

**Montgomery County, Maryland  
Office of the County Executive  
Office of Internal Audit**



**HIPAA Compliance - Phase 1 Risk Assessment**

**May 30, 2017**

# Highlights

## Why MCIA Did this Project?

In early 2016, the County identified the County's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as one of the high risk areas in a countywide risk assessment. Additionally, the County received an inquiry from the federal Office of Civil Rights regarding the County's HIPAA compliance program.

Montgomery County sought to assess current compliance with HIPAA regulations and to identify risks that the department(s) and the County should address to safeguard personal health information (PHI) and improve its HIPAA compliance level. CohnReznick was engaged by the Montgomery County Office of Internal Audit (MCIA) to conduct the initial phase of the work.

## What MCIA Recommends?

The County should finalize County-wide HIPAA Policies that are currently in draft form, and ensure that Procedures are comprehensively developed by the Departments that are Covered Components, where required. Additionally, the County should perform a comprehensive assessment of the status of Business Associate Agreements across all Covered Components to ensure that all Business Associates within the County are properly identified and have an agreement in place.

Additional audit review is necessary to more comprehensively assess HIPAA compliance, including:

1. Detailed Information Security and Controls Assessments for the systems in place which store and transmit data.
2. Business Continuity/Disaster Recovery Audits for all four County departments which are considered Covered Components.
3. Detailed HIPAA Compliance Audits within DHHS in order to comprehensively assess compliance with HIPAA requirements and whether the established controls are operating effectively.

## May 2017

### HIPAA Compliance - Phase 1 Risk Assessment

#### What MCIA Found

We conducted interviews with key stakeholders at each of the four departments to define risks specific to each area and/or process. Additionally, we met with the Deputy Privacy Official, who leads the County-wide HIPAA Workgroup, and with other stakeholders to better understand the current risks and potential areas of improvement to ensure full compliance with HIPAA. We gathered information related to the transmission and storage of PHI and electronic PHI (ePHI), and the management of Business Associates, including the maintenance of Business Associate Agreements.

County-wide HIPAA policies have not been finalized and formally accepted and, in aggregate, departmental procedures do not encompass all of the policies and procedures required to protect the privacy and security of PHI. There is no cohesive, organized set of policies and procedures to allow the County to assess whether they are in compliance with HIPAA requirements and currently, there is no process to review and assess the adequacy of policies and procedures on an annual basis.

Other specific risks identified:

- Within DHHS Child Welfare Services (CWS), emails are being sent password protected, but not encrypted. Passwords for documents are shared amongst many individuals within CWS and in the County.
- The County has not obtained third party reports such as Reports on Service Organization Controls (SOCs) for hosted systems which store or transmit PHI. These reports assess the design and operating effectiveness of internal controls over the applicable systems. They also indicate control considerations that are County responsibility.
- There is no county-wide effort to review in-place contracts to assess whether the changes to the definition of Business Associates in the implementation of the HIPAA Omnibus Rule in 2013 has impacted the list of County contractors, and whether there are existing contracts which require an updated agreement. The report also identifies areas that would benefit from additional, focused reviews.

# Table of Contents

Overview .....	4
Background .....	4
Objectives .....	7
Approach and Methodology .....	8
Data Collection:.....	8
Survey and Mapping of PHI/ePHI .....	9
Information Related to Business Associate Agreements .....	9
Identification of the Applicable Risk Universe .....	9
Observations and Recommendations .....	10
Policies and Procedures .....	10
Protection of PHI/ePHI .....	12
Business Associate Agreements.....	13
Recommended Additional Assessments.....	13
Department Comments and MCIA Evaluation .....	14
Appendix A – Departmental Risk Mapping .....	15
Appendix B – Policy Mapping .....	17
Appendix C – Department Response.....	21

## Overview

Montgomery County, Maryland (hereafter referred to as “Montgomery County” or “County”) sought to conduct a review of the County’s overall compliance with requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and to identify risks that the department(s) and the County should address to safeguard Private Health Information (PHI) and improve its HIPAA compliance level. This objective of the current effort was to obtain a baseline understanding of the scope and current status of HIPAA compliance. The results will be used to identify areas of improvement within the County’s HIPAA compliance program, and, as appropriate, areas where additional, subsequent focused and targeted assessments are needed to more specifically assess risks.

Montgomery County’s Chief Administrative Officer (CAO) is responsible for development and implementation of County policies and procedures for HIPAA, and for enforcement of these policies to ensure HIPAA compliance. The CAO has delegated these responsibilities to the County’s Privacy Official and Deputy Privacy Official. The Privacy Official (and Deputy) monitor the County’s compliance with HIPAA requirements to ensure that departments included in the health care component of the County comply with applicable HIPAA regulations and do not disclose protected health information (PHI) to non-authorized entities.

The County has designated the following departments performing covered functions as a health care component within the County:

- Health and Human Services
- Fire and Rescue Service
- Medicaid Transportation (part of Department of Transportation)
- Office of Human Resources (Benefits Section)

The County has identified itself as a hybrid entity, which means that some portions of the County will be considered part of the *covered component*, and other parts will not. In 2004, the County conducted an analysis to identify which departments and functions met the definition of a Covered Component or Internal Business Associate. The above noted departments are considered Covered Components of the Hybrid Entity. (Although Fire and Rescue Service was initially not considered a Covered Component, the department’s status changed when they began billing for services provided.) Internal Business Associates are those entities within the County that do not specifically create or maintain PHI/ePHI, but who may provide an internal support function, or may at times come in contact with PHI/ePHI.

The County requires these departments to comply with HIPAA regulations applicable to covered functions performed within the department; develop and maintain privacy policies, procedures, and practices for PHI applicable to the covered functions within the department; and enter into appropriate contracts with external Business Associates to protect the use and further disclosure of PHI by these entities. Each of these departments is also responsible for conducting a self-assessment of HIPAA compliance and reporting the results of this self-assessment to the County Deputy Privacy Official.

## Background

PHI, as defined under HIPAA, is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual. This is interpreted rather broadly

across the healthcare industry and includes any part of a patient's medical record or payment history. Individuals, for the purpose of the County HIPAA Risk Assessment, include

- Those who have received health or certain other services from the County's Department of Health and Human Services;
- Those who have received and been billed for emergency medical services from Fire and Rescue Service;
- Those who have received medical transportation services from the Department of Transportation; and
- Benefits eligible active and retired County employees, and Participating Agency employees as well as all eligible dependents that receive or have received healthcare coverage through the Office of Human Resources.

## HIPAA

The Health Insurance Portability and Accountability Act was enacted by Congress in 1996. Title I of HIPAA regulates the availability and breadth of group health plans and certain individual health insurance policies. Title II of HIPAA defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information, outlines numerous offenses relating to health care, and sets civil and criminal penalties for violations. It also creates several programs to control fraud and abuse within the health care system.

## Privacy Rule

The effective compliance date of the Privacy Rule was April 14, 2003. The HIPAA Privacy Rule regulates the use and disclosure of PHI held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions). By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "Business Associates".

## Security Rule

The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003, with a compliance date of April 21, 2005 for most covered entities. The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all PHI, whether paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (ePHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required implementation specifications must be adopted and administered by covered entities as dictated by the Rule:

1. Administrative Safeguards – policies and procedures designed to clearly show how the entity will comply with the act;
2. Physical Safeguards – controlling physical access to protect against inappropriate access to protected data; and
3. Technical Safeguards – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

For addressable implementation specifications, covered entities must perform an assessment to determine whether the specification is a reasonable and appropriate safeguard in the Covered Entity's environment.

### HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act<sup>1</sup> requires entities covered by HIPAA to report data breaches, which affect 500 or more persons, to the US Department of Health and Human Services (HHS), to the news media, and to the people affected by the data breaches. This subtitle extends the complete Privacy and Security Provisions of HIPAA to the Business Associates of covered entities. The Rule was published in the Federal Register on August 25, 2009 and took effect on November 30, 2009.

Another significant change of the HITECH Act was for the accounting of disclosures of a patient's health information. It extended the current accounting for disclosure requirements to information that is used to carry out treatment, payment and health care operations when an organization is using an Electronic Health Record (EHR).

### Omnibus Rule

In January 2013, HIPAA was updated via the Final Omnibus Rule, with an effective compliance date of March 26, 2013 for most components of the Rules' provisions. Included in the changes were updates to the Security Rule and Breach Notification portions of the HITECH Act. The greatest changes relate to the expansion of requirements to include Business Associates, whereas previously only covered entities had been required to comply with these sections of the law.

### County Roles and Responsibilities

The County Administrative Procedure (AP) 8-2<sup>2</sup> mandates the development of HIPAA Policies, and lays out the following responsibilities:

#### Privacy Official –

Ensures that County-wide HIPAA Policies and Procedures are developed and implemented.

#### Deputy Privacy Official –

- Participates in the activities of the Privacy Workgroup<sup>3</sup>;
- Develops HIPAA privacy policies and procedures for the department;
- As necessary, investigate complaints, known or suspected privacy violations, and known or suspected violations of privacy or security practices involving the covered entity departments;
- Respond to complaints or questions about the department's privacy or security policies and practices; and

---

<sup>1</sup> Enacted as part of the American Recovery and Reinvestment Act of 2009, which was signed into law on February 17, 2009,

<sup>2</sup> Issued January 9, 2007.

<sup>3</sup> Defined in the AP as "The ongoing committee that is: chaired by the Privacy Official; composed on the Deputy Privacy Official and Privacy Contacts from each of the health care component departments; and responsible for assisting with developing, implementing, and monitoring compliance with HIPAA policies and procedures."

- Provides internal business associates with HIPAA-compliant privacy policies and procedures, as appropriate.

#### Director of a Covered Entity Department –

- Develop and implement written policies and procedures that
  - state how PHI will be used;
  - state the conditions under which PHI will be disclosed;
  - limit the department's use and disclosure of PHI to the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure;
  - limit the department's requests for PHI to the minimum amount of PHI necessary to accomplish the purpose of the request;
  - limit the access of workforce members to PHI to only those who must have access to accomplish the department's work by specifying:
    - the members of the workforce or classes of workers who need access to PHI to perform their job duties;
    - the categories of PHI to which each worker or class of worker needs access in order to perform their job duties;
    - the conditions under which each worker or class of worker will be given access to PHI; and
  - state how the identity and authority of individuals who request PHI will be verified.
- Establish a process to:
  - identify and document designated record sets of PHI that are held by the department or by business associates, as required under HIPAA;
  - ensure that appropriate individuals receive a copy of the department's notice of privacy practices;
  - allow individuals to ask questions or file complaints about the department's:
    - policies and procedures on the use or disclosure of PHI; or
    - compliance with its policies and procedures on the use or disclosure of PHI;
  - receive and respond to questions and complaints on the department's use or disclosure of PHI;
  - allow individuals to ask questions about their PHI and receive answers;
  - allow individuals to request access to PHI and to either allow or deny access;
  - allow individuals to request an amendment to their PHI in appropriate circumstances and to grant or deny the amendment;
- Develop and implement appropriate administrative, technical, and physical safeguards to protect PHI against intentional and unintentional disclosure in violation of regulations.

Additionally, the County Attorney's office provides guidance to the Privacy Official, Deputy Privacy Official and the HIPAA Workgroup regarding legal opinions of HIPAA regulations.

## Objectives

The overall goal of this Phase 1 assessment was to obtain a baseline understanding of the scope and current status of HIPAA compliance in the County. Specific objectives included the following: develop an initial Risk Assessment of HIPAA compliance program areas that represent high risk to the County, determine where more detailed inquiries and procedures are needed to fully assess risk levels, and develop a preliminary mapping of where Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) reside.

The results of the assessment will be used to identify areas of improvement within the County's HIPAA compliance program, and, as appropriate, areas where additional, subsequent focused and targeted assessments are needed to more specifically assess risks.

## Approach and Methodology

To accomplish the HIPAA Risk Assessment objective, CohnReznick conducted interviews with key stakeholders at each of the four departments to further define risks specific to each area and/or process. Additionally, we met with the Deputy Privacy Official, who leads the County-wide HIPAA Workgroup, and with other stakeholders to better understand the risks and current state of compliance with HIPAA. We gathered information related to the transmission and storage of PHI and ePHI, and the management of Business Associates, including the maintenance of Business Associate Agreements.

### Data Collection:

#### Review of Background Information

We reviewed certain documents provided by the Deputy Privacy Official and others, in order to identify the current status of HIPAA compliance, including the following:

- A number of Business Associate Agreement (BAA) guidance documents;
- County-wide Business Associate Agreement last updated in October 2014;
- Prior reports developed by external consultants assessing HIPAA requirements and compliance as of 2004 and 2007;
- Existing and draft policies and procedures related to HIPAA; and
- Various authorization and records management documentation from the respective departments.

#### Interviews with those responsible for compliance with HIPAA regulations

We conducted a series of information-gathering interviews with key stakeholders responsible for HIPAA compliance in the above noted departments, as well as certain Internal Business Associates, including the following:

- Department of Health and Human Services (DHHS)
  - Child Welfare Services, Kinship Supervisor
  - Behavioral Health and Crisis Services, Deputy Chief
  - Public Health Services, Administrator, HIV/STD Services
  - Special Needs Housing, Homeless Services Administrator
  - Chief Information Officer and Enterprise Service Area Representative
- Department of Fire and Rescue Service, Battalion Chief, EMS Section
- Department of Transportation, Medicaid Transportation Program, Chief and Program Manager
- Office of Human Resources (OHR), Benefits Section, Chief
- Office of the County Attorney, Assistant County Attorney
- Office of the County Executive, Assistant Chief Administrative Officer
- Department of Finance, Contracts and Special Projects Manager
- Department of Technology Services, Enterprise Information Security Official
- CountyStat Manager



## Survey and Mapping of PHI/ePHI

Based on the interviews with the above noted participants, CohnReznick developed process flows for each department which identify receipt of PHI/ePHI into the department, physical location of PHI/ePHI, applications or databases where ePHI reside and potential transmission points for PHI and ePHI.

We also sent questionnaires to the key stakeholders to further identify vendors, physical server locations, system access, reporting to external parties and other relevant information about the applications and databases in use in the selected County departments.

## Information Related to Business Associate Agreements

When we met with those responsible for managing external Business Associates, we inquired of the status of BAAs. Most of the key stakeholders noted that they rely upon the County Attorney's office to ensure that BAAs are current. We met with the Deputy Privacy Official and Assistant County Attorney to gain an understanding of the current state of BAAs and the universe of Business Associates.

## Identification of the Applicable Risk Universe

The table below identifies potential risks related to the County's compliance with HIPAA organized in six risk areas. The detailed risks were used to guide our interviews, inquiries and assessments. Appendix A, *Departmental Risk Mapping*, presents an overall assessment of the status of compliance within the four departments for each of the risk areas.

Risk Area	Detail of Risk
Policies and Procedures	<ul style="list-style-type: none"> <li>• County-wide HIPAA policies and procedures may not be in place, or be updated to include requirements of HIPAA regulations issued subsequent to January 2007</li> <li>• Comprehensive and up-to-date departmental HIPAA procedures may not be in place; current procedures have not been updated to include requirements of HIPAA regulations issued subsequent to January 2007</li> <li>• Policies and procedures may not be communicated to all staff in the respective department who are responsible for compliance</li> </ul>
Protection of PHI/ePHI	<ul style="list-style-type: none"> <li>• PHI/ePHI may not be adequately protected when resting in place (stored)</li> <li>• PHI/ePHI may not be adequately protected during transmission</li> <li>• PHI/ePHI may not be adequately disposed of when it is no longer required to be maintained</li> <li>• Access to PHI/ePHI may not be appropriately limited and controlled</li> </ul>
Training	<ul style="list-style-type: none"> <li>• Employees with responsibility over PHI/ePHI may not be adequately trained or receive periodic security awareness training covering their responsibilities over the protection of PHI/ePHI</li> </ul>
Business Associates	<ul style="list-style-type: none"> <li>• Business Associate Agreements may not be in place with all applicable current contracts</li> <li>• Internal Business Associates may not be properly identified and adequate agreements/policies/procedures may not be in place</li> <li>• External Business Associates may not have adequate oversight &amp; safeguards in place to protect PHI/ePHI</li> </ul>

Risk Area	Detail of Risk
Business Continuity/ Disaster Recovery	<ul style="list-style-type: none"> <li>• Plans may not be in place in the case of an emergency or other occurrence which could damage systems containing PHI/ePHI</li> <li>• ePHI may not be restored after an emergency</li> <li>• PHI/ePHI may not be adequately protected when the organization is operating in emergency mode</li> </ul>
Breach Identification and Reporting	<ul style="list-style-type: none"> <li>• Security incidents may not be detected, identified or reported</li> <li>• Departments may not have adequate oversight and processes in place to identify, investigate and implement safeguards to prevent breaches.</li> <li>• Business Associates may not have adequate oversight and processes in place to identify, investigate and implement safeguards to prevent breaches.</li> <li>• Appropriate notification of confirmed breaches to the Secretary, individuals and the media may not occur</li> </ul>

## Observations and Recommendations

We did not perform detailed testing in this phase, but relied on the information communicated to us in interviews and our review of the documents provided to develop a preliminary assessment of risk and compliance. We have provided below key observations and recommendations based on our assessment. Our recommendations address three significant risk areas: Policies and Procedures; Protection of PHI/ePHI; and Business Associates Agreements. In addition, we have identified high risk areas where additional reviews are required to more fully assess risk and compliance with HIPAA requirements.

### Policies and Procedures

As noted in the introduction section of this report, the expectation is that the Deputy Privacy Official and the HIPAA Workgroup will establish policies over HIPAA, and that the Departments (advised by members of the HIPAA Workgroup) will develop and implement the procedures and processes to ensure compliance. The County Attorney's Office provides guidance to the Deputy Privacy Official and HIPAA Workgroup regarding legal opinions on HIPAA regulations and their application to County policies. Appendix B, *Policy Mapping*, provides a list of HIPAA-required Policies and Procedures, maps the requirements to existing policies/procedures and identifies gaps where policies/procedures were not provided.

1. Administrative Procedure 8-2. The current, formally approved County-wide Administrative Procedure 8-2, HIPAA Compliance and Responsibilities, is dated 2007. There are significant differences in how the County Roles and Responsibilities currently operate from how they are described in AP 8-2. The current, formally approved Administrative Procedure 6-7, Information Resources Security (which addresses certain required security requirements, as outlined in the 2003 Security Rule regulation), is dated 2005. Changes in HIPAA regulations in 2009 and 2013 require certain updates to policies, including updating Notices of Privacy Practice, Business Associate Agreements, Breach Notifications and Accountings of Disclosures, among other requirements; such changes have not been reflected in any amendment of the current AP 8-2. Similarly, we reviewed updated draft versions (most recent draft dated May, 2015) of HIPAA Administrative Manual (HIPAA Policies and Procedures) and noted that the policies have not been

finalized and formally accepted. We did note that certain departmental policies and procedures had been updated more recently. Specifically, DHHS has various updates from 2010 to 2014; OHR HIPAA Policies are updated through 2014; and certain policies related to HIPAA in the Department of Fire and Rescue policies were updated in 2016.

We also noted a request from the Deputy Privacy Official to the County Attorney's office dating back to May 2015 requesting clarification of roles of Business Associates, which was lacking response as of December 2016.

Based on our observations, we identified the following obstacles to completing and finalizing policies and procedures:

- Lack of resources e.g., (having a part-time Deputy Privacy Official; not bringing in temporary resources to periodically update the County policies/procedures based on changes in federal HIPAA law/regulations);
- Lack of prioritization and/or resources by departments to complete procedures;
- Lack of guidance from County Attorney's office regarding internal business associates, impacting the Workgroup's ability to define responsibilities;
- Possible lack of training or knowledge at the departmental level to develop the required procedures.

Recommendation:

We recommend that the completion and approval of the updated HIPAA Policies be given the highest priority by the Deputy Privacy Official and the Privacy Official, and that departments revise, develop or update department-specific procedures as soon as County-wide policies are formally updated. This will require that the County Attorney's office provide timely guidance to the Deputy Privacy Official and the HIPAA Workgroup for any and all areas which require clarification to finalize the Policies. Additionally, the Department of Technical Services should review and update the Information Resources Security (AP 6-7) to ensure that it addresses all HIPAA required Security Polices. [NOTE: As noted above, resource limitations may be one factor affecting the current absence of updated and comprehensive County policies/procedures. It is strongly suggested that the County consider options to address this situation, including the potential use of contracted HIPAA expertise to ensure that the required HIPAA policies/procedures are developed and finalized.]

2. Sanctions Policy. Based on our review of policy documents provided, we determined there is not a formally accepted county-wide sanctions policy as required by HIPAA Security Rule 164.308(a)(1)(ii)(c).

Recommendation:

Subsequent to the updating and approval of county-wide HIPAA Policies, required sanctions policies should be developed and formally approved.

3. Periodic Review of Policies/Procedures. Best practice is that policies are reviewed at least annually and updated as needed to reflect changes in the business environment, organizational structure, and emerging legal and regulatory requirements. The County has recently implemented policy management software which may help establish a routine review process and mitigate the risks associated with outdated policies and procedures.

Recommendation:

The County should institute an annual review requirement for both County-level policies/procedures, as well as department-level procedures to ensure that policies and procedures are timely updated to reflect current HIPAA requirements.

## Protection of PHI/ePHI

We noted that there are at least five major systems currently in use within the county which store or transmit PHI/ePHI:

- CHESSIE (used by Health and Human Services Child Welfare Services, but maintained by the State of Maryland);
  - eMEDS (used by Fire and Rescue, but maintained by the State of Maryland);
  - HMIS (used by Health and Human Services Special Needs Housing, hosted by the vendor, Medaware);
  - Oracle (used by the Office of Human Resources, and maintained on a server at the Department of Technology Services); and
  - NextGen (used by Health and Human Services Behavioral Health and Crisis Services and Public Health Services, maintained on a server at the Department of Technology Services).
4. Based on our discussions, it does not appear that County has obtained a third-party attestation report such as Reports on Service Organization Controls (SOC) No.1 or No.2 for the hosted systems. A SOC No.1 report (replacing the older SAS 70 reports) provides a report on the system of internal control for purposes of complying with internal control over financial reporting. A SOC No.2 report addresses controls at a service organization relevant to security, availability, processing integrity, confidentiality, and/or privacy. Complementary User Control Considerations included in the SOC report provide limitations of the system related to security and privacy and help the user (the County or departments using certain hosted systems) understand the limitations for protection of data within these systems.

Recommendation:

Best practices indicate that third party attestation reports (such as SOC No.2) should be obtained annually for hosted systems that support operations and procedures relevant to storing, transmitting, processing and securing PHI/ePHI. The reports should be reviewed by knowledgeable County personnel to assess if the third-party provider has required controls in place and if they are operating effectively. The County should also assess if it has controls in place to sufficiently address the Complimentary User Control Considerations identified in the reports.

5. Within DHHS Child Welfare Services (CWS), emails are being sent password protected, but not encrypted. Passwords for documents are shared amongst many individuals within CWS and in the County. While we recognize that there are technological challenges associated with sharing documents via the County encryption program, CWS should identify other encryption tools or technologies to satisfy the requirements of 164.312(a)(2)(iv).

Recommendation:

The County should ensure that all documents containing PHI/ePHI which are transmitted via email are sent with encryption.

## Business Associate Agreements

A business associate (BA), with respect to a Covered Entity, is defined as an organization or person who:

- (i) On behalf of such Covered Entity or of an organized health care arrangement in which the Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and re-pricing; or
- (ii) Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of protected health information from such Covered Entity or arrangement, or from another business associate of such Covered Entity or arrangement, to the person.

The HIPAA Omnibus Rule of 2013 updated the definitions of BAs, and in many cases across the healthcare industry, expanded the definition of a BA to include vendors that had previously not been considered a BA. The Omnibus Rule required that Covered Entities have Business Associate Agreements (BAAs) in place for all current (at the time) BAs by September 26, 2014, and for all newly entered contracts with BAs by September 26, 2013.

Contracts are updated by the Procurement Department, with guidance on legal matters from the County Attorney's office. The County Attorney's office provided an updated BAA in October 2014 for use as contracts were updated or put in place. The Deputy Privacy Official is responsible to ensure that an assessment was conducted to ensure that BAAs are in place where required.

6. There has been no County-wide effort to review in-place contracts to assess whether the implementation of the HIPAA Omnibus Rule in 2013 impacted the County's list of Business Associates, and whether there are existing contracts which require an updated agreement. Most County contracts are maintained on a three plus one-year basis, and contracts in effect in 2013 are expected to be updated/renewed by the end of 2016. The updated BAA was implemented in October 2014, where necessary, for all renewed or new contracts. For this reason, *it is believed* that the majority of BAA's are current. However, without appropriate controls in place to ensure that appropriate BAA's are in place and functioning, the risk is increased that vendors and other Business Associates are not in compliance with HIPAA.

### Recommendation:

We recommend that the County perform a comprehensive assessment of the status of BAA's across all Covered Entities of Montgomery County.

## Recommended Additional Assessments

The goal of Phase 1 was to conduct an initial Risk Assessment of HIPAA compliance program areas, identify Departments and areas that represent high risk to the County, determine where more detailed

inquiries and procedures are needed to fully assess risk levels and develop a preliminary mapping of where Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) reside.

Based on the results of our work in Phase 1, we recommend additional procedures (in order of priority) in the following areas:

7. In order to ensure that the County departments which store and transmit PHI are in fact following established security procedures, we recommend that the County perform detailed Information Security and Controls Assessments for the systems in place which store and transmit data, with a focus on HIPAA and other protected information. We recommend that priority be given to the systems in place in the Department of Health and Human Services.
8. The County is required to develop and maintain policies and procedures for a Contingency Plan as required by 164.308a7i. This requirement was covered under the Administrative Procedure 6-7, Information Resources Security (dated May 4, 2005). We recommend that the County perform Business Continuity/Disaster Recovery Audits for all four County departments which are considered Covered Components.
9. The scope of this audit was broadly defined to address the four Covered Components (Departments) at the County, and, as such, we were only able to review documents and procedures at a high-level. Based on our review, we determined that the highest risks exist at the Department of Health and Human Services, specifically in the departments noted below. We recommend a detailed HIPAA Compliance Audit focused on HHS in order to comprehensively assess compliance with HIPAA requirements and whether the established controls are operating effectively for the following areas of HHS:
  - Child Welfare Services
  - Behavioral Health and Crisis Services
  - Public Health Services
  - Special Needs Housing

## Department Comments and MCIA Evaluation

MCIA provided a draft of this report to the Montgomery County (Deputy) Privacy Official for review and comment. There are nine (9) recommendations contained in the report. The Deputy Privacy Official concurred with the first eight recommendations. With respect to the ninth recommendation (that a detailed HIPAA Compliance Audit focused on HHS be conducted in order to comprehensively assess compliance with HIPAA requirements and whether the established controls are operating effectively), the Deputy Privacy Official stated that such an assessment should be conducted after the HHS Process and Technology Modernization Project has been implemented, and as part of a broader HIPAA compliance assessment within the County. The Internal Audit Manager has reviewed these comments and does not believe any change to the report findings and recommendations is warranted. With respect to the more detailed assessments of areas identified under Recommendation #9, the County will need to determine the appropriate timing for conducting such assessments based on implementation of the modernization program within HHS. A copy of the Privacy Officer's memorandum appears as Appendix C.

## Appendix A - Departmental Risk Mapping

Risk Area	Detail of Risk	DHHS	OHR	Fire and Rescue	DOT MTU	
Policies and Procedures	Required HIPAA policies and procedures may not be in place	County-wide HIPAA policies have not been finalized and formally accepted and, in aggregate, departmental procedures do not encompass all of the policies and procedures required to protect the privacy and security of PHI. There is no cohesive, organized set of policies and procedures to allow the County to assess whether they are in compliance with HIPAA requirements and currently, there is no process to review and assess the adequacy of policies and procedures on an annual basis.				
	HIPAA policies and procedures may not be updated to include new regulations	There is no formal county-wide sanctions policy as required by HIPAA Security Rule 164.308(a)(1)(ii)(c).				
Protection of PHI/ePHI	PHI/ePHI may not be adequately protected when resting in place (stored)	Systems used by the various HHS departments which store PHI appear to have appropriate protections in place to protect ePHI. However, the limited scope of this audit did not allow us to perform a detailed test of controls.	OHR utilizes Oracle for benefits management. Protections over ePHI appear to be adequate. OHR maintains confidentiality over hard copy containing PHI through access controls in "HIPAA hall"	Laptops are encrypted, and data is submitted and removed from devices.	Databases are maintained on a segregated network maintained by DTS	
	PHI/ePHI may not be adequately protected during transmission	Within CWS, emails are being sent password protected, but not encrypted. Passwords for documents are shared amongst many individuals within CWS and in the County. This does not satisfy the requirements of 164.312(e)(2)(iv)	We were not able to comprehensively assess during Phase I and recommend further testing to ensure security controls are functioning as planned.	Based on discussions with Fire and Rescue Management, all PHI is encrypted both on a laptop and during transmission	Electronic transmission is limited, as most information is collected by paper or telephonically	
	PHI/ePHI may not be adequately disposed of when it is no longer required to be maintained	In large part, many departments send documents to the County Record Center when no longer needed at the departmental level. Review of the County Record Center was not included in the scope of this audit.				
	Access to PHI/ePHI may not be adequately limited	We were not able to comprehensively assess during Phase I and recommend further testing to ensure security controls are functioning as planned.	Access to PHI/ePHI appears to be adequately limited and segregated.	Access to PHI/ePHI appears to be adequately limited and segregated.	Access to PHI/ePHI appears to be adequately limited and segregated.	

Risk Area	Detail of Risk	DHHS	OHR	Fire and Rescue	DOT MTU
Training	Employees with responsibility over PHI/ePHI may not be adequately trained or receive periodic security awareness training covering their responsibilities over the protection of PHI/ePHI	Employees receive county-wide security training and additional HHS-specific HIPAA training	Employees receive county-wide security training, and benefit/HR-specific training (from HR consultant)	Employees receive county-wide security training	Employees receive county-wide security training
Business Associates	Internal Business Associates may not be properly identified and adequate agreements/ policies/procedures may not be in place	We were told that there is no current County-wide agreement on the definition of an Internal Business Associate.			
	Third parties may not have adequate oversight & safeguards in place to protect PHI/ePHI	Within HHS, most contracts are renewed on a 3-5 year cycle, and new contracts have included the updated BAA. HHS maintains an inventory of contracts with BAA's	OHR is currently undergoing an effort to renew/review contracts and assess whether there is an updated BAA in place where required.	Fire and Rescue does not maintain a list of BAAs. However, all vendors that handle PHI for MCFRS have contracts that have been signed within last five years and those include BAAs.	DOT MTU does not maintain a list of BAAs
Business Continuity/ Disaster Recovery	Plans may not be in place in the case of an emergency or other occurrence which damages systems containing PHI/ePHI	We were told that there has been no county-wide effort to identify whether there may be existing contracts which require, but do not have, an updated BAA.			
	ePHI may not be restored after an emergency	Although Business Continuity / Disaster Recovery is addressed in County-wide policies, these policies are outdated. We recommend a Disaster Recovery / Business Continuity Assessment be performed for all Covered Components of Montgomery County			
	PHI/ePHI may not be adequately protected when the organization is operating in emergency mode	Electronic incidents are monitored by the Department of Technical Services. Vulnerability assessments are performed weekly and reported to departments. DTS has a planned, comprehensive Risk Assessment over all systems. However, the authority of DTS within the county is decentralized and DTS staff is limited, which may increase risks that vulnerabilities and risks may not be appropriately identified and followed up on.			
Breach Identification and Reporting	Security incidents may not be detected, identified or reported	There is no county-wide Memorandum of Agreement with the union regarding what to do in the event that a HIPAA violation involves them			
	Departments may not have adequate oversight and processes in place to identify, investigate and implement safeguards to prevent breaches.	There are concerns over whether the former Fire and Rescue software vendor has appropriate controls in place over the protection and destruction of data that they still maintain.			
	Business Associates may not have adequate oversight and processes in place to identify, investigate and implement safeguards to prevent breaches.	We were unable to determine this within the scope of this phase of work.	We were unable to determine this within the scope of this phase of work.	We were unable to determine this within the scope of this phase of work.	We were unable to determine this within the scope of this phase of work.
	Appropriate notification of confirmed breaches to the Secretary, individuals and the media may not occur	We were unable to determine this within the scope of this phase of work.	We were unable to determine this within the scope of this phase of work.	We were unable to determine this within the scope of this phase of work.	We were unable to determine this within the scope of this phase of work.



## Appendix B – Policy Mapping

The tables below document policies and procedures required by the various HIPAA regulations and provide a preliminary mapping to County policies provided during our fieldwork. Other policies may exist but were not provided. Development of policies and procedures should include completion of mapping to requirements to ensure all required areas are addressed either as discrete policies or procedures or within other County documents.

### Privacy Policies:

According to HIPAA Privacy Policy §164.530(i)(1) Standard: Policies and procedures, a covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance.

We reviewed existing County Privacy policies and procedures provided to us by the Deputy Privacy Officer as well as policies provided by Departments. Some Departments have developed updated policies and processes, however the existing County-wide policies have not been formally updated. The table below describes the overall Privacy Policies required by regulation and the current County-wide policies which address the requirements. A prior report, prepared in 2005 by an external consultant, Fox, provides detail on specific policies required. These should be implemented with consideration for any recent regulatory updates.

<b>Requirement</b>	<b>County Policy which addresses requirement</b>
Uses and Disclosures of Protected Health Information	AP 8-2 (2007), HHS Uses and Disclosure Policies and OHR Uses and Disclosure Policies
Notice of Privacy Practices for PHI	AP 8-2 (2007), HHS Notices of Privacy Practices and OHR Notices of Privacy Practices
Patient/Participant's Rights Policies (including Inspection, Amendments, Restrictions, Accounting of Disclosures, etc.)	AP 8-2 (2007), and OHR Participant's Rights
Business Associate Agreements	No specific policy regarding Business Associates, incorporated into AP 8-2, and departmental policies and procedures. Updated County-wide agreement as of October 2014.

### Security Policies:

<b>Security Standards Matrix (Appendix A of the Security Rule)</b>			
<b>ADMINISTRATIVE SAFEGUARDS</b>			
<b>Standards</b>	<b>Sections</b>	<b>Implementation Specifications (R)= Required, (A)=Addressable</b>	<b>County Policy which addresses requirement</b>
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R) AP 6-7 (2005) 4.13
		Risk Management	(R) AP 6-7 (2005) 4.13

<b>Security Standards Matrix (Appendix A of the Security Rule)</b>				
<b>ADMINISTRATIVE SAFEGUARDS</b>				
		Sanction Policy	(R)	AP 6-7 (2005) 3.6 and proposed Sanctions Policy
		Information System Activity Review	(R)	AP 6-7 (2005) 4.13
Assigned Security Responsibility	§ 164.308(a)(2)			AP 6-7 (2005)
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)	AP 6-7 (2005)
		Workforce Clearance Procedure	(A)	Not noted or not provided
		Termination Procedures	(A)	AP 6-7 (2005) 4.4
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)	Not noted or not provided
		Access Authorization	(A)	AP 6-7 (2005) 4.16
		Access Establishment and Modification	(A)	AP 6-7 (2005) 4.8
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)	Not noted or not provided
		Protection from Malicious Software	(A)	AP 6-7 (2005) 4.8
		Log-in Monitoring	(A)	AP 6-7 (2005) 4.9
		Password Management	(A)	AP 6-7 (2005) 4.4
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)	Not noted or not provided
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)	Not noted or not provided
		Disaster Recovery Plan	(R)	Not noted or not provided
		Emergency Mode Operation Plan	(R)	Not noted or not provided
		Testing and Revision Procedures	(A)	Not noted or not provided
		Applications and Data Criticality Analysis	(A)	Not noted or not provided
Evaluation	§ 164.308(a)(8)	Written Contract or Other Arrangement	(R)	Not noted or not provided
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)	Not noted or not provided

<b>PHYSICAL SAFEGUARDS</b>				
<b>Standards</b>	<b>Sections</b>	<b>Implementation Specifications (R)= Required, (A)=Addressable</b>		<b>County Policy which addresses requirement</b>
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)	Not noted or not provided
		Facility Security Plan	(A)	Not noted or not provided
		Access Control and Validation Procedures	(A)	Not noted or not provided
		Maintenance Records	(A)	Not noted or not provided
Workstation Use	§ 164.310(b)			AP 6-7 (2005) 4.5
Workstation Security	§ 164.310(c)	Disposal	(R)	AP 6-7 (2005) 4.5
Device and Media Controls	§ 164.310(d)(1)	Media Re-use	(R)	Not noted or not provided
		Accountability	(A)	Not noted or not provided
		Data Backup and Storage	(A)	Not noted or not provided
		Data Backup and Storage	(A)	Not noted or not provided


<b>TECHNICAL SAFEGUARDS</b>				
<b>Standards</b>	<b>Sections</b>	<b>Implementation Specifications (R)= Required, (A)=Addressable</b>		<b>County Policy which addresses requirement</b>
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)	AP 6-7 (2005) 4.4
		Emergency Access Procedure	(R)	Not noted or not provided
		Automatic Logoff	(A)	AP 6-7 (2005) 4.5
		Encryption and Decryption	(A)	Not noted or not provided
Audit Controls	§ 164.312(b)			Not noted or not provided
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)	Not noted or not provided
Person or Entity Authentication	§ 164.312(d)			AP 6-7 (2005)
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)	Not noted or not provided
		Encryption	(A)	Not noted or not provided

<b>ORGANIZATIONAL REQUIREMENTS</b>				
<b>Standards</b>	<b>Sections</b>	<b>Implementation Specifications (R)= Required, (A)=Addressable</b>		<b>County Policy which addresses requirement</b>
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	<b>(R)</b>	Not noted or not provided
		Other Arrangements	<b>(R)</b>	Not noted or not provided
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	<b>(R)</b>	OHR HIPAA Policies and Procedures

## Appendix C – Department Response



To: William Broglie, Internal Audit Manager  
Office of Internal Audit

From: Joy Page   
Deputy Privacy Official

Subject: County HIPAA Audit

I have reviewed the *Montgomery County HIPAA Compliance – Phase 1 Risk Assessment* audit report completed by Cohn Resznick.

---

### Observations and Recommendations

#### Recommendation:

1. We recommend that the completion and approval of the updated HIPAA Policies be given the highest priority by the Deputy Privacy Official and the Privacy Official, and that departments revise, develop or update department-specific procedures as soon as County-wide policies are formally updated.
  - 1a. This will require that the County Attorney's office provide timely guidance to the Deputy Privacy Official and the HIPAA Workgroup for any and all areas which require clarification to finalize the Policies.
2. Additionally, the Department of Technical Services should review and update the Information Resources Security (AP 6-7) to ensure that it addresses all HIPAA required Security Policies.
3. County should consider use of contracted HIPAA expertise to ensure the required HIPAA policies and procedures are implemented.

#### County Privacy Response:

The County Deputy Privacy Official agrees with all of the above recommendations. The Workgroup is moving towards those goals. The County Deputy Privacy Official and the assigned

---

General Counsel from the Office of the County Attorney have established a process for developing and approving Countywide policies and procedures using policy briefs. Additionally, the Aruvio software has been further developed to incorporate policy briefs and Incident response. It should be noted that the HIPAA General Counsel works part time. The Department of Technical Services is currently updating all of its Security policies. The Chief Security Official and the Deputy Privacy Official meet bi-weekly to address the privacy and HIPAA crosswalk to security requirements. There is a great deal of research and drafting that goes into policy development. The County Privacy Workgroup is under resourced and in need of additional assistance.

**Recommendation:**

1. We recommend that the required sanctions policies should be developed and formally approved.

**County Privacy Response:**

The County Deputy Privacy Official agrees with the above recommendation. A Sanctions Policy was developed and submitted for approval in 2015. We are happy to review the policy to move it towards review and approval.

**Recommendation:**

1. The County should institute an annual review requirement for both County level policies and procedures, as well as department level procedures to ensure that policies and procedures are timely updated to reflect current HIPAA requirements.

**County Privacy Response:**

The County Deputy Privacy Official agrees with the above recommendation. The Aruvio policy management settings will be set to reflect the recommended standard.

---

**Recommendation:**

1. Best practices indicate that third party attestation reports (such as SOC No.2) should be obtained annually for hosted systems that support operations and procedures relevant to storing, transmitting, processing and securing PHI/ePHI. The reports should be reviewed by knowledgeable County personnel to assess if the third-party provider has required controls in place and if they are operating effectively. The County should also assess if it has controls in place to sufficiently address the Complimentary User Control Considerations identified in the reports.

**County Privacy Response:**

The County Deputy Privacy Official agrees with the above recommendation. The recommendation will be forwarded to the County Security Official to be developed.

---

Within DHHS Child Welfare Services (CWS), emails are being sent password protected, but not encrypted. Passwords for documents are shared amongst many individuals within CWS and in the County. While we recognize that there are technological challenges associated with sharing documents via the County encryption program, CWS should identify other encryption tools or technologies to satisfy the requirements of 164.312(a)(2)(iv).

**Recommendation:**

1. The County should ensure that all documents containing PHI/ePHI which are transmitted via email are sent with encryption.

**County Privacy Response:**

The suggested recommendation is subject to an external barrier. The Child Welfare program within the Department of Health and Human Services is a State of Maryland program that is locally administered and uses the state Department of Human Resources system. All of Montgomery County has been upgraded to Office365 G3 licenses that have built in encryption. There is a conflict between the CWS uses of 365 and the State system. The County is working with DHR as it is currently building a new system that will upgrade its technology. Montgomery County DHHS is an

integral partner in the planning of that system update. The encryption issue will be presented at the appropriate time.

**Recommendation:**

1. We recommend that the County perform a comprehensive assessment of the status of BAA's across all Covered Entities of Montgomery County.

**County Privacy Response:**

The County Deputy Privacy Official agrees with the above recommendation.

**Additional Recommendation:**

1. We recommend that the County perform detailed Information Security and Controls Assessments for the systems in place which store and transmit data, with a focus on HIPAA and other protected information. We recommend that priority be given to the systems in place in the Department of Health and Human Services.

**County Privacy Response:**

The County Deputy Privacy Official concurs with the above recommendation. DTS is currently updating all of the Security Policies and Procedures for the County. This assessment would be the appropriate next step once the policies have been implemented and tested.



2. County is required to develop and maintain policies and procedures for a Contingency Plan as required by 164.308a7i. This requirement was covered under the Administrative Procedure 6-7, Information Resources Security (dated May 4, 2005). We recommend that the County perform Business Continuity/Disaster Recovery Audits for all four County departments which are considered Covered Components.

**County Privacy Response:**

The County Deputy Privacy Official agrees with the above recommendation.

3. The scope of this audit was broadly defined to address the four Covered Components (Departments) at the County, and, as such, we were only able to review documents and procedures at a high-level. Based on our review, we determined that the highest risks exist at the Department of Health and Human Services, specifically in the departments noted below. We recommend a detailed HIPAA Compliance Audit focused on HHS in order to comprehensively assess compliance with HIPAA requirements and whether the established controls are operating effectively for the following areas of HHS:

- Child Welfare Services
- Behavioral Health and Crisis Services
- Public Health Services
- Special Needs Housing

**County Privacy Response:**

The County Deputy Privacy Official disagrees with the above recommendation. The County allocated several million dollars for a Process and Technology Modernization Project at the Department of Health and Human Services. All of the systems have been implemented but the project is not yet complete. It will take some time to finalize implementation. HIPAA compliance was at the forefront of the PTM project. At some time in the future, it will fully be appropriate to assess the efficiency and effectiveness of those controls as part of a larger compliance assessment for the County.

# # #