imposed by the Federal Sentencing Guidelines which dictate the punishment to be imposed for federal offenses.

Employees have the responsibility to keep themselves informed of updates and revisions to VCU Health System policies. Management reserves the right to change policies at its discretion and without advance notice. Management has the right to interpret the provisions of this summary, as well as, corporate policies and procedures. Management further reserves the right to make exceptions to policies, procedures, or the provisions of the summary if it is deemed to be appropriate. Also, check with your supervisor for additional departmental guidelines that may be enforced.

*Information contained in this summary is effective as of May 2005. All updates/revisions will be clearly marked with corresponding effective dates.



8 Elements of a Model Compliance Plan

1. Written Policies and Procedures
2. Designation of Responsibilities
3. Communication of Standards
4. A Reporting Mechanism
5. Response to Identified Offenses
6. Conducting Audits
7. Investigations and Enforcement
8. Evaluating the Program

*The VCU Health System's Compliance Program has been formulated based on the eight elements of a model compliance plan as recommended by the Health and Human Services Office of the Inspector General.

Legal and Ethical Obligations

Each VCU Health System employee must conform to all laws and regulations that apply to VCU Health System business. The individual policies contained in this summary describe specific responsibilities you must fulfill in order to perform your duties as a VCU Health System employee within the bounds of the law. However, you also have basic responsibilities, which apply to the overall Compliance Program:

- *Know the policies.* Learn the details of the policies that relate to the work you do as a VCU Health System employee. While you are not expected to know every policy word for word, you should have a basic understanding of the issues covered under each policy and a more detailed understanding of those policies that apply to your job.
- *Ask questions.* If you have questions about any of the policies and how they apply, seek assistance from your manager, the Compliance Department or the Office of the General Counsel. You are not expected to become a lawyer, if you are not sure about your actions, **ask**.
- *Think before you act.* If you encounter any of the following warning signs, pay attention and think before you act. These signs may indicate a legal dilemma which should be avoided at all costs:

“Well, maybe just one time.”

“The competition is doing this, why can’t we?”

“Off the record...”

“No one will ever know.”

“What’s in it for me?”

“We have procedures, but we’ve got a business to run, so...”

- *Report concerns.* You are required to report promptly:
 - Any concerns you may have about possible violations of a compliance policy;
 - Any concerns others may have about possible violations of a compliance policy; and
 - Any concerns about a possible request to violate a compliance policy.
- *Seek resolution.* If you report a policy concern and the issue is not resolved, raise it with one of the other contacts listed in this booklet under “Where to Find Help.”
- *Cooperate.* You are expected to cooperate with VCU Health System investigations into concerns involving violations of compliance policies.
- *Attend Training Sessions.* VCU Health System offers a wide range of training opportunities designed to enhance your knowledge of corporate programs, policies and procedures.



What are my basic responsibilities as a VCU Health System employee?

1. Know the policies
2. Ask questions
3. Think before you act
4. Report concerns
5. Seek resolution
6. Cooperate
7. Attend training sessions

Meeting VCU Health System's high ethical standards is also important. In addition to following the law, each VCU Health System employee is required to practice ethical business conduct, which is well above the minimum requirements of the law. We want our patients, physicians and business contacts to be comfortable with our company, and we want you to feel good about yourself and your colleagues. The slightest hint of inappropriate business conduct can damage our reputation, even when the law is being followed. To avoid even the *perception* of wrongdoing, conduct all of your business practices with honesty, fairness and integrity. These qualities are evidenced by truthfulness and the absence of deception or fraud.

False Claims Act

The prohibition against false claims arises under both the Federal False Claims Act and the Virginia Fraud Against Tax Payers Act. The False Claims Act encompasses health care fraud, false claims, and false statements of material fact and allows any person who discovers fraud on the federal or state government, to report it through specialized procedures. VCU Health System also encourages and provides employees procedures for communicating fraud or abuse through our Compliance Helpline, 1-800-620-1438 or via the web at <https://www.compliance-helpline.com/welcomePageVCUHS.jsp>. The following is an overview of the provisions of the False Claims Act as well as the protections for those who report violations of federal, state, or VCUHS policy.

- **Health Care Fraud**

Any attempt to obtain money or property from a health care benefit program, such as Medicare, Medicaid, or state health plans through false pretenses. This can include billing for services that were never given or billing for a higher reimbursement than the services produced.

- **False Statements**

A statement in connection with a government benefit program, whether oral or written that an employee deliberately makes or causes to be made, which he or she knows to be untrue.

- **False Claims**

The act of filing, presenting, or conspiring to use a record to defraud the government into paying or approving a claim for benefits under a government benefit program, which an employee knows to be untrue or misleading.

- **Whistleblowers**

A whistleblower is a current or former employee or member of an organization who reports misconduct or wrongdoing within their organization to outside persons or entities that have the power to take corrective action.

- **Protection of whistleblowers**

The False Claims Act was amended in 1986 to encourage protection for whistleblowers. Under the False Claims Act, an employer is prohibited from harassing or retaliating against an employee for attempting to uncover or report fraud against the government. No employee who in good faith reports a violation shall suffer harassment, retaliation or adverse personnel actions. Any employee who retaliates against someone who has reported a violation in good faith is subject to discipline, up to and including dismissal from VCU Health System. Employee are encouraged to tell their supervisor, a human resources representative, the Compliance Officer, or contact the VCUHS Compliance Helpline if they feel retribution has been taken against them or another employee.

- **Violations of the False Claims Act**

- Knowingly presenting (or causing to be presented) to the federal government a false or fraudulent claim for payment.
- Knowingly using (or causing to be used) a false record or statement to get a claim paid by the federal government.
- Conspiring with others to get a false or fraudulent claim paid by the federal government.
- Knowingly using (or causing to be used) a false record or statement to conceal, avoid, or decrease an obligation to pay money or transmit property to the federal government.

- **Violations within the healthcare environment**
 - Examples of violations of the False Claims Act that are specific to our healthcare environment include, but are not limited to the following:
 - Billing for work or tests not performed
 - Double billing
 - Charging more than once for the same goods or service.
 - Kickbacks or bribes
 - Forgery of a physician's signature
 - Fraudulent cost reports
 - Upcoding:
 - Billing at a doctor's rate for work that was actually conducted by a nurse or resident intern.
 - Inflating bills by using diagnosis codes that suggest a more expensive illness or treatment.
 - Unbundling
 - Using multiple billing codes instead of one billing code for a drug panel test in order to increase remuneration.

- **Penalties for violations under the False Claims Act**

For those who knowingly submit or cause another person or entity to submit false claims for payment of government funds, federal penalties include liability for three times the government's damages plus civil penalties of \$5,500 to \$11,000 per false claim. Similarly, state penalties include liability of \$5,500 to \$11,000 per false claim and liability for three times the amount of damages sustained by the Commonwealth of Virginia.

Penalties for Violation

Our compliance policies should govern your behavior and decisions while at VCU Health System. It is your responsibility to be familiar with these policies and to be sensitive to any situation that could lead you or others to engage in actions that would violate them. Ignorance, good intentions or bad advice will not be accepted as excuses for noncompliance. Employees who fail to comply with these policies are subject to disciplinary action, up to and including dismissal.

The following list of employee infractions and violations applies to the VCU Health System Compliance Plan. Consistent with the Federal Sentencing Guidelines, VCU Health System will treat the listed infractions as follows:

Employee Action	*Corrective Action
Negligently providing incorrect information to VCU Health System or a government agency.	First Offense: Written Counseling/Reprimand Second Offense: Formal Discipline (no suspension) Third Offense: Suspension without pay Fourth Offense: Termination
Willfully providing false information to VCU Health System or a government agency, customer, insurer, or the like.	Termination
Felony violation of any state or federal criminal statute.	Determination made based on offense and job requirements
Willful failure to report conduct by an employee of VCU Health System, which a reasonable person should know is criminal.	Termination
Willful failure to report another employee's violation of any duties under this Compliance Plan or being a party to a report containing false or misleading information.	First Offense: Suspension without pay Second Offense: Termination

Intentional misuse of the Compliance Helpline by knowingly and willfully providing false information to the Chief Compliance and Privacy Officer.	Termination
Willful failure to detect conduct by an employee of VCU Health System, which a reasonable person should know is criminal and reasonably could be expected to detect.	First Offense: Suspension without pay (if willful) Second Offense: Termination
Willful failure to take action as prescribed under the VCU Health System Compliance Plan or to comply with any duties, express or implied forth in the Plan.	First Offense: Formal written reprimand Second Offense: Suspension without pay Third Offense: Termination or demotion
Engaging in any conduct prohibited in the employee handbook and/or by policy that is considered unbecoming to a VCU Health System employee.	First Offense: Written Counseling/Reprimand Second Offense: Formal discipline Third Offense: Suspension without pay Fourth Offense: Termination

Breaking the law and subjecting yourself or the company to criminal penalties (fines or jail sentences) or civil sanctions (damage awards or fines) is also a violation. All charges related to criminal penalties must be reported promptly to your supervisor for determination as to impact on performing job duties pending the outcome of court action.

VCU Health System will cooperate with law enforcement authorities and regulatory agencies in connection with the investigation and prosecutions of any employee who violates applicable state and federal laws governing the VCU Health System.

*The VCU Health System has a policy of progressive discipline for infractions committed by an employee. The form of discipline imposed will be case specific. Whether the violation involved simple negligence, gross negligence, or willfulness will be considered in determining and administering punishment. Additionally, the form of punishment will be influenced by (a) whether the employee promptly reported his or her own violation; (b) whether the report constitutes VCU Health System's first awareness of the violation and the employee's involvement; (c) whether the employee cooperates fully in investigating and/or correcting the violation; and (d) the employee's previous record of disciplinary actions.

Training

We are committed to training you on the laws that govern the areas you will deal with as a VCU Health System employee. After your initial training, supplemental training will vary depending on the position you hold. If you do not feel you have received adequate training on the laws that govern your areas of responsibility, you are expected to notify your supervisor, the Chief Compliance and Privacy Officer, a human resources representative, or call the Compliance Helpline, so you can meet your obligations as a VCU Health System employee. We view this as a team effort, and we are committed to helping each other meet the obligations, which VCU Health System has adopted on behalf of all staff and associates.



New employees will be introduced to the VCU Health System's Compliance Program and HIPAA standards during their new employee orientation. Within 30 days of dates of hire, designated employees should access the HIPAA on-line Healthcare Compliance Training (<http://www.vcuhealth.org/employees.asp>) and successfully complete the required modules.

Chief Compliance and Privacy Officer

The VCU Health System has appointed a Chief Compliance and Privacy Officer to oversee the Compliance Program. The Chief Compliance and Privacy Officer is assigned responsibility for the Compliance Helpline and is available to address your concerns and questions regarding this Compliance Program.

You should feel completely at ease in contacting the Chief Compliance and Privacy Officer for any reason relating to the Compliance Program. The Compliance Officer is a neutral point-of-contact with whom you can confidentially discuss your concerns and questions regarding the compliance process and/or report suspected compliance violations.

The Chief Compliance and Privacy Officer may recommend changes to the Compliance Program to improve the compliance process, as necessary, based on information provided by VCU Health System management and communications with individual VCU Health System employees.

The Chief Compliance and Privacy Officer makes periodic reports to the Authority Board concerning developments in the Compliance Program. These reports, which are made on an as needed basis, but no less than annually, include the results of compliance audits and annual reviews, allegations of wrongdoing, ongoing investigations, and developments and changes in relevant laws, which may affect Compliance Program policies.

Reporting Concerns

It is your obligation to report any violation of these policies. If you are concerned that a violation of a compliance policy has occurred, you should discuss the situation with your supervisor, a human resources representative or the Compliance Officer. You also may contact the VCU Health System Compliance Helpline at 1-800-620-1438. All calls to the Compliance Helpline will be treated fairly and all communications will be kept in confidence. If you are not comfortable with making your report in person or by telephone, you may send your written concerns to:

Compliance Services
P.O. Box 980471
Richmond, VA 23298-0471

VCU Health System employees at all levels are prohibited from taking retribution or retaliating against anyone for reporting or supplying information about a policy concern. If you feel retribution has been taken against you or another employee, tell your supervisor, a human resources representative, the Compliance Officer, or contact the VCU Health System Compliance Helpline.



Where to Find Help

Compliance Helpline (available 24 hours a day):.....1-800-620-1438
Compliance e-mail:complianceservices@mcvh-vcu.edu
Compliance Services:1001 East Broad Street, Suite 205 (Old City Hall)
P.O. Box 980471
Richmond, VA 23298-0471

Cynthia H. Earnhardt,
Chief Compliance and Privacy Officer:(804) 828-0500
Robert "Buzz" Willis,
HIPAA Privacy Issues:(804) 628-1853
David Houlette,
Information Security Officer:(804) 628-1144
Human Resources.....(804) 628-0649

HIPAA AND PRIVACY

HIPAA – It's The Law

This section is about the VCU Health System privacy and confidentiality policies. Because each department may have its own policies, this section will concentrate on the Health Insurance Portability and Accountability Act (HIPAA), which is a set of federal regulations that apply to all areas within the Health System. It contains information that will help you understand important ways in which HIPAA affects your job. If you think a person's right to privacy might be broken by an action you are about to take, it will be useful to read applicable parts of this document again.

The HIPAA law has many parts, but three of the regulations (rules) that must be followed are especially important:

- The Privacy Rule
- The Security Rule
- The Electronic Transactions and Code Sets Rule

The Privacy and Security Rules require that employees receive training about how the two Rules work and what the workers need to know to do their jobs in a way that does not violate the law. Employees in a business that has health information about people must keep that health information private and safe. There are fines and penalties for not keeping a person's health information private and safe.

The law allows two kinds of fines and penalties—civil and criminal. Some examples of fines and penalties for breaking the HIPAA law are:

- Fines of \$100 per violation per person (can't be more than \$25,000 total per calendar year) for anyone who knew or should have known about this law (this means you);
- Fines of up to \$50,000, or going to prison for up to one year, or both if a person's health information was knowingly used inappropriately (the violation was not a mistake);
- Fine of up to \$100,000, or going to prison for up to five years, or both for inappropriately accessing a person's health information by falsely claiming a reason to have it; and,
- Fines of up to \$250,000, or going to prison for up to 10 years, or both for any worker or health care business that knowingly discloses (gives to another person or business) or obtains a person's health information so they can harm the person or so they can get something they want (like money in exchange for the information).

PROTECTED HEALTH INFORMATION

What is Protected Health Information (PHI)?

Protected health information (PHI) is health information that could reveal the identity of a person. Under the HIPAA regulations, PHI identifiers include:

- Name
- Street Address, City, County, Precinct, Zip Code
- Dates (except year) that directly relate to a person (including birth date, admission date, discharge date, date of death, and all ages over 90)
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers



What is HIPAA?

In 1996, Congress passed a law called the Health Insurance Portability and Accountability Act, or HIPAA. This law says that employees can keep their health insurance when changing jobs. Also, the law protects a person's medical information. It requires that hospitals, doctor's offices, health insurance companies and other businesses that keep medical information must insure it is private and safe from someone getting or seeing it when they should not.

- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifiers (for example, finger prints or voice prints)
- Full-face photographs or similar images
- Any other unique identifying number, characteristic or code



The above identifiers apply to health information in forms such as:

- Electronic records
- Paper records
- Spoken words (including telephone and voice-mail)
- Faxed documents

The Importance of Protected Health Information (PHI)

Under this law, a person's health information is protected from discriminatory (unfair to the person) or wrongful use or disclosure. Disclosure means to release, transfer, or provide access to protected health information, or to give PHI in any way, to anyone outside the VCU Health System. Examples of discriminatory or wrongful use or disclosure are:

- Insurance companies using protected health information to deny life or disability coverage;
- Employers using protected health information to make decisions about hiring or firing; and
- Nosy neighbors, family members or reporters using protected health information for their own ends (curiosity or sometimes to make money).

Treatment, Payment, and Health Care Operations (TPO)

Protected health information (PHI) is health information that could reveal the identity of a person. The law allows PHI to be used or disclosed for medical treatment of a person, handling payment activities for the medical services or products the person received, and health care operations (the day to day work of a health care business). These are called TPO uses and disclosures. In most cases, PHI cannot be used or disclosed for non-TPO purposes without getting the person's written permission (authorization).

Minimum Necessary Information

HIPAA allows using and disclosing (giving to another person) a person's protected health information (PHI) for Treatment, Payment or Health Care Operations (TPO) without getting special written permission from the person. But the use or disclosure of PHI for TPO reasons must be limited to the minimum (least amount) necessary information to do the TPO job. The VCUHS has policies and procedures that direct employees to access only the "minimum necessary" PHI for the TPO jobs the employee does. Departmental policies and procedures must clearly explain if the employee has limits on his or her access to (to be able to get) and use of PHI based on what the worker does in his or her job. A worker may have access to computers and computer networks, but what he or she is allowed to access in the computer programs may be limited.

Reasonable Safeguards for PHI

The VCU Health System must work to provide "reasonable safeguards," to make sure that PHI stays private. The safeguards used should not slow down, delay, or stop quality patient care. Examples of reasonable safeguards are:

- Using lowered voices in reception, registration, or other common areas so PHI can't be overheard;
- Setting up curtains or temporary wall dividers to create semi-private spaces in common areas for discussion;
- Physicians dictating notes in a private location, such as an office, rather than in a hall or other common area;
- Properly getting rid of PHI on paper not kept in paper medical records (for example, patient name and dietary information on food tray cards, or lab containers with patient names and

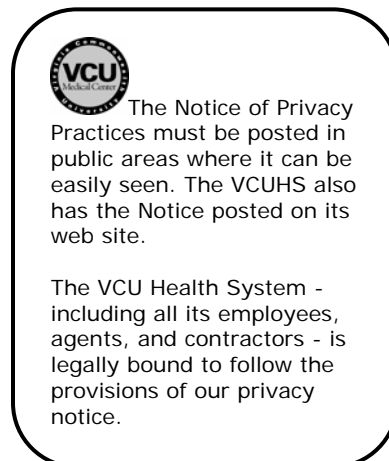
- tests to be performed on the contents); and,
- Being careful not to reveal PHI when leaving voice-messages on answering machines.
- Never using PHI in email that is not entirely behind the VCUHS Firewall.

Notice of Privacy Practices

Providers of health care and health insurance plans are required by HIPAA to make a good faith effort to give a written notice to individuals who receive healthcare or who are covered under the health insurance plan. This written document is called the "Notice of Privacy Practices." It explains the uses and disclosures of protected health information made by the VCU Health System for treatment, payment or health care operations. With respect to using and disclosing PHI, an individual's rights and our responsibilities are also explained in the notice. In addition, the VCU Health System must:

- Obtain the individual's written acknowledgment that he or she received the notice of privacy practices;
- Document the reasonable efforts made to obtain written acknowledgment.

If an emergency exists and the individual is unconscious or unable to communicate, the individual may be treated without receiving the Notice of Privacy Practices. However, the notice must be given to the individual as soon as his or her condition permits or it may be given to someone legally allowed to act on the individual's behalf. Written acknowledgement that it was received must be obtained, or an explanation for why the written acknowledgement could not be obtained from the individual must be documented.



Written Authorization (Permission) is Required for Non-TPO Uses or Disclosures

Health care businesses may use PHI for treatment, payment, and health care operations (TPO) without specific authorization from the person. Other uses or disclosures need the person's written authorization. The person (or someone legally acting on the person's behalf) must sign that he or she authorizes the use or disclosure described on the form.

The VCU Health System's Authorization Form can be found on the VCU HIPAA Website (<http://www.vcu.edu/amsweb/HIPAA/amshipaa.htm>). It includes:

- The specific uses and disclosures that will be made of the person's protected health information;
- Space for it to be signed and dated by the individual or a person legally acting on the patient's behalf; and,
- Clearly written information so that the person can understand what he or she is authorizing.

Treatment or health care insurance coverage may not be refused when a patient refuses to authorize such uses or disclosures of PHI. When there is an overriding public interest, limited use and disclosure of PHI for purposes that are not TPO can take place without authorization. "Limited use" means that only the PHI that is necessary to meet the overriding public interest need may be used or disclosed without authorization. Examples of overriding public interest include:

- Public health activities and other governmental functions;
- Reporting abuse or neglect; or,
- Under appropriate circumstances, judicial or law enforcement purposes.

A person must authorize a PHI disclosure requested by an employer. If the person does authorize the disclosure of PHI to the employer, that PHI becomes part of the employment record and is no longer protected health information. Examples of this situation are a person authorizing a doctor to give the employer PHI about a medical condition that makes sick leave necessary; or a person might authorize disclosure of the findings in a fitness for duty examination to obtain employment.

Patient Rights Under HIPAA

A person generally has certain rights regarding his or her PHI under HIPAA. These rights include:

- To receive a written notice that explains how the person's PHI will be kept private and how it might be used or disclosed;
- To access, inspect or copy his or her own PHI;
- To request that changes be made to his or her own PHI;
- To request that disclosure not be made to certain persons (for example a family member);
- To request that communications that include his or her PHI be made in other ways or to other locations than the health care business usually uses;
- To receive a listing of all PHI disclosures that were not for treatment, payment, or health care operations; limited data sets (see Appendix A: Definitions); or very minor, unintended disclosures (like someone overhearing PHI in a waiting room even though the receptionist was using a lowered voice).

The VCU Health System has responsibilities with regard to these patient rights. These responsibilities are:

- To allow the individual access, inspection, and copying of PHI within 30 days if the PHI is on-site and within 60 days, if the PHI is off-site;
- To determine whether a requested amendment of PHI is appropriate and, if appropriate, to make the amendment requested unless:
 1. HIPAA does not allow the patient access to the PHI (such as Psychotherapy notes),
 2. the PHI is already accurate and complete, or
 3. the provider being asked to amend it did not create the PHI and the creator is available to address the amendment request
- To give an accounting of PHI disclosures for the six-year period before the individual's request (the six year period does not extend back before the implementation date of the Privacy Rule – April 14, 2003).
- An accounting of disclosures does not include disclosures made for treatment, payment, or health care operations, those based on a patient's signed authorization, incidental disclosures, or those that were part of a limited data set.
- To document, maintain and honor reasonable requests to restrict the communication of PHI to specified locations or in specified ways for a minimum of six years (except in emergencies).

Patients Do Not Have The Right To Access, Inspect, and Copy All PHI

Some exceptions to the rights listed above are:

- Psychotherapy notes
- Information that a health care professional thinks could be harmful to the patient
- Information for use in a civil or criminal trial or administrative proceeding
- Certain laboratory information

If access to certain PHI—but not all PHI—is denied, then only the denied information may be kept from the individual, and the rest of the information must be given.

De-Identified and Limited Data Sets

Health information is considered de-identified when it does not identify an individual and the VCU Health System has no reason to believe that the information can be used to identify an individual. The Privacy Rule allows two possible ways for health information to be de-identified:

- Using generally accepted statistical and scientific principles and methods to declare that the patient cannot be identified, or
- Removing all of the PHI identifiers (see "Protected Health Information (PHI)" above) from the health information.

In either case, very small or no risk that the remaining health information could be used to identify an individual can exist.

A limited data set has all direct PHI identifiers removed (see Appendix A: Definitions for a list of PHI identifiers that may remain in the data set) and leaves selected indirect identifiers. A Data Use Agreement between the covered entity giving the limited data set and the entity receiving it must be in place before the limited data set can be given.

HIPAA Privacy Rule and State Privacy Law

In addition to the federal HIPAA Privacy Rule, Virginia also has privacy laws. State privacy law, instead of the HIPAA Privacy Rule, must be followed when they are tougher than HIPAA. This happens in two ways:


- When the HIPAA Privacy Rule does not address something the State privacy law does address, and
- When certain parts of a State privacy law are tougher than the parts of HIPAA that deal with the same topic.

When only part of a State privacy law is tougher than the HIPAA Privacy Rule, only that part must be followed and the rest of the time the HIPAA Privacy Rule must be followed.

HIPAA AND SECURITY

Security of Electronic Protected Health Information (E PHI)

These security guidelines outline minimum standards for ensuring the confidentiality and integrity of electronic protected health information (E PHI) received, maintained or transmitted by the VCU Health System (VCUHS), as well as other offices which support our organization. All VCUHS Department/Entities shall meet or exceed these standards by implementing the necessary administrative, physical and technical safeguards as appropriate based, on their assessments of risk.



Is the HIPAA Security regulation the same as the HIPAA Privacy regulation?

While closely linked, the HIPAA (Health Information Portability and Privacy Act) Security regulation is different from the HIPAA Privacy regulation because it applies to the Electronic storage and transmission of Protected Health Information (E PHI), compared with the privacy regulation which applies to all forms of PHI and prescribes more detailed requirements for securing data

Electronic protected health information (E PHI) is identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

Electronic media means:

- Electronic storage media including memory devices in computing workstations (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory device (USB drive, iPod, PDA, etc.); or
- Transmission media used to exchange information already in the form of electronic storage media. Transmission media include, for example, the Internet, Intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage

media. Certain transmissions, including of paper via facsimile and of voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

VCU Health System has put into place a number of measures to protect critical information assets and sensitive electronic information:

Administrative Safeguards (Policies, Procedures, Guidelines, etc.)

- Risk analysis – Periodic evaluations of the existing security safeguards for critical electronic information assets and recommendations for improving the management of information security risks.
- Access – Procedures that provide access to E PHI by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction or process.

- Sanctions - Appropriate sanctions against workforce members who fail to comply with the security procedures of the organization.
- System Monitoring - Procedures to regularly review records of information systems activity, such as audit logs, access reports, and security incident tracking reports.
- Workforce Supervision - Procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.
- Appropriate Access - Procedures to determine that the access of a workforce member to EPHI is appropriate to support her/his role in business or clinical operations.
- Access Termination - Departmental procedures for terminating access to EPHI when employment ends or need for access no longer exists.
- Business Associate Obligations - Ensure safeguards are contractually mandated with any Business Associate or transaction clearinghouse that may have access to Health System EPHI.
- Awareness Training – On-going security awareness through training or other means that provide workforce (including management) with updates to procedures and policies for guarding against, detecting and reporting malicious software.
- Incident Response – Procedures for responding to, documenting and mitigating where practicable, suspected or known security incidents and their outcomes.
- Contingency and Disaster Planning – Procedures for ensuring that continued availability of mission-critical information resources in the event of unforeseen circumstances (floods, fires, hurricanes, terrorism, etc.)

Physical Safeguards (Doors, Walls, Locking Devices, etc.)

- Physical Access - Procedures to limit physical access to EPHI and the facility or facilities in which it is housed while ensuring that properly authorized access is allowed.
- Physical Identification Validation - Access must be physically safeguarded to prevent tampering and theft. Procedures must address control and validation of a person's access to facilities based on his/her role or function, including visitors, employees, faculty, students and vendors.
- Media Movement - Procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.
- Media Final Disposition - Procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored. Procedures include process for removal of EPHI from electronic media before the media is made available for other use.

Technical Safeguards (Computer Security Hardware or Software)

- User Sign-on - Access procedures that assign unique names or numbers for identifying and tracking user identity. Electronic sessions terminate automatically after a predetermined time. EPHI must be encrypted and decrypted when necessary and appropriate for electronic transmission.
- Data Integrity - Procedures that protect EPHI from improper alteration or destruction, which include a mechanism to authenticate EPHI and corroborate that it has not been altered or destroyed in an unauthorized manner.
- Authentication - Procedures or mechanisms to verify that a person or entity seeking access to EPHI is the one claimed.
- Data Transmissions - Technical safeguards to insure EPHI transmitted over an electronic communications network (including wireless networks) is not accessed by unauthorized persons or groups, and that such information is not improperly modified without detection until disposed of.
- Auditing – Monitoring information assets in order to detect unauthorized or inappropriate use or disclosure of electronic sensitive information such as EPHI.

User Responsibilities

The VCUHS systems and data are for use only by the individual granted access. Access must not be shared, since shared use often leads to abuse. User accounts must be protected with passwords. Login scripts must not include scripted passwords.

The user must ensure that any restricted information stored on his/her personal computer is safeguarded through physical security (locked offices or keyboards), access control software, and/or encryption.

When a computer is left signed on, it is easy for someone to gain unauthorized access. Users must either sign off before they leave their computer, or restrict access by some other means (locked office/keyboard,

desktop access control, or a password-protected screen saver). Note, however, that many access control packages and screen savers can be easily bypassed.

As an individual whose position requires interaction with the VCU Health System's information systems, you may be provided with direct access to confidential and valuable data and/or use of data/voice systems. In the interest of maintaining the integrity of these systems and of ensuring the security and proper use of Health System resources, you must:

- Maintain the confidentiality of your password for all systems to which you have access.
- Maintain in strictest confidence the data to which you have access. Any confidential information must not be shared in any manner with others who are unauthorized to view such data.
- Use your computer access for the sole purpose of conducting official business of the Health System. Understand that the use of these systems and their data for personal purposes is prohibited.
- Understand that any abuse of access to the VCU systems and their data, or any illegal use or copying of software, any misuse of the Health System's equipment may result in disciplinary action, loss of access to the computer systems, and possible termination of employment.
- Report immediately any actual or suspected violations of information security to your supervisor or Information Security.

Use of Electronic Resources

Use of the VCU Health System electronic information environment should be in support of the Health System's mission of education, research and service.

By using the VCUHS electronic information systems you assume personal responsibility for their appropriate use and agree to comply with all applicable VCU Health System policies, as well as city, state and federal laws and regulations.

VCUHS reserves the right to monitor your usage of its electronic information systems, including email, for inappropriate, improper, or unauthorized use and/or unauthorized disclosure of sensitive electronic information.

Improper use of information systems and/or equipment can result in penalties up to and including loss of system access and employment termination. In addition some activities may lead to risk of legal liability, both civil and criminal.

NON-Acceptable Use of Electronic Resources

The following specific uses of VCU Health System computing resources are not allowed. This is not a complete list of prohibited practices, but is intended to illustrate the general standards involved with the use of computers. Additional specific prohibitions may be enforced for individual computer systems or networks or departments.

The following activities and behaviors are prohibited:

- Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication;
- Acquiring or attempting to acquire passwords of others;
- Using or attempting to use the computer accounts of others;
- Alteration of the content of a message originating from another person or computer with intent to deceive;
- The use of computer resources or electronic information without or beyond one's level of authorization;
- The interception or attempted interception of communications by parties not explicitly intended to receive them;
- Making Health System computing resources available to individuals not affiliated with the VCUHS without approval of an authorized official;
- Making available any materials the possession or distribution of which is illegal;
- Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential;
- Intentionally compromising the privacy or security of electronic information and revealing

HIPAA Definitions

- Covered Entities - HIPAA defines these to include:
 - Health care providers that transmit any health information in electronic form in connection with one of the transaction formats covered in the Electronic Transaction Rule,
 - Health plans, and
 - Health care clearinghouses.
- Data Custodians – The VCUHS organizations or their staff that are responsible for maintaining sensitive information on local servers, VCUHS servers, mainframes or the individuals that maintain the logical and physical information on a workstation that they are responsible for.
- Disclosure - Disclosure means the release, transfer, provision of access to (to be able to get) Protected Health Information (PHI)), or divulgence of PHI in any manner to anyone outside the entity that maintains the PHI.
- Health Information - Any information, whether oral or recorded in any other form or medium, that:
 - Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
- Limited Data Sets
 - These PHI DIRECT Identifiers *must* be removed to create a Limited Data Set:
 - Name
 - Postal address information (other than City, State, and Zip Code)
 - Telephone and fax numbers
 - E-mail address
 - Social security number
 - Certificate/license number
 - Vehicle identifiers and serial numbers
 - URLs and IP addresses
 - Full-face photos and other comparable images
 - Medical record numbers, health plan beneficiary numbers, and other account numbers
 - Device identifiers and serial numbers
 - Biometric identifiers including finger and voiceprints

After the Direct Identifiers are removed, these are the only elements of PHI that may remain for a Limited Data Set:

- Geographic subdivisions (City, County, Precinct, State, Five Digit Zip Code)
- Dates
 - Birth Date
 - Date of Death
 - Admission, Discharge, and Service Dates
 - Age (including age 90 or over)
- Minimum Necessary Information - The principle that, to the extent practical, individually identifiable health information should only be disclosed to the amount needed to support the purpose of the disclosure.

- Privacy - Limiting who may have access to information about an individual. It also means that those authorized to have access to information about an individual must keep the individual's health information confidential. In other words, the information must not be disclosed to others who are not involved in the individual's direct treatment, payment for the individual's treatment, or other health care operations defined in the entity's "Notice of Privacy Practices" without written authorization from the individual.
- Treatment - The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another.
- Workforce or Workers – Under HIPAA this means employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity.
- Workstation – Can be owned by VCUHS or be the personal property of the personnel; connected (cable or wireless) to a local or VCUHS server or remain standalone; (e.g. Blackberry, cell phone, laptop, PDA, remote dictation unit, desktop computer, laboratory diagnostic instrument, fax, digital camera, handheld bedside or data collection unit, intelligent wristband or proximity badge).



Virginia Commonwealth University Health System Integrity Agreement

I _____, acknowledge that I have received and understand the *Virginia Commonwealth University Health System (VCU Health System) Compliance and HIPAA Summary for New Employees*.

I understand that every employee is required to comply with the provisions described in the summary as well as the full text of the policies and procedures of the VCU Health System.

I understand that the summary is intended as a general overview only and that the full text of the policies is available from department directors or Compliance Services.

The information presented is intended to be accurate as of the published date. The provision of the summary as well as all VCU Health System policies and procedures are subject to change (without prior notice) based on VCU Health System needs and administrative approval. It is the responsibility of each employee to keep himself or herself informed of updates and revisions to VCU Health System policies and procedures. All updates/revisions will be clearly marked with corresponding effective dates.

SIGNATURE _____

DATE _____

NAME _____
Please Print

DEPARTMENT _____



Virginia Commonwealth University Health System Integrity Agreement

**REMOVE THIS PAGE FROM BOOKLET. PLEASE COMPLETE AND RETURN
AT THE COMPLETION OF NEW EMPLOYEE ORIENTATION**

I _____, acknowledge that I have received and understand the *Virginia Commonwealth University Health System (VCU Health System) Compliance and HIPAA Summary for New Employees*.

I understand that every employee is required to comply with the provisions described in the summary as well as the full text of the policies and procedures of the VCU Health System.

I understand that the summary is intended as a general overview only and that the full text of the policies is available from department directors or Compliance Services.

The information presented is intended to be accurate as of the published date. The provision of the summary as well as all VCU Health System policies and procedures are subject to change (without prior notice) based on VCU Health System needs and administrative approval. It is the responsibility of each employee to keep himself or herself informed of updates and revisions to VCU Health System policies and procedures. All updates/revisions will be clearly marked with corresponding effective dates.

SIGNATURE _____

DATE _____

NAME _____
Please Print

DEPARTMENT _____



MCV Hospitals and Physicians

VCU HEALTH SYSTEM COMPLIANCE PLAN

**To read the full test version of
The VCUHS Compliance Plan please go to:**

<http://www.corpcomp.mcvh-vcu.edu/>

and click on the words “Corp Compliance Plan”