CHESTERFIELD COUNTY
ADMINISTRATIVE POLICIES AND PROCEDURES

Department:	**Human Resource Management**	**Policy Number:**	**6-4**
Subject:	**Privacy of Information**	**Supersedes:**	**09/01/15**
		Date Issued:	**06/30/16**

I. PURPOSE

The purpose of this policy is to establish a process for developing and implementing specific policies to protect the privacy of personal information. This policy also addresses the county's obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among other provisions, HIPAA requires that the county provide specific measures to ensure the security and privacy of Protected Health Information **(**PHI**)** that the county obtains about certain individuals. This policy sets forth the county's policy and procedure for ensuring compliance with the security and privacy requirements imposed by HIPAA. This policy is divided into two parts.

Sections III - V pertain to privacy of Personal Information. Sections VI – VIII pertain to HIPAA privacy compliance. Departments that do not meet the definition of a HIPAA Business Associate or HIPAA Covered Entity need only comply with Sections III - V. Departments meeting the definition of a HIPAA Business Associate or HIPAA Covered Entity must comply with all sections of this policy.

II. DEFINITIONS

A. **HIPAA** - Health Insurance Portability and Accountability Act of 1996

B. **HIPAA Business Associate** –Internal county departments conducting business on behalf of HIPAA Covered Entity Departments that involves the disclosure or use of protected health information (PHI). Such departments include Accounting, IST, County Attorney, Human Resource Management, Internal Audit, Risk Management and the Treasurer.

C. **HIPAA Covered Entity Department** - The departments of Mental Health Support Services, Fire & EMS and HRM, to the extent that it administers the county's self-insured health plan, are considered Covered Entities under HIPAA because these departments transmit protected health information (PHI) electronically.

D. **Non-Record Document** – Includes, but is not limited to, working papers, drafts, rough notes, research used to formulate a final record copy of a document, duplicate copies of a public record, carbon paper and unused pre-printed forms.

E. **Personal Information** – For the purpose of this procedure, personal information shall include the social security number, date of birth, home address, personal telephone numbers, personal e-mail addresses, bank account numbers and credit card account numbers of a person.

F. **Protected Health Information (PHI)** - PHI as defined by HIPAA. Individually identifiable health information created or received by a HIPAA Covered Entity that relates to the past, present or future physical or mental health of a patient, and the provision of health care to the patient or payment for the provision of health care to the patient.

III. POLICY

This policy is implemented in order to protect personal information that is created, received and maintained during its regular course of business. Additionally, this policy sets forth the county's policy and procedure for ensuring compliance with the security and privacy requirements imposed by HIPAA.

IV. RESPONSIBILITIES

Human Resource Management - The Department of Human Resource Management (HRM) has overall responsibility for assuring that all county departments are in compliance with Sections III-V of this policy related to privacy of personal information.

Internal Audit – The Department of Internal Audit, in coordination with the department of Information Systems Technology, has responsibility for investigating data breaches involving personal information and making recommendations to ensure such breaches do not re-occur.

Information Systems Technology (IST) – The Department of IST, in coordination with the department of Internal Audit, has responsibility for investigating data breaches involving personal information and making recommendations to ensure such breaches do not re-occur. IST, in coordination with Risk Management, Internal Audit and Police, as necessary, is responsible for maintaining an Incident Response Plan for responding to, containing and mitigating data breaches of electronic information.

Risk Management - The Department of Risk Management has overall responsibility for assuring that the county departments that are HIPAA Covered Entities or HIPAA Business Associates are in compliance with the sections of this policy related to HIPAA security and privacy requirements. The Department of Risk Management, in coordination with IST, is responsible for investigating data breaches involving personal information and Protected Health Information and making recommendations to ensure such breaches do not re-occur.

V. REQUIREMENTS APPLICABLE TO ALL DEPARTMENTS

It is the responsibility of Chesterfield County departments to develop privacy of information policies and procedures. Specific privacy policies and procedures must be developed at the department level because departments conduct their business operations using different methods based on the nature of their work. The department director shall take into account the most efficient and effective methods for ensuring the protection of personal information while promoting consistency in the management of personal information throughout the department.

HRM will be available to assist departments in developing departmental procedures. HRM shall provide training as needed for departmental staff assigned responsibility for drafting departmental policies and procedures related to privacy.

The policies and procedures shall address the following privacy requirements:

A. Training - The policies shall address training of all employees who are likely to have access to personal information. At a minimum, training shall be provided to all employees for newly developed privacy policies, to new employees during new employee department orientation, and to all employees whenever significant changes are made to privacy policies.

B. Safeguards - Policies shall address administrative, technical and physical safeguards that protect the privacy and security of personal information the county creates, receives, maintains or transmits from unauthorized use or inadvertent disclosure to persons other than the intended recipient. Measures taken will relate directly to the structure and activities of the department.

C. Processes and Systems – Policies shall require an evaluation of all processes and automated systems to ensure personal information that is requested of customers is done so in accordance with applicable federal and state law. This may include a review of third party contractor privacy practices. The County Attorney's office is available to assist departments with this evaluation.

D. Access – Policies shall limit or restrict access to personal information by employees and other requestors of information. If access to personal information is authorized, access shall be limited to the "minimum necessary" information required to fulfill a need or request.

Verification of the identity and authority of requestors for personal information shall be required prior to disclosure of the requested information.

E. Review and Correction of Personal Information - Policies will afford persons appropriate controls over their personal information maintained by the department. Such controls shall include the person's right to review, correct or amend their personal information.

F. Disposal of Personal Information - Policies shall address the proper disposal of non-record documents, as defined in Section II of this procedure that contain personal information. Disposal shall include shredding of non-record documents that include personal information.

VI. REQUIREMENTS FOR HIPAA COVERED ENTITY AND HIPAA BUSINESS ASSOCIATE DEPARTMENTS

A. HIPAA's requirements shall apply only to certain components of county operations that handle PHI. The County is a hybrid HIPAA Covered Entity. Some components of county government handle PHI while other components do not. The health care components to which HIPAA requirements shall apply are the Department of Mental Health Support Services (MHSS), the Department of Fire & EMS (Fire & EMS) and HRM, to the extent that it administers the county's self-insured health plan. Other departments are subject to HIPAA requirements only to the extent that such departments perform HIPAA covered functions or activities on behalf of Covered Entity departments. When departments perform HIPAA-covered functions or services on behalf of Covered Entity departments, such departments are considered under HIPAA to be "HIPAA Business Associates." Such departments include Accounting, IST, County Attorney, Human Resource Management, Internal Audit, Risk Management and Treasurer.

B. HIPAA Covered Entity Departments and HIPAA Business Associate Departments shall develop and implement policies and procedures to ensure appropriate staff, which have access to and handle PHI, receive training on the protection of PHI. The Departments shall be responsible for maintaining a training register to document appropriate staff have received training on the protection of PHI.

C. HIPAA Business Associates may disclose PHI to, and permit the use of PHI by, its employees, contractors, agents or other representatives only to the extent directly related to and necessary for the performance of its duties and obligations to Covered Entity departments. HIPAA Business Associates should use appropriate safeguards to prevent use or disclosure of PHI other than as necessary and request from Covered Entity departments no more than the minimum PHI necessary to perform its duties and obligations. HIPAA Business Associates will not use or disclose PHI in a manner inconsistent with HIPAA. HIPAA Business Associates shall ensure that any agent, including any subcontractor to whom it provides PHI, agrees to the same restrictions and conditions that are imposed under this policy for the protection of PHI.

D. HIPAA Business Associates shall notify Covered Entity departments as soon as practicable after becoming aware of an improper disclosure of PHI by HIPAA Business Associate or by a third party to which HIPAA Business Associate disclosed PHI. HIPAA Business Associates shall cooperate with Mental Health, Fire & EMS or HRM to implement procedures for mitigating the harmful effects from any improper use and/or disclosure of PHI. Upon notification by a HIPAA Business Associate of an improper disclosure of PHI, MHSS or Fire & EMS shall notify Risk Management.

E. HIPAA Business Associates may use PHI for the proper management and administration of its department or to carry out their legal responsibilities, including without limitation use and disclosure required to comply with applicable professional standards and obligations, and other requirements of law consistent with HIPAA.

F. HIPAA Covered Entity and HIPAA Business Associate Departments shall develop and implement policies that address the proper disposal of non-record documents, as defined in Section II of this

procedure, that contain PHI. Disposal shall include shredding of non-record documents that include personal information.

VII. HIPAA ADMINISTRATION

The County Administrator has appointed a HIPAA Advisory Board, which shall be responsible for initiating and overseeing the county's compliance with HIPAA. The county's Risk Management Director shall be the county's HIPAA Privacy Official, the contact person to receive complaints about HIPAA privacy violations and provide information about the county's HIPAA policies and procedures. The Risk Management Director or designee shall chair the HIPAA Advisory Board. IST's Data Security Administrator shall serve as the HIPAA Security Official and be a member of the HIPAA Advisory Board. The HIPAA Advisory Board shall be comprised of representatives from at least the following county departments: County Attorney, Fire & EMS, HRM, MHSS, Risk Management and IST. The HIPAA Advisory Board is responsible for the following:

A. Identification of county departments, employees and operations impacted by HIPAA

B. Coordination and oversight of HIPAA compliance efforts by impacted departments and employees, including but not limited to the following areas:

   1. Training of personnel as appropriate and necessary
   2. Imposing appropriate administrative, technical and physical safeguards to protect the privacy and security of PHI the County creates, receives, maintains or transmits
   3. Imposing appropriate measures to notify the public of their rights under HIPAA
   4. Establishing a process and or processes for individuals to make complaints concerning a county department's policies and procedures or its compliance with such policies and procedures
   5. Establishing a process for individuals to access and amend their PHI
   6. Establishing a process for individuals to have an accounting of their PHI disclosures
   7. Imposing progressive discipline for breach of HIPAA procedures
   8. Establishing mitigation processes if a breach of HIPAA protocol occurs

C. Determining the need for HIPAA Business Associate agreements or memoranda of understanding between county departments and between the county and third parties that ensure compliance with HIPAA privacy requirements.

VIII. HIPAA COMPLIANCE

All county departments determined by the HIPAA Advisory Board to have responsibilities under HIPAA shall cooperate and comply with all conditions imposed by Risk Management and the HIPAA Advisory Board.