VCU Health System

Compliance and Privacy Program

Updated October 2024

Table of Contents

I. PURPOSE OF THE COMPLIANCE AND PRIVACY PROGRAM

The VCU Health System Compliance and Privacy Program (the Program) was developed to support VCU Health System's (VCUHS) ethical standards, principles, and values. The Program provides guidance in complying with regulations governing our business, as specified by the Office of the Inspector General (OIG) of the Department of Health and Human Services (HHS). The Program includes VCUHS affiliates and team members. The Program supports the mission of VCUHS by providing guidance for the prevention and correction of compliance- and privacy-related matters. The Program provides consultation, education, investigation, auditing, monitoring, and enforcement. The mission of the Program is to promote a culture of integrity and accountability by providing collaborative, risk-based, and objective services. Compliance and Privacy Services will partner with VCUHS departments in the implementation and management of the Program.

Compliance and Privacy Services supports the effectiveness of the Program by providing compliance and privacy training, encouraging good faith reporting of all concerns, timely responding to the compliance and privacy concerns, promoting appropriate remedial action, and committing to the standard of integrity promoted by the Program.

The Program routinely evaluates the ethical and organizational risks of VCUHS business and clinical activities for those areas outlined below in section B, Compliance and Privacy Services. Compliance and Privacy Services team members have the responsibility to keep themselves informed of updates and revisions related to the compliance industry and patient privacy in order to be an effective resource to VCUHS.

An organization with an effective compliance and privacy program in place at the time of a violation may avoid more severe penalties imposed by the U.S. Federal Sentencing Guidelines and Office for Civil Rights. VCUHS will review all suspected noncompliance to determine if an investigation is needed, and report all confirmed violations of regulations and law to the appropriate regulatory or law enforcement agency, as well as plan sponsors as required by contract.

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

- Facilitate conduct of operations in compliance with laws and regulations;
- Advise on regulatory and policy changes in a timely manner, responding to identified compliance and privacy needs;
- Increase organization-wide vigilance of legal and regulatory requirements;
- Respond appropriately to investigations, audits and other compliance and privacy issues; and
- Decrease the likelihood of wrongdoing or recurrence which could lead to criminal and civil liability.

II. ELEMENTS OF AN EFFECTIVE PROGRAM

The Compliance Program is based on the elements of an effective compliance program as set forth in the Federal Sentencing Guidelines and the guidance provided by the Department of Health and Human Services (HHS) Office of the Inspector General (OIG.) The Privacy portion of the Program is governed by guidance provided by the HHS Office for Civil Rights (OCR). This Program addresses each of the elements.

A. STANDARDS, POLICIES AND PROCEDURES

An effective program defines the expected conduct of VCUHS' team members through written policies and procedures. VCUHS is committed to following applicable laws and regulations. Compliance and Privacy Services supports this commitment by creating and maintaining appropriate policies and procedures to guide team members in their work environment. These policies and procedures are developed to reflect laws and regulations that include, but are not limited to, those laws and regulations that address health care fraud, waste, and abuse for example, the Federal False Claims Act, Stark Law, Anti-Kickback Statute, the Heath Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH). The policies are developed under the direction of the Compliance Committee, Executive Leadership, and other key stakeholders and are provided to team members. VCUHS' policies and procedures are maintained on the VCUHS Intranet in a searchable database and are made accessible to all VCUHS team members. Policies and procedures are revised to reflect changes in law, regulations, or identified risks of VCUHS.

In support of VCUHS' commitment to an environment of uncompromising integrity and ethical conduct, VCUHS has established a Code of Conduct. It is the expectation of the Health System that each team member embraces the Code of Conduct in support of safety, teamwork, accountability, relationships, and STAR Service.

B. PROGRAM STRUCTURE AND OVERSIGHT

The development and management of the Program is a collaborative effort between the VCUHS Operational Compliance Committee and Compliance and Privacy Services.

VCUHS Operational Compliance Committee

The primary function of the VCUHS Operational Compliance Committee is operational oversight. The Committee assists the Chief Compliance and Privacy Officer in the following responsibilities:

- Implementing the Program throughout the clinical enterprise;
- Obtaining senior management support and partnership;
- Collaborating with operational and supporting departments to align strategic decision making with risk management and compliance;
- Gaining business unit support and partnership;
- Reviewing proposed documents for board level approval;

- Providing review and discussion of departmental annual work plans;
- Assisting in identifying and addressing key risks to the enterprise.

VCUHS Authority (VCUHSA) Board of Directors - Audit and Compliance Committee

The Audit and Compliance Committee is composed of individuals with diverse experiences and backgrounds. The Committee is comprised of four or more Directors. The majority of the Directors are external with no financial, family, or other material personal relationships that would infringe on their independent oversight of compliance activities. Internal Directors are also a part of the Committee. The Committee is governed by a charter, which is updated annually.

The Audit and Compliance Committee meets at least four times annually. Additional meetings may be required depending on the circumstances.

The Audit and Compliance Committee's responsibilities include, but are not limited to:

- Receive notification of investigations into any matters within the Audit and Compliance Committee's scope of responsibilities;
- Monitor VCUHS' conflict of interest policies and related procedures;
- Review and approve the Compliance and Privacy Program document on an annual basis;
- Review and approve the annual Compliance and Privacy Services work plan and any significant changes to the plan;
- Review annually the qualifications of the Compliance and Privacy Services staff, the level of staffing, and the departmental budget;
- Assess the effectiveness of the Program's function, including its independence and reporting relationships;
- Review completed reports and progress reports on executing the approved work plan;
- Require management to report on those procedures that provide assurance that the VCUHS Code of Conduct and VCUHS compliance and privacy policies are available to all team members;
- Review results of compliance reviews to ensure systems and controls are designed to reasonably ensure compliance with laws and regulations, VCUHS policies, and the Code of Conduct consistent with OIG and OCR requirements, as well as privacy laws;
- Inquire of the Chief Audit and Compliance Executive and/or the Chief Compliance and Privacy Officer regarding any difficulties encountered during compliance reviews, including any restrictions on the scope of work or access to required information.

Chief Compliance and Privacy Officer

VCUHS has a designated Chief Compliance and Privacy Officer to oversee the Program. The Chief Compliance and Privacy Officer is a senior-level individual responsible for the implementation, administration, and oversight of the VCUHS Compliance & Privacy Program. This person is the lead administrator for the Program and reports to the Chief Audit and Compliance Executive with a dotted line to the CEO of VCUHS.

Team members should feel comfortable contacting the Chief Compliance and Privacy Officer for any reason relating to the Program. The Chief Compliance and Privacy Officer, or designee, is a neutral point-of-contact with whom team members can confidentially, to the fullest extent permitted by law and/or VCUHS policy, discuss their concerns and questions regarding the compliance and privacy process and/or report suspected compliance or privacy violations.

The Chief Compliance and Privacy Officer may recommend changes, as needed, to the Program to improve the process based on information provided by management, the Audit and Compliance Committee, and communications with team members.

The Chief Compliance and Privacy Officer is responsible for the following:

- Implementation of the Program, which includes supervision, monitoring, auditing, and reporting activity within the scope of the program;
- Providing leadership for VCUHS' compliance efforts, to include serving as the authority on risks associated with billing for hospital and professional services;
- Developing policies and procedures for implementation and operation of the Program;
- Encouraging awareness among health care providers and other team members about compliance and privacy matters and the importance of adherence to the Code of Conduct by developing, coordinating, and participating in a training program that focuses on compliance- and privacy-related issues;
- Maintaining a retaliation-free system for reporting non-compliance or concerns related to federal and state regulations, VCUHS policies, and the Code of Conduct;
- Assisting in the development of corrective action plans;
- Serving as the Privacy Officer for VCUHS and the VCU Affiliated Covered Entities;
- Collaborating with the Chief Information Security Officer on privacy and information security matters;
- Serving as the chair of the VCUHS Operational Compliance Committee;
- Reporting results of monitoring, auditing, and reporting activity to the VCUHSA Board of Directors - Audit and Compliance Committee, the VCUHS Operational Compliance Committee, the MCVP Board of Directors, and the MCVP Compliance and Audit Advisory Committee;
- In collaboration with the Office of General Counsel, retaining the services of attorneys, accountants, consultants, and other professionals as needed;
- Investigating reports of possible wrongdoing involving compliance- and privacy-related issues and reporting in a timely manner to the appropriate authorities;
- Monitoring the Compliance and Privacy Helpline and ensuring that issues are resolved in a timely and appropriate manner.
- Upholding the highest standards of ethics in research activities, ensuring all participant data is handled confidentially and in compliance with all policies, regulations, and applicable laws.

Compliance and Privacy Services

Compliance Services supports the mission of VCUHS by promoting a culture of

compliance through consultation, education, monitoring, and enforcement.

VCUHS departments and team members will cooperate with the Chief Compliance and Privacy Officer (and designees) in implementing the Program.

To carry out this mission, Compliance Services will:

- Develop and maintain the Program for VCUHS;
- Routinely assess and monitor the effectiveness of the Program;
- Establish and support the VCUHS Operational Compliance Committee;
- Report on the status of the Program to the Board of Directors on at least an annual basis;
- Perform compliance and privacy risk assessments as needed;
- Provide compliance and privacy education for team members, as appropriate to their responsibilities, on an annual basis;
- Develop and implement a compliance and privacy auditing and monitoring work plan based on the organization's identified risk;
- Monitor the implementation of billing regulations and guidelines;
- Monitor changes in regulations and provide guidance as needed to the appropriate operational areas;
- Develop and implement appropriate updates to policies and procedures regarding patient privacy and compliance matters related to fraud, waste, and abuse;
- Serve as a resource to operational departments regarding patient privacy issues and the prevention and detection of fraud, waste, and abuse;
- Collaborate with other supporting functions such as Revenue Cycle, Finance, Internal Audit, Information Technology, Health Information Management, Human Resources, Legal, Quality and Safety, Risk Management and Marketing to identify and address risks and other compliance concerns.
- Review all research activities pertaining to any research data, patients, or resources at VCUHS.

Compliance Services will provide guidance as needed in the areas identified by the Office of Inspector General, including:

Billing: Compliance Services will have specific authority to review the billings and billing practices for compliance with health care program requirements of any enterprise facility, department, or health care provider. The Chief Compliance and Privacy Officer (or designee) may restrict billing of any health care services if they believe that the billing would not comply with applicable laws and regulations and may require billing to be performed in a specific manner. VCUHS departments will notify the Chief Compliance and Privacy Officer before engaging any external billing consultant not affiliated withVCUHS. Additionally, any VCUHS department that receives or is made aware of an external audit or inquiry relating to billing must notify the Chief Compliance and Privacy Officer or designee in a timely manner.

- **Medical Necessity for Services:** Claims will be submitted to payers only for medically necessary services ordered by an appropriately licensed medical professional. Medical necessity is to be determined and documented by the responsible provider or other licensed individual. Medical necessity is

defined as a service that is reasonable and necessary for the diagnosis or treatment of an illness, disease, injury, or to improve the functioning of a malformed body member.

- **Billing for Items or Services Actually Rendered:** Claims that are submitted must be representative of an actual service performed by the provider. Only those medical services to patients that are consistent with acceptable standards of medical care may be billed. VCUHS will only bill for those actual services provided and will comply with applicable rules and regulations.

- **Billing with Adequate Documentation:** All documentation supporting claims must be complete and accurately reflect the service rendered to the patient. Documentation must comply with all applicable regulations and policies. A bill should not be submitted for payment if the documentation or scope of service is unclear.

- **Correct Coding:** The OIG recognizes inaccurate coding as a longstanding risk. Regulations, rules, and policies governing billing procedures are to be followed. Team members responsible for billing and coding will be trained in the appropriate rules governing billing, coding, and documentation.

- **Overcoding:** This occurs when a billing code representing a higher level of service and payment rate is used rather than the billing code that reflects the appropriate, medically necessary service provided to the patient. Team members responsible for providing and/or coding must not engage in any form of upcoding.

- **Duplicate Billing:** Reflects the practice of submitting more than one claim for the same service or submitting a claim to more than one primary payer at the same time. While duplicate billing may be seen as a billing error, repeated double billing could be viewed as a false claim, especially if the overpayment is not properly refunded.

- **Cost Reporting:** Cost reports will be prepared in compliance with applicable regulations. Cost reports must be prepared with appropriate and accurate documentation. Unallowable costs will not be claimed for reimbursement. In addition, all costs will be allocated to the appropriate accounting unit.

- **Overpayments:** Improper or excess payments that result from patient billing or claims processing errors will be returned to the patient and the Medicare Administrative Contractor (MAC) within 60 days of identifying the overpayment. In addition, overpayments identified through cost reports will be returned by the later of 60 days from when the overpayment is identified, or the date of the corresponding cost report.

- **Quality and Patient Safety Integration:** Patient safety and other quality compliance issues will be included in the risk universe for Compliance Review.

- **Anti-Kickback:** VCUHS will comply with laws and regulations relating to the prohibition of improper payments, bribes, kickbacks, interest-free loans, free or below market rents, or fees for administrative services. Team members may not offer, provide, accept, or ask for anything of value to influence or be influenced

by patients, their families, suppliers, contractors, vendors, physicians, third-party payers, managed care organizations, or government officials. Team members may not offer or accept anything of value in exchange for referrals for services covered by Medicare, Medicaid, or any other federal health care programs.

- **Self-Referrals:** Stark Law is a self-referral law prohibiting physicians from referring Medicare or Medicaid patients for certain "designated health services" where the physician or immediate family member has a financial relationship or financial interest. An example of a prohibited relationship would include an ownership or investment interest or a compensation agreement.

- **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; it allows any person who discovers fraud against the federal or state government to report it through specialized procedures known as Whistleblower Protections. Under the provisions of the False Claims Act, whistleblowers are afforded protection from retaliation or retribution for reporting dishonest or illegal activities. VCUHS also encourages and provides team members procedures for communicating fraud or abuse through the Compliance Helpline, 1-800-620-1438 or via the web at https://app.convercent.us/en-us/LandingPage/caa17cba-31d8-eb11-a840-000d3afda485

- **Conflicts of Interest or Commitment:** VCUHS is committed to maintaining the highest quality of care, treatment, and services unhindered by financial interest. Conflicts of interest include situations involving team members or their immediate families where activities may compromise or appear to compromise--a team member or a team member's immediate family member's judgment in performing any of their job duties. Conflicts of commitment include outside activities that interfere with or compromise an individual's ability to meet Health System responsibilities or obligations. All actual or perceived conflicts of interest or commitment must be disclosed to maintain VCUHS' culture of integrity and transparency. Additionally, team members deemed in a position of trust are required to complete additional reporting as outlined in the Code of Virginia and identified by the Virginia Conflict of Interest and Ethics Advisory Council (LD.LD.002 Annual State Conflict of Interest Disclosure Process).

- **Excluded Individuals and Entities:** The Health System is prohibited from employing or contracting with any individual or entity excluded from participation in federally funded health care programs. The OIG has exclusion authority pursuant to Sections 1128 and 1156 of the Social Security Act. All new hires are checked against the OIG List of Excluded Individuals and Entities (LEIE) prior to hire and team members are checked each month. Contractors are required to attest that neither their organization nor any of their employees have been excluded by a federally funded program.

Privacy for Research Compliance will provide guidance as needed in the areas identified by the Office for Human Research Protections (OHRP), including:

- **Common Rule (45 CFR 46):** VCUHS is committed to protecting the integrity

and confidentiality of individuals participating in research. VCUHS is required to comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, in addition to OHRP regulations, for research that involves Protected Health Information (PHI).

- **Informed Consent and Privacy:** VCUHS is required to ensure all researchers obtain legally effective informed consent from all research participants, unless a waiver is obtained. The informed consent forms should describe what PHI will be accessed, how long it will be retained, and how privacy will be protected.

- **Limited Data Sets and Data Use Agreements:** VCUHS is required to comply with all applicable federal and state privacy laws. In general, the more restrictive law applies.

- **Data Security and Confidentiality:** VCUHS upholds the Minimum Necessary Rule by ensuring researchers implement appropriate safeguards to protect PHI from unauthorized access, use, or disclosure. VCUHS directs researchers to minimize the collection and retention of PHI, keeping only what is necessary for the study.

Privacy Services provides guidance to comply with patient privacy laws and the Office for Civil Rights, including:

- **HIPAA Privacy and Security Rule:** VCUHS is committed to protecting the integrity, confidentiality, and availability of protected health information (PHI) in any format. VCUHS is required to implement administrative, technical and physical safeguards to prevent impermissible uses or disclosures of protected health information and to ensure compliance of its Team Members.

- **Federal and State Privacy Laws**: VCUHS is required to comply with all applicable federal and state privacy laws. In general, the more restrictive law applies.

- **Reporting:** VCUHS is required to conduct risk assessments of privacy violations. Following completion of a risk assessment, all breaches of protected health information which do not fit within an exception or that do not represent a “low probability of compromise” are reported to the Office for Civil Rights. VCUHS also provides patient and media notifications as required by OCR and notifications required by other regulatory bodies.

- **Business Associates:** Business Associates are persons or entities that perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or provide services to, VCUHS. VCUHS must have satisfactory written assurances, typically in the form of a Business Associate Agreement, that the Business Associate will appropriately safeguard the protected health information it receives or has created on behalf of VCUHS.

C. EDUCATION AND TRAINING

Compliance and Privacy Services is committed to providing training on the laws,

regulations, and best practices that relate to the areas described in Section B. After initial training at hire, supplemental training will vary depending on position or job responsibilities. Should a team member feel they have not received adequate training on the laws, rules, or policies that govern their area of responsibility, they are expected to notify their supervisor, the Chief Compliance and Privacy Officer, HR4U, or to call the Compliance Helpline at 1-800-620-1438. Team members may also send a request to complianceservices@vcuhealth.org.

Training courses will be conducted on compliance and privacy-related topics designated by the Chief Compliance and Privacy Officer based on feedback from the Compliance Committee, Executive Leadership, and other key stakeholders, as well as regulatory changes, and/or issues identified through internal audits and risk assessments.

Training content will include, but is not limited to:

- Identification and explanation of acceptable standards of practice defined by applicable regulatory authorities, including, but not limited to: health care compliance, billing procedures, coding, privacy safeguards, and associated documentation requirements;
- Identification and explanation of unacceptable compliance and privacy practices and improper activities;
- Explanation of the regulatory and institutional penalties for non-compliance;
- Explanation of the Program, its elements, auditing guidelines, monitoring activities, investigation protocols, and reporting procedures.
- Periodic updates given to health care providers and other team members about the Program, as well as significant changes in policy, procedure, or law.
- Periodic updates to the research community about pathways to access patient data and resources available.

Compliance Services will be given the opportunity to review training material(s) from outside vendors with adequate time for review prior to presentation. This includes materials related to general or research compliance, privacy, coding or billing documentation.

Mandatory Training: New Team Member, Annual Privacy and Annual Compliance trainings are mandatory. These trainings are intended to establish and thereafter reinforce “doing the right thing” in our environment. Completion will be tracked and reported using the learning management system. In addition to the mandatory training, Compliance and Privacy Services will identify, where necessary, specific training to address previous misconduct, and lessons learned from prior compliance and privacy incidents. Compliance and Privacy Services will evaluate the extent training has an impact on team members’ behavior or operations.

Mandatory training will include, but may not be limited to, the following and as outlined in policies mandating such training:

HR.EM.012: Compliance and Privacy Education

MCVP-05: Required Compliance Training for Billing Providers

D. AUDITING AND MONITORING

Compliance and Privacy Services will conduct compliance auditing and monitoring activities to detect violations of laws and regulations within its scope of work. Auditing and monitoring are both fundamental components of the Program and provide a means for measuring its effectiveness. Compliance and Privacy Services collaborates with third party vendors as related to these activities.

Auditing and monitoring activities utilize a standard methodology to identify, analyze, and address risks and are included in the yearly Compliance Work Plan. The Compliance Audit Work Plan is reviewed on a quarterly basis as described herein for continued relevance and reflects the dynamic OIG Work Plan, other enforcement activities, regulatory changes, and previous compliance audits.

Auditing is a detailed assessment of the environment's compliance with standards and regulations. Auditing may be from internal or external sources and either prospective or retrospective. Audits include written reports with findings, recommendations, and potential next steps. Audits are conducted following the VCU Health Clinical Enterprise Compliance Audit & Monitoring Plan (Appendix A).

Monitoring activities
Monitoring activities are routine (weekly, monthly, or quarterly) and are used to measure compliance in everyday operations. Team members and associates are expected to cooperate fully with any monitoring activity. Such monitoring is used to collect data on a regular basis to assess compliance with the established standards of practice-- specifically regarding billing guidelines, elements necessary to meet HIPAA Requirements, and those topics given special attention by the Office of the Inspector General (OIG).

Examples of monitoring include:

Privacy Monitoring
Privacy Services monitors the organization's compliance with HIPAA requirements by using system-based tools to detect privacy violations. The information is reviewed to address violations and collected and analyzed to identify risk areas and detect potential vulnerabilities to patient privacy that may be minimized with additional training or other internal controls.

Compliance Monitoring
Compliance Services monitors various coding, billing and compliance activities as needed to ensure that processes are working as expected and detect any anomalies that may need further review or audit.

E. ROUTINE RISK ASSESSMENT

An effective Program can be evaluated by the organization's identification and assessment of risks and the degree to which attention and resources are utilized to address such risks. Risk assessments are data driven based upon operational data and information across functions. Compliance Services is committed to assessing the risks of non-compliance and misconduct in the environment and monitoring on a regular basis, paying special attention to high-risk areas. Compliance Services has

developed a methodology to assess risks and takes appropriate steps to review the Program annually for needed changes to assist in mitigating non-compliance. The department utilizes lessons learned from prior risk-related issues, as well as issues affecting teaching hospitals. Risk assessments may include evaluating concerns identified by the OIG, the Centers for Medicare and Medicaid Services (CMS), or the Office for Civil Rights (OCR). These steps include the following:

- Conducting risk-based audits;
- Aggregating and reviewing data obtained through incident management;
- Conducting question-based risk reviews;
- Collaborating with Quality and Patient Safety and other supporting departments to identify risks related to those areas;
- Updating the compliance work plan based on incident management and audit data; and
- Recommending updates to policies, procedures, and controls.

F. OPEN LINES OF COMMUNICATION AND REPORTING

Compliance Services helps to maintain a transparent environment in which team members are expected to bring forth concerns as well as reportable events, as described below, regarding conduct that is inconsistent with applicable laws, regulations, policies, and procedures. Team members have the responsibility to report actual or suspected misconduct. For more information on reporting obligations, see VCUHS policy LD.RM.002 Compliance Reporting.

If a team member is concerned about a reportable event, they should discuss the situation with their supervisor, HR4U, or the Chief Compliance and Privacy Officer (or designee). A report may also be made to any Compliance Services team member. A concerned team member also may contact the VCUHS Compliance Helpline at 1-800-620-1438, or through the compliance web-based reporting system at https://app.convercent.us/en-us/LandingPage/caa17cba-31d8-eb11-a840-000d3afda485. All reports to the Compliance Helpline will be treated fairly and communications will be kept in confidence. If a team member is not comfortable with making a report in person or by telephone, written concerns may be sent to:

Chief Compliance and Privacy Officer
Compliance and Privacy Services
Box 980471
Richmond, VA 23298-0471

Concerns may also be sent by email to complianceservices@vcuhealth.org. While some methods, such as the Compliance Helpline, allow for anonymous reporting, all reports, regardless of method of intake, will be kept confidential to the extent possible. In the event an investigation reveals a violation of legal or compliance standards, the impacted department or operational unit will be responsible for taking necessary and appropriate responsive and corrective actions. Compliance Services will provide consulting and monitoring assistance to the department or operational unit, as needed, in conjunction with other VCUHS departments, such as the Office of General Counsel, Human Resources, Financial Services, and/or Patient Relations. Compliance Services, in partnership with the Office of General Counsel, will assist with appropriate disclosure of reportable events. The effectiveness of the Compliance Helpline is measured through periodic surveys and tracking calls from

start to finish.

Reportable Event

A reportable event is any matter that a reasonable person would consider to be fraud, waste, or abuse, a violation of the Program, a violation of the Code of Conduct, a violation of VCUHS policy or procedure, or a violation of applicable law or regulation for which penalties or exclusions may be authorized.

Types of violations that should be reported may include, but are not limited to:

- Billing and documentation concerns;
- Conflicts of interest or commitment;
- Anti-kickback or self-referral concerns;
- Fraud, waste, and abuse concerns;
- False statements to a government agency;
- Falsification of any documents;
- Privacy concerns such as unauthorized access, use or disclosure of PHI;
- Actual or potential criminal violations.

VCUHS has a zero-tolerance policy of retaliation for reporting compliance and privacy concerns. For information regarding anti-retaliation, see policy HR.SC.001, Standards of Behavior and Performance. Incidents involving this behavior will be immediately reported to Compliance and Privacy Services.

Reported acts of retaliation, harassment, or intimidation against any individual who is a party to an investigation will be reviewed promptly. Appropriate corrective action will be implemented as necessary.

G. RESPONDING TO CONCERNS

Upon receiving notification of an allegation, the Chief Compliance and Privacy Officer (or designee) will make a preliminary determination whether the allegation involves an issue that should be investigated by Compliance and Privacy Services or if it should be forwarded to another department with subject matter expertise.

Responsibility for conducting the investigation will be decided on a case-by-case basis. Those assigned to Compliance and Privacy Services will result in written status and resolution reports provided to the Chief Compliance and Privacy Officer in accordance with the compliance reporting and investigations procedure.

A summary report of all Compliance Helpline calls will be provided annually to the Board of Directors' Audit and Compliance Committee.

Upon completion of an investigation performed by Compliance Services, if a corrective action plan is required, the Chief Compliance and Privacy Officer has the responsibility to monitor for resolution and to report outcomes to VCUHS Leadership. Corrective action plans will be in writing with consultation from the appropriate administrative or clinical senior level official.

Results of investigations requiring a corrective action plan will be reported to the appropriate leadership. The Chief Compliance and Privacy Officer will also report the results of the investigation to the VCUHSA Board of Directors, Audit and Compliance

Committee, the VCUHS Operational Compliance Committee, and the MCVP Compliance and Audit Committee, as appropriate.

If an investigation reveals a violation of legal or compliance requirements, Compliance Services, in conjunction with other appropriate areas, will take necessary responsive and corrective action, including the disclosure of reportable events to appropriate federal and state authorities.

H. ENFORCEMENT AND CORRECTIVE ACTION

VCUHS is committed to an environment of integrity and "doing the right thing." Team members are to perform their job duties in a manner that upholds the Code of Conduct and Program philosophy. In addition, team members are to display STAR Service in their daily work environment.

VCUHS policies and procedures govern a team member's behavior and decisions while at VCUHS. Team members must be familiar with these policies and be sensitive to any situation that could lead them to engage in actions that would violate the policy. Ignorance, good intentions, or bad advice will not be accepted as excuses for non-compliance. Team members who fail to comply with these requirements are subject to corrective action, up to and including separation of employment.

VCUHS utilizes corrective action steps to address noncompliant behavior. Compliance and Privacy Services will partner with Employee Relations regarding recommended corrective action and ensure that disciplinary action is fair and consistent across VCUHS. Consequences for noncompliant behavior apply equally to all levels of team members.

Compliance and Privacy Services will cooperate with law enforcement authorities and regulatory agencies in connection with the investigation and prosecution of any team member who violates applicable laws and regulations governing VCUHS. Probable violations of law will be reported to the appropriate law enforcement agency.

Corrective Action Policy, HR.SC.013

I. EVALUATION OF PROGRAM EFFECTIVENESS

Maintaining an effective compliance program is an essential process as outlined by the OIG and Department of Justice (DOJ). Compliance Services recognizes the importance of measuring the effectiveness of the compliance program. The department has developed and implemented metrics that assist in the consistent measure of the program. The following are examples, but not all inclusive, of metrics and other mechanisms to assess program effectiveness:

- Measure the effectiveness of incident responses per 100 team members by the type of incident;
- Conduct policy and procedure assessments to measure effectiveness in the environment (i.e. Statement of Economic Interests and exclusion reviews);
- Measure the ethical culture of VCUHS through surveys utilizing the seven elements of compliance; and/or

- Measure the effectiveness of education and training based on completion rates and the volume of incidents received.

III. CONCLUSION

The Compliance and Privacy Services Program (Program)_was created to support the ethical standards, principles, and values of VCUHS. In addition, it provides guidance to aid in complying with certain laws and regulations that govern our business. The Program is based on the model compliance program recommended by the Office of the Inspector General (OIG).

The Program is an evolving program that responds to changes in laws and regulations governing VCUHS, as well as to identified risks through internal monitoring and formal audits. Such laws and regulations refer to billing, coding, documentation rules, results of audits, or suggestions by the leadership team and governing committees. Compliance and Privacy Services is responsible for keeping team members informed of updates and revisions as they relate to industry standards.

Compliance Helpline

1-800-620-1438 24/7/365
Toll Free & Confidential

VCU Health offers a confidential helpline where you can report concerns regarding questionable or potential violations of policy, laws and regulations governing our business or patient privacy matters. **If you suspect or witness inappropriate conduct, call the Compliance Helpline to make a report.**

Questions or Concerns?
Online: Compliance and Privacy Reporting Portal
Email: ComplianceServices@vcuhealth.org
Office: 804-828-0500

Scan the QR code to visit the Compliance Services website.

If you need further assistance in resolving your concerns, other resources are available to help you:

Compliance Services.....**804-828-0500**
Clinical Administrator.....**804-628-0034**
Epidemiology.....**804-828-2121**
24 Hour Pager #4085
Human Resources.....**804-628-HR4U**
Information Security, On-Call Analyst.....**804-519-6841**
Patient Centered Services.....**804-628-0400**
Patient Safety.....**804-828-8731**
Regulatory Compliance Coordinator.....**804-828-9342**
Risk Management.....**804-828-1707**
After Hours Pager #6107
Safety and Security Office.....**804-828-6595**

VCU Health™

Approved 11/04; 3/07; 10/07; 11/08; 10/09; 10/10; 10/11; 8/12; 10/13; 9/14; 8/15; 9/16; 8/17; 10/18; 12/20; 12/22; 12/23, 12/24

Appendix A

SECTION I: ESTABLISHMENT AND PURPOSE OF THE VCU HEALTH CLINICAL ENTERPRISE COMPLIANCE AUDIT & MONITORING PLAN.

A. PURPOSES OF THE COMPLIANCE AUDIT & MONITORING PLAN:

1. The purpose of the Compliance Audit & Monitoring Plan is to align with the OIG's expectation of a standardized auditing and monitoring process, which is one of the seven elements of an effective compliance program;

2. To evaluate correct documentation, coding and billing for all health care services and compliance with applicable laws, regulations, policies, and manual instructions pertaining to Medicare, Medicaid and federal health care programs;

3. To detect and mitigate fraud, waste and abuse;

4. To mitigate financial and reputational risk to the VCUHS and its affiliated entities;

5. To promote timely and efficient compliance auditing and monitoring coordination among the VCU Clinical Enterprise;

6. To implement the compliance guidance recommendations of the Office of the Inspector General (OIG) and the Department of Justice (DOJ).

SECTION II: COMPLIANCE RISK ASSESSMENT & WORK PLAN

A. Compliance Services has a routine risk assessment process and written fiscal year work plan describing the audit and monitoring activities intended to be undertaken by the Clinical Enterprise per quarter.

B. The work plan is reviewed by the VCUHS Chief Compliance Officer (CCO) for final approval.

C. The Compliance Coordinators of each entity participate in the risk assessment process and development of a work plan based upon data analysis, regulatory guidance and/or changes, special requests, past audits and identified potential compliance risks faced by the organization.

D. The work plan identifies the individual or individuals responsible for undertaking the plan's activities, which may include internal team members or external reviewers.

E. Compliance Coordinators of each entity collaborate on a quarterly basis to identify opportunities, potential risks, and other concerns to promote efficiency and consistency in results and reporting.

F. As risk assessment is an ongoing and evolving process, the audit and monitoring work plan is assessed quarterly for updates and modification.

G. At times, the risk assessment may not result in an audit. On these occasions, Compliance Services works with the entity to mitigate identify risks. Mitigations

efforts include process development and/or process improvement.

SECTION III: AUDITING

A. Resources

1. Compliance Services will maintain sufficient resources to coordinate and/or conduct the auditing activities of the Clinical Enterprise taking into account working with individual entities to engage in self-auditing and monitoring activities.

2. Upon request of the Compliance Coordinator of each entity, the VCU Health CCO may approve the utilization of external auditors based on need. The persons or entities responsible for conducting the audit or review will have knowledge of health care compliance requirements in the specific audit area and must have valid VCU Health contractual agreements in place.

B. Audit Scope

1. Provides structure and clarity around the issue and outlines the breadth of the review and sampling methodology;

2. Utilizes the data analytics tools available to the organization e.g. auditing software, internal data metrics;

3. Assesses the risk to the Clinical Enterprise of non-compliance to the process under review;

4. Includes the audit or monitoring rationale, sample size, dates of service, target completion date, and as applicable all procedure billing codes and processes under review;

5. Must be approved by Compliance Services prior to the initiation of all scheduled audits and ongoing monitoring activities.

C. Procedure

1. It is the expectation that management of areas under audit will cooperate fully and respond in a timely manner to an auditor's request for necessary documents or information.

2. Audits are conducted from a representative, judgmental, or statistically valid sample as appropriate and outlined in the audit scope.

3. Audits are routinely conducted retrospectively but may also be prospective at the discretion of the VCU Health CCO as necessary for risk mitigation.

4. As applicable to the audit scope, documentation is reviewed to confirm:

i. Services rendered are supported and accurately billed as per American Medical Association (AMA) coding guidelines;

ii. Adherence to applicable policies and procedures;

iii. Adherence to CMS requirements, as well as National and Local Coverage Determinations (NCDs and LCDs).

5. If during the audit process the potential need for attorney privilege is identified by the entity's Compliance Coordinator, they consult Compliance Services. The VCU Health CCO, or his/her designee, initiates the appropriate legal counsel consultation if necessary.

6. Corrective Action Plans (CAPs) are required follow-up actions to any audit that does not meet the accuracy expectation established by the VCU Health CCO.

SECTION III: MONITORING

1. Routine monitoring activities are conducted retrospectively by Compliance Services.

2. Regularly scheduled monitoring of high-risk areas is performed by Compliance Services through data analytics on a monthly basis or as individually outlined in ongoing CAPs.

3. Compliance Services will review each entities' ongoing CAP monitoring activities for effectiveness.

4. Departmental prospective monitoring may be required when a high-risk area is identified.

SECTION IV: REPORTING

1. At the conclusion of each audit, a timely summary report will be provided to Compliance Services and individual departmental stakeholders as applicable.

2. Routine monitoring activities are recorded on a monthly basis with a summary provided to the VCU Health CCO each quarter.

3. Compliance Services reports each affiliated entity's auditing and monitoring activities to the Compliance and Audit Committee of the VCU Health Board on a quarterly basis:

i. current status, outcomes, identified trending and monitoring of CAPs of all internal audit activities;

ii. current status of ongoing data monitoring and investigations related to billing activities; and

iii. evaluation and results of all audits conducted by external government entities.