

Miami-Dade County Public Schools Office of Management and Compliance Audits



AUDIT OF ESE & RISK BENEFITS (IDEA & HIPAA) COMPLIANCE



Some safeguards for protecting personally identifiable information and protected health information, as well as policies for complying with HIPAA privacy rules and IDEA confidentiality requirements are in place. However, additional safeguards are needed to remove identified areas of exposure and to more fully comply with the cited rules and requirements.

March 2017

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA

Dr. Lawrence S. Feldman, Chair
Dr. Marta Pérez, Vice Chair
Dr. Dorothy Bendross-Mindingall
Ms. Susie V. Castillo
Dr. Steve Gallon, III
Ms. Perla Tabares Hantman
Dr. Martin Karp
Ms. Lubby Navarro
Ms. Mari Tere Rojas

Superintendent of Schools

Mr. Alberto M. Carvalho

Office of Management and Compliance Audits

Mr. José F. Montes de Oca, CPA
Chief Auditor

Contributors to this report:

Audit Performed by:

Mr. Michael A. Hernández, CPA
Mrs. Jeny Priante
Ms. Teresita M. Rodriguez, CPA

Audit Supervised and Reviewed by:

Ms. Teresita M. Rodriguez, CPA
Mr. Trevor L. Williams, CPA





Miami-Dade County Public Schools

giving our students the world

Superintendent of Schools

Alberto M. Carvalho

Chief Auditor

José F. Montes de Oca, CPA

Miami-Dade County School Board

Dr. Lawrence S. Feldman, Chair

Dr. Marta Pérez, Vice Chair

Dr. Dorothy Bendross-Mindingall

Susie V. Castillo

Dr. Steve Gallon III

Perla Tabares Hantman

Dr. Martin Karp

Lubby Navarro

Mari Tere Rojas

February 9, 2017

The Honorable Chair and Members of the School Board of Miami-Dade County, Florida
Members of the School Board Audit and Budget Advisory Committee
Mr. Alberto M. Carvalho, Superintendent of Schools

Ladies and Gentlemen:

In accordance with the Audit Plan for the 2015-16 fiscal year, we have performed an audit to evaluate the processes for collecting and storing protected information, by various departments, pursuant to HIPAA Privacy Rule and IDEA Confidentiality requirements. The objective of the audit was to determine the adequacy of internal control and safeguards to assure the District's compliance with the applicable HIPAA and IDEA rules and requirements and protecting PHI and PII.

Our audit found that the Miami-Dade County Public School District is keenly concerned about protecting sensitive personal health and identifying information. The School Board has approved a Comprehensive Identity Protection Plan and various policies aimed at reducing the risk of identity theft and protecting sensitive information. We found both sets of documents established a good foundational framework for achieving their intended goals, but concluded that enhancements to them are needed to address certain areas of risk and compliance.

We also concluded that, generally, physical controls over sensitive information collected and maintained, in the context of the scope of this audit, are adequate. Nevertheless, there were otherwise identified areas of exposure to sensitive information and non-compliance with HIPAA and IDEA rules and requirements that the administration will need to address.

Our findings and recommendations were discussed with management and their responses are included. We would like to thank management for their cooperation and for the courtesies extended to our staff during the audit.

Sincerely,

José F. Montes de Oca, CPA, Chief Auditor

Office of Management and Compliance Audits

Office of Management & Compliance Audits

• School Board Administration Building • 1450 N.E. 2nd Ave. • Suite 415 • Miami, FL 33132 •
305-995-1318 • 305-995-1331 (FAX) • <http://mca.dadeschools.net/>

TABLE OF CONTENTS

	Page Number
EXECUTIVE SUMMARY	1
INTERNAL CONTROL ASSESSMENT	3
BACKGROUND	4
ORGANIZATIONAL CHART	7
OBJECTIVE, SCOPE, AND METHODOLOGY	8
 FINDINGS AND RECOMMENDATIONS	
General Finding of Compliance	10
 1. The Board-Approved Comprehensive Identity Protection Plan Is Only Partially Implemented	 13
 2. Extensive Safeguards to Protect Confidential Student Information Are in Place, but Additional Measures Are Needed to Limit Exposure of Student’s, Employee’s, and Retiree’s Sensitive Information	 17
 3. The Extent and Nature of Training in the Handling and Safeguarding of PII and PHI R&B Staff Receives Is Insufficiently Documented	 31
 4. R&B Policies and Procedures can be Strengthened to Address the Requirements of the HIPAA Privacy Rule	 33
 5. The District Is Compliant with Safeguarding Data Stored in Copiers Removed from Service, but Could Strengthen Its Policy on Safeguarding Data Stored in Computers When Disposed	 35
 6. Information System’s Access Protocol can be Strengthened to Prevent Exposure of PII and PHI	 41
 7. Service Organization Report Relevant to Security, Confidentiality, and Privacy Should be Obtained from Some Vendors Providing Healthcare Services, and Contracts Should be in Place for All Healthcare Vendors	 43

**APPENDIX A: Summary of the Completeness of R&B’s Policy to
Ensure Compliance with the Relevant Requirements of
the HIPAA Privacy Rule 47**

**APPENDIX B: Summary of Compliance with Relevant
IDEA Confidentiality Requirements 53**

MANAGEMENT’S RESPONSE 55

GLOSSARY OF TERMS, ABBREVIATIONS, AND ACRONYMS

AICPA – American Institute of Certified Public Accountants
CFR – Code of Federal Regulations
CUM – Student Cumulative Records File
ePHI – Electronic Protected Health Information
FBMC – Fringe Benefits Management Company
FERPA – Family Education Rights and Privacy Act
GB – Gallagher Bassett
HIPAA – Health Insurance Portability and Accountability Act
IDEA – Individuals with Disabilities Education Act
IRP – ITS’ Incidence Response Plan (draft)
ITS – Information Technology Services
LEA – Local Educational Agency
M-DCPS – Miami-Dade County Public Schools
M-DSPD – Miami-Dade Schools Police Department
NSS – The District’s Network Security Standards
PHI – Protected Health Information
PII – Personally Identifiable Information
PSA – Public Service Announcement
R&B – The Office of Risk and Benefits Management
R&BO – Risk and Benefits Officer
SEA – State Educational Agency
SOC – Service Organization Controls
TPA – Third Party Administrator
USC – United States Code

Why We Did This Audit

The District collects and stores, from its students and employees, certain information that is protected under the Federal Individuals with Disabilities Education Act (IDEA) and Health Insurance Portability and Accountability Act (HIPAA). Non-compliance with the confidentiality and privacy provisions of these acts may result in severe consequences for the violator.

What We Recommend

We are making 13 recommendations to management to strengthen internal controls over the privacy and security of sensitive information, as follows:

- *The M-DSPD should develop the PSA to be televised during morning announcements and made available on the Department's website and YouTube channel, as required by the Comprehensive Identity Protection Plan.*
- *The District should develop a common, uniform notice containing all elements required for annually notifying parents and eligible students of their rights to inspect and review student educational records. Authorized school personnel should annually review student records and remove images of Social Security cards.*
- *Maintain written documentation of HIPAA-related training provided to R&B staff members and the on-site representatives.*
- *The R&BO should amend R&B's existing HIPAA Privacy and Security Policy to include all relevant requirements of the HIPAA Privacy Rules and implementing regulations.*
- *The District's policy for protecting sensitive data in electronic form should require staff to properly document the destruction of the data before the equipment containing the data is disposed.*
- *Further analyze certain login protocols that may cause exposure of personal sensitive information and implement reasonable solutions that will eliminate the risk.*
- *All service organizations providing health benefit administrative services to M-DCPS should be required to annually submit an SSAE No. 16 SOC 2 report to R&B.*
- *The District administration should execute contracts with all vendors providing healthcare services to District employees.*

What We Found

Our audit found that the District was generally compliant with some of the requirements of HIPAA and IDEA we deemed relevant to our audit objectives. In general, policies and procedures for safeguarding the security, privacy, and confidentiality of protected health information (PHI) and/or personally identifiable information (PII) were in place, although incomplete.

Recent actions taken by the District, including revising the training content for school registrars, promulgating School Board Policy for the development of a Comprehensive Identity Protection Plan, and transitioning to an alternate student identification number, demonstrate that the District is acutely aware of and diligently addressing the risks of identity theft.

We found that although policies are in place to address some requirements, adherence to these policies did not always occur. For instance, some features of the Comprehensive Identity Protection Plan are yet to be developed. Copies of students and/or parents' Social Security cards are stored in student cumulative files. The notice to parents informing them of their rights under the Family Education Rights and Privacy Act (FERPA) omits certain required elements. Physical safeguards to protect against unauthorized disclosure of PHI and PII in the possession of R&B and on-site representatives' staff can be strengthened. Documentation of the training received by Risk and Benefits staff handling PHI and PII, as well as, of the disposition of computer hard drives

that may contain PHI and PII is insufficient. The policies and procedures developed by R&B for managing HIPAA privacy requirements could be enhanced, as it lacks certain important components. Certain information system access protocol needs to be strengthened in order to limit the potential exposure of sensitive information, including PHI and PII. Although R&B obtains certain reports on financial controls at service organizations that receive and store sensitive information pertaining to M-DCPS employees, the safeguard could be strengthened by requiring that a report providing a higher level of assurance about those organizations' security and controls be submitted to the Office of Risk and Benefits Management. Contractual agreements with some companies providing health and life insurance products to District employees, through the District, are also needed.

Based on our observations, we made 13 recommendations. Our detailed findings and recommendations start on page 13. There were other matters that came to our attention during our audit, which were deemed non-reportable because they were either immaterial or inconsequential. These were nevertheless discussed with management for their information and/or follow-up. We would like to thank the administration for their cooperation and the courtesies extended to our staff during the audit.

Because of the complex nature of the subject matter reported on, this report contains various important details and must be carefully read, in its entirety, to obtain an accurate understanding of our observations and conclusions.

INTERNAL CONTROL ASSESSMENT

Our overall evaluation of internal controls related to the collecting, storing, and safeguarding of sensitive information in compliance with IDEA Confidentiality requirements and HIPAA Privacy Rule for the period under audit is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls		X	
Policy & Procedures Compliance		X	
Effect		X	
Information Risk		X	
External Risk	X		

INTERNAL CONTROLS LEGEND			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance	In compliance	Non-Compliance Issues exist	Non-compliance issues are pervasive, significant, or have severe consequences
Effect	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk	Information systems are reliable	Data systems are mostly accurate but can be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk	None or low	Potential for damage	Severe risk of damage

BACKGROUND

Health Insurance Portability and Accountability Act – HIPAA:

In an effort to improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) included *Administrative Simplification Rules* that required the Federal Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, due to advances in electronic technology that could destroy the privacy of health information, Congress incorporated into HIPAA rules that mandated the adoption of Federal privacy protections for individually identifiable health information (commonly known as the “Privacy Rule”).

The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information (PHI) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires that appropriate safeguards to protect the privacy of PHI be put in place and sets limits and conditions on the uses and disclosures of such information without patient authorization. The Rule also gives rights to patients over their health information, including rights to obtain a copy of, examine, and request corrections to their health records.

HIPAA also contains a Security Rule, which establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires that appropriate *administrative, physical, and technical safeguards* be in place to ensure the confidentiality, integrity, and security of electronic protected health information. As it relates to HIPAA compliance, the focus of our audit was with the Privacy Rule.

All of the HIPAA *Administrative Simplification Rules* are located at 45 CFR Parts 160, 162, and 164.

Individuals with Disabilities Education Act – IDEA:

The Individuals with Disabilities Education Act (IDEA) is a Federal law that requires schools to serve the educational needs of eligible students with disabilities. Infants and toddlers with disabilities (birth to 2-years old) and their families receive early intervention

services under IDEA Part C. Children and youth (ages 3-21) receive special education and related services under IDEA Part B.

According to the Confidentiality section of IDEA Parts B and C, appropriate action must be taken to ensure the confidentiality of any personally identifiable data, information, and records collected or maintained. Parents of a child are afforded the right to confidentiality of personally identifiable information (PII), including the right to written notice of, and written consent to, the exchange of that information among agencies, consistent with Federal and State laws.

Section 300.612 of the IDEA implementing regulations requires schools to give notice that is adequate to fully inform parents about the requirements related to protecting the confidentiality of any PII collected, used, or maintained under the Family Education Rights and Privacy Act (FERPA) and its implementing regulations in 34 CFR Part 99. Records that an educational agency or institution that is subject to FERPA maintains on students with disabilities receiving services under Part B of IDEA are “education records” subject to FERPA.¹ Student health records, including immunization records, maintained by an educational agency or institution subject to FERPA are “education records” subject to FERPA.² Such records, however, are not subject to the HIPAA Privacy and Security Rules.³

Family Education Rights and Privacy Act – (FERPA):

Student Educational Records are confidential documents protected by FERPA, which defines “education records” as all records that schools maintain about students. Pursuant to FERPA, the student holds the same rights as his or her parents hold with respect to education records. FERPA gives parents the right to review and confirm the accuracy of education records. These rights, under FERPA, transfer to the student when he or she reaches 18 years of age or enters a postsecondary institution at any age, at which time he or she is defined as an “eligible student”.

The primary rights of parents and students under FERPA are the right to:

- Inspect and review education records.
- Seek amendments to education records.
- Have some control over the disclosure of PII from educational records.

¹ Joint Guidance on the Application of the *Family Educational Rights and Privacy Act (FERPA)* and the *Health Insurance Portability Accountability Act of 1996 (HIPAA)* To Student Health Records, U.S. Department of Health and Human Services and U.S. Department of Education, November 2008.

² *Ibid*

³ *Ibid*

Although schools must have written permission from the parent or eligible student to release PII, FERPA allows schools to disclose those records without consent to the following parties:

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

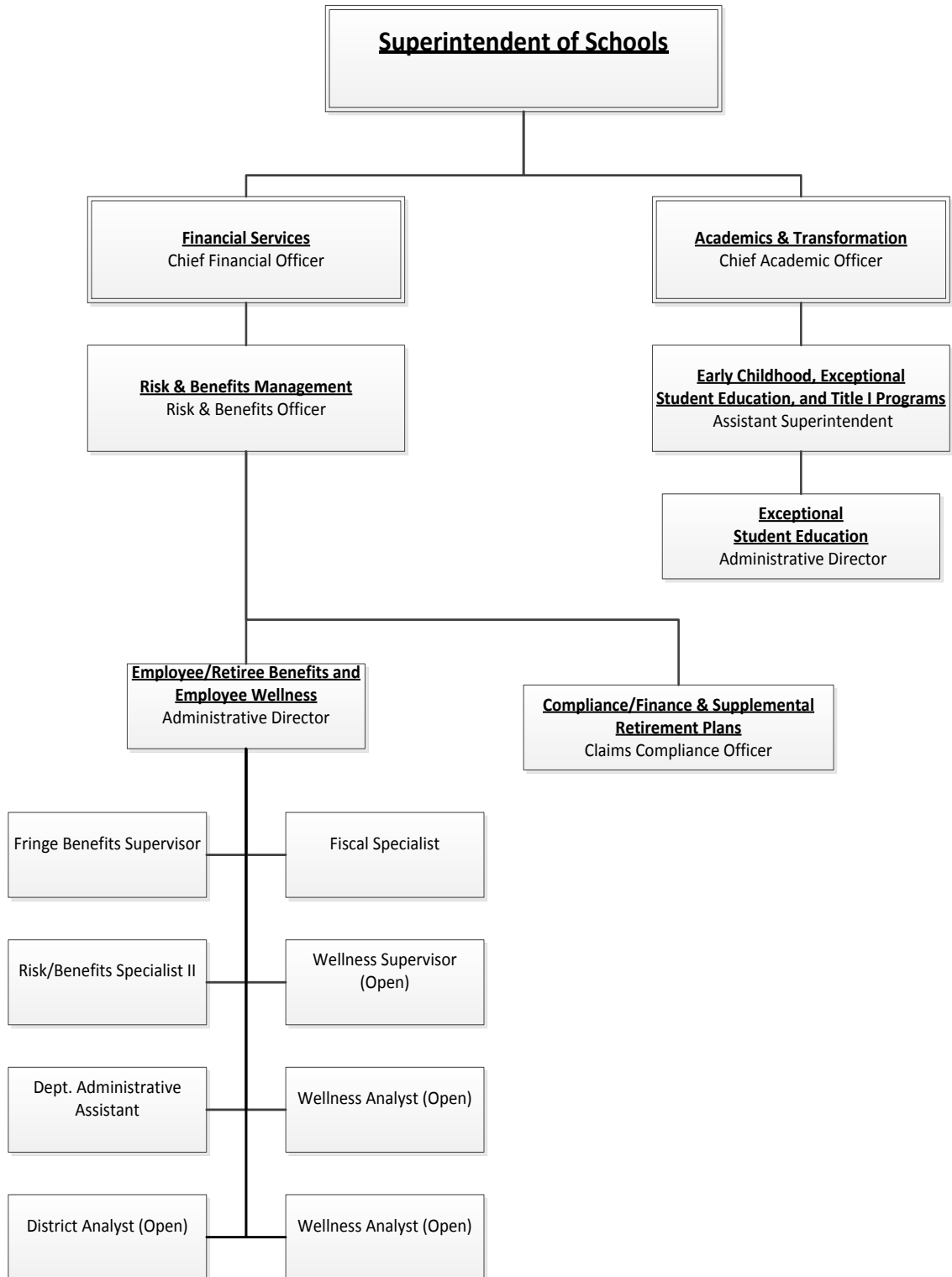
In addition, prior consent is not required for schools to disclose information from a student's education record to the parents if the eligible student is a dependent for Federal income tax purposes under the Internal Revenue Services (IRS) rules.

Lastly, FERPA § 99.7 requires schools to annually notify parents and attending eligible students of their rights under FERPA.

Areas of Responsibility for HIPAA, IDEA, and FERPA Compliance Within M-DCPS

The Office of Risk and Benefits Management (R&B) under Financial Services administers the District's health insurance programs and has primary responsibility for ensuring M-DCPS' compliance with applicable HIPAA Rules. The Office of Exceptional Student Education (ESE) of the Office of Academics and Transformation administers programs for students with disabilities. In accordance with IDEA, ESE is responsible for ensuring that the requirements of IDEA are carried out, including the areas where IDEA and FERPA intersect. Generally, School Operations is responsible for ensuring compliance with FERPA.

ORGANIZATIONAL CHART



OBJECTIVE, SCOPE, AND METHODOLOGY

In accordance with the Audit Plan for the 2015-16 fiscal year, we have performed an audit to evaluate the processes for collecting and storing protected information pursuant to HIPAA Privacy Rule and IDEA Confidentiality requirements. The objective of the audit was to determine the adequacy of internal control and safeguards to assure the District's compliance with the applicable HIPAA and IDEA rules and requirements and protecting PHI or PII.

The scope of our audit covered the current operations and the processes in place during FY's 2014-15 and 2015-16. Our audit primarily focused on the operations of the Office of Risk and Benefits Management and the Office of Exceptional Student Education since these functional units are responsible for ensuring compliance with the audited HIPAA and IDEA requirements, respectively. We also performed certain auditing procedures at selected schools to satisfy our audit objective.

We performed the following procedures to satisfy the audit objective:

- Obtained an understanding of HIPAA and IDEA Privacy and Security Rules as well as other general provisions.
- Obtained an understanding of FERPA in relation to its implementation related to IDEA.
- Obtained an understanding of applicable Florida Statutes and School Board Policies and guidelines.
- Obtained an understanding of the R&B, ESE, and school site operations related to HIPAA, IDEA, and FERPA compliance in the context of our audit objective.
- Observed district staff and contracted benefit consultants in the performance of their duties, including "Open Enrollment," to ascertain the safeguards in handling and storing PHI and PII, including virtual and physical security.
- Reviewed policies and practices for the disposing of certain equipment that may have stored sensitive information.
- Examined student cumulative (CUM) files for evidence of compliance with IDEA, FERPA, and district policy.
- Assessed the adequacy of the District's data recovery plan and breach notification procedures in the context of the audit objective.

- Surveyed appropriate school administrators and staff regarding training received related to the handling and storing of sensitive information, including PII.
- Performed other auditing procedures deemed appropriate.

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards* issued by the Comptroller General of the United States of America. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. A performance audit is an objective analysis, based on sufficient and appropriate evidence, to assist management and those charged with governance and oversight to improve program performance and operations, reduce costs, facilitate decision-making, and contribute to public accountability. Performance audits encompass a wide variety objectives, including assessments of program effectiveness, economy, and efficiency; internal control; compliance; and prospective analyses.⁴ Planning is a continuous process throughout the audit. Therefore, auditors may need to adjust the audit objectives, scope, and methodology as work is being conducted.⁵

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our audit objectives.

⁴ Comptroller General of the United States, *Government Auditing Standards*, 2011 Revision, (Washington D.C.: United States Government Accountability Office, 2011), pp. 17-18.

⁵ *Ibid.*, p. 126.

FINDINGS AND RECOMMENDATIONS

GENERAL FINDING OF COMPLIANCE

HIPAA Compliance

The HIPAA Privacy Rule, which contains “*Standards*” and “*Implementation specifications*,” comprises a variety of requirements to ensure the privacy of individually identifiable health information collected, stored, maintained, and discarded by a covered entity. Implementation specifications also include provisions that are “*addressable*,” meaning they must be implemented if deemed “reasonable and appropriate.”⁶ To determine compliance, we focused on the Administrative Requirements of the Rule (§ 164.530) that are applicable to M-DCPS.

Based on evidence obtained from auditing procedures applied, we conclude that the District is generally compliant with the following relevant standards, as described:⁷

- Privacy policies and procedures – As authorized by School Board Policies 1419.01, 3419.01, and 4419.01, the Risk & Benefits Officer (R&BO) has developed and implemented written policies and procedures to comply with HIPAA Security and Privacy Rules. These policies and procedures, however, can be enhanced to include important required privacy provisions that are omitted.
- Privacy personnel – Pursuant to the aforementioned School Board Policies, and to comply with the HIPAA Privacy Rule, the Board has designated the R&BO as the District’s “Privacy and Security Personnel.”
- Workforce training and management – Some M-DCPS workforce members who have access to protected and individually identifiable health information receive training, as necessary and appropriate for them to carry out their functions. This was

⁶ Pursuant to the Act, if an “Addressable” requirement is not deemed reasonable or appropriate; the agency must document the basis for its determination and implement an equal alternative.

⁷ Of the nine principal Administrative Safeguards, we determined that eight were either relevant to M-DCPS, based on its role as a plan sponsor or the ability to audit the requirements. We found the District to be non-compliant with having procedures for individuals to register a complaint about its compliance with its privacy policies and procedures and the Privacy Rule. (See Finding No. 4) We also found non-compliance with the documentation requirements of the Rule. (See Finding No. 3) While the District’s policies and procedures contain various safeguards, including instructing staff to store records containing PHI in locked areas of controlled or limited access and in locked storage units, and shred documents containing PHI prior to disposing them, these policies and procedures were not always followed, making the District non-compliant with the data safeguards requirements. We did not test the District’s compliance with the “Retaliation and Waiver” requirements and the “Fully-insured Group Health Plan” exception, which does not apply to the District.

particularly evident for the on-site representatives of contracted service providers of healthcare services⁸ but not for R&B staff, as documentation of training provided or received is not maintained.

- Mitigation – Principally, through three main documents—School Board Policy 8351, the District’s Network Security Standards (NSS), and ITS’ draft Incidence Response Plan (IRP)—the District has developed mechanisms to mitigate the harmful effects from known unauthorized use or disclosure of electronic PHI (ePHI). Interviews with School Police personnel also confirmed the existence of mitigation mechanisms. Although satisfying the requirements of HIPAA, these mechanisms might not be as effective as intended, because their “trigger of action” is at either too high a level in the organizational structure (the Superintendent of Schools in the case of Policy 8351) or isolated (ITS in the cases of the NSS and IRP). The safeguards would be more effective if each District department handling PHI, such as R&B, has a mitigation plan that addresses known incidences at their originating point.

IDEA Compliance

The IDEA confidentiality provisions are contained in Subpart F—Monitoring, Enforcement, Confidentiality, and Program Information Monitoring, Technical Assistance, and Enforcement, of the Act. These provisions are intended to ensure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by SEAs and LEAs. Of the 16 sections comprising the Confidentiality of Information provisions, we determined five sections were relevant to our audit objectives, because they were specifically the responsibility of the LEA and were not initiated in response a request from a parent.

⁸ By definition under the HIPAA regulations, these individuals may be considered as members of the covered entity’s “workforce” due to the circumstances under which they operate.

Based on evidence obtained from auditing procedures applied, we conclude that the District is generally compliant with the following relevant standards, as described:⁹

- To comply with the “Access Rights” established by § 300.613, the District has developed policies, including parental notification, that permit parents to inspect and review any education records related to their children that are collected, maintained, or used by the District.
- In compliance with the “Consent” provisions of § 300.622, the District has established procedures for obtaining parental consent before personally identifiable information is disclosed to parties, other than officials of participating agencies, when applicable.
- Of the four paragraphs comprising § 300.623, *Safeguards*, the District has mechanisms, including policies and procedures, which establish compliance with two of the four requirements. Specifically, mechanisms are in place to protect the confidentiality of personally identifiable information at the collection, storage, disclosure, and destruction stages. However, documentation of the destruction of computer hard drives would enhance the destruction process. In addition, the school principal has been identified as the individual responsible for ensuring the confidentiality of any personally identifiable information collected and stored at school site, whereas, the Superintendent is responsible for non-school sites.
- To comply with the “Destruction of Information” provision of § 300.624, the District has developed policies to ensure that parents are informed when personally identifiable information collected, maintained, or used under this part is no longer needed to provide educational services to the child.

RECOMMENDATION:

None; however, for specific recommendations to address matters of concern, please refer to recommendations contained in the detailed findings in the following pages.

⁹ Of the five sections and four subparagraphs deemed relevant to our audit objectives, we found the District to be non-compliant with three of the provisions. Specifically, while the District’s policy requires that a Record of Access Card be maintained to identify parties obtaining access to education records collected, maintained, or used, pursuant to § 300.614 of the Act, we found a number of cases of deviation from the policy. (See Finding No. 2) In addition, although training is provided to school registrars, we found instances where not “all persons” collecting or using personally identifiable information received the required training pursuant §300.623(c) of the Act. (See Finding No. 1) Also, we found no evidence that the District complied with §300.623(d) of the Act to maintain, for public inspection, a current listing of the names and positions of those employees within the District who may have access to personally identifiable information. (See Finding No. 2)

FINDINGS AND RECOMMENDATIONS

1. THE BOARD-APPROVED COMPREHENSIVE IDENTITY PROTECTION PLAN IS ONLY PARTIALLY IMPLEMENTED

On August 6, 2014, the Miami-Dade School Board (“the Board” or “Board”) approved the development of a comprehensive identity protection plan to safeguard the personal information of all students and employees. This was in response to a breach of student data and the high rate of identity theft in Florida. The plan is to provide specific information on awareness, education, and prevention of identity theft.

On June 19, 2015, as a follow-up to the above action of the Board, a Comprehensive Identity Protection Plan (“Plan”) was provided to the Board. The Plan refers to collaboration among the Miami-Dade Schools Police Department (M-DSPD), School Operations, and the Federal and State Compliance Office in its development and proposed the following pertaining to student’s PII and PHI:

Awareness and Education –

- (1) The M-DSPD Community Affairs unit will produce a public service announcement (PSA), which will be televised during morning announcements at senior high schools at the beginning of the school year and later during the school year.
- (2) A "Preventing Identity Theft" tab with tips on how to reduce the chances of being a victim of identity theft will be posted in the M-DSPD website.
- (3) Identity theft prevention information will be shared with parents and guardians through Connect-Ed and social media.

Prevention –

- (1) The masking of ID/Social Security number on all mainframe applications.
- (2) The removal of Social Security number, ethnicity, and gender information from the Student Emergency Data Form (FM-2733).

- (3) The implementation of a new Florida Education Identification Number used for reporting student data in lieu of the Social Security number.
- (4) The inclusion of training on the safeguarding of sensitive student information (i.e., PII) in registrars workshops.

Based on our audit testing, we have concluded that some parts (“Awareness and Education” part 2; and “Prevention” parts 1 – 4) of the Comprehensive Identity Protection Plan have been implemented, whereas, others parts (“Awareness and Education” parts 1 and 3) have not been implemented. For instance, the M-DSPD website includes a “resource tab” containing several links that provide general information, including the types of identity theft attacks and actions to take if victimized by identity theft. However, one of the links directs the user to a vendor that sells various products for identity/credit protection and may incorrectly lead the user to assume that M-DCPS recommends or endorses the products.

Data fields for the collection of student’s Social Security number, date of birth, ethnicity, and gender were removed from the Emergency Student Data Form (FM-2733) and through a “Weekly Briefing” dated April 23, 2015, school principals and assistant principals were instructed to use the revised FM-2733.

We verified that M-DCPS’ Office of Federal and State Compliance conducted multiple workshops for registrars, in which the collecting and handling of sensitive data, including Social Security number was discussed. In addition, we conducted an on-line survey of 25 participants who attended registrar workshops in the 2014-15 and/or 2015-16 fiscal years.

We selected participants from schools with ESE student population ranging between 94 and 933 such students. Of the 25 participants surveyed, 16 (64%) responded as follows:

Survey Questions	Yes	No
1. Was the handling of sensitive personal student information (example: Social Security number, birthdates, addresses, etc.) discussed during your training?	16	0
2. Were the following topics for proper handling of personal student information discussed during your training?		
a. Discontinuing the use of Social Security number on student data cards.	16	0
b. Schools are not to request Social Security numbers/cards.	16	0
c. Schools are not to make copies of Social Security numbers/cards.	16	0
d. School staff's responsibilities to safeguard sensitive personal student information (hardcopy or electronic) and limiting access only to those authorized.	15	1

The survey results confirm that training on the safeguarding of sensitive student information is occurring during registrars workshops as required by the District’s Comprehensive Identity Protection Plan. However, at one school visited—a specialized center—two members of the office staff (not registrars) who are primarily responsible for the custody and maintenance of student records stated they had not received training on the confidentiality of student records containing PII and/or PHI.

Through our audit testing, we have also concluded that two requirements of the Plan—the production of a PSA on identity theft and the dissemination of information on identity theft prevention through Connect-Ed and social media—have not occurred. We contacted the M-DSPD and inquired whether the said PSA had been produced. The department acknowledged that a video on identity theft protection was to be produced for showings during morning announcements and placement on the M-DSPD website and the Department’s YouTube channel. As of the date of our report, however, we have not received a copy of said video or evidence of its production, despite our multiple requests for the same. Moreover, we have not been able to locate the said video on either the M-DSPD website or YouTube channel.

The Plan requires that identity theft prevention information be shared with parents and guardians through Connect-Ed and social media. According to M-DSPD staff, their intention is to use Connect-Ed to communicate updates to students and parents whenever an emergency occurs; however, to date, they have not done so.

As noted above, it is evident that M-DCPS has taken significant steps toward combating identity theft and safeguarding sensitive information. Awareness and education are important factors in this fight. For an effective defense, that knowledge must be possessed by both the District staff charged with collecting and safeguarding sensitive information and the individuals—students and parents—whose information is being collected. Although the said information is passively available to students and parents via the M-DSPD website, it is less likely to have the intended effect since it would require those individuals to actively seek out and search the M-DSPD website. A PSA that is televised at senior high schools and information shared with parents and guardians through Connect-Ed and social media, as required by the Plan, will directly reach the target population of students and parents; thus, increasing the likelihood of the Plan’s effectiveness.

RECOMMENDATION:

- 1.1 One of the essential parts of the Comprehensive Identity Protection Plan is the production of a public service announcement to be televised during morning announcements at senior high schools to educate students on how to reduce the chances of becoming a victim of identity theft. We recommend that the M-DSPD develop the PSA to be televised during morning announcements and made available on the Department’s website and YouTube channel, as required by the Comprehensive Identity Protection Plan. In addition, parents should be provided information on preventing identity theft, as also required by the Plan.**

Responsible Department:

Miami Dade Schools Police Department

Management Response: *Miami-Dade Schools Police Department (MDSPD) has taken corrective action by way of removing a link from Miami-Dade Schools Police (MDSPD) website that included a vendor that sells various products for identity/credit protection that might have incorrectly lead the user to assume that Miami-Dade County Public Schools recommended or endorsed the products.*

MDSPD has also provided the Office of Management and Compliance with a Public Service Announcement (PSA) script with the goal of providing information to parents regarding how to reduce the possibility their child may become a victim of identity theft. The script was also shared with Ms. Daisy Gonzalez Diego, Chief Communications Officer. The PSA is in the process of being filmed and edited and will be found on the MDSPD website by January 21, 2017. MDSPD recently hired part time hourly staff to conduct such functions since we did not previously possess the personnel nor resources to produce this item. Once completed, a link to the video will be provided to the Office of Management and Compliance Audits.

2. EXTENSIVE SAFEGUARDS TO PROTECT CONFIDENTIAL STUDENT INFORMATION ARE IN PLACE, BUT ADDITIONAL MEASURES ARE NEEDED TO LIMIT EXPOSURE OF STUDENT’S, EMPLOYEE’S, AND RETIREE’S SENSITIVE INFORMATION

The National Institute of Standards and Technology (NIST) defines PII as any information about an individual maintained by an agency, including:

- any information that can be used to distinguish or trace an individual’s identity
- any other information that is linked or linkable to an individual

Some types of PII are of a sensitive nature and require more careful handling because of the increase risk of harm to an individual and possible exposure to identity theft, if the information is disclosed or misused. The table below provides examples of PII and sensitive PII:

PII	Sensitive PII
Name	Social Security Number
Home Address	Passport Number
Phone Number	Alien Registration Number
E-mail Address	Financial/Credit Account Number
	Driver's license or state ID number
	Biometric identifiers
	Citizenship or immigration status*
	Medical Information*
	Ethnic or religious affiliation*
	Sexual orientation*
	Account passwords*
	Last 4 digits of SSN*
	Date of birth*
	Criminal History*
	Mother's maiden name*

* = if paired with another identifier

The District uses student information in order to provide appropriate educational services and programs. Federal laws, IDEA and FERPA, protect the privacy of Student Educational Records and apply to all schools that receive funds under an applicable program of the U.S. Department of Education.¹⁰ Therefore, as a recipient of such funds, the District is responsible for safeguarding PII from loss and misuse.

Confidentiality of Student Information Safeguards

Pursuant to IDEA section 617(c) and its implementing regulation, 34 CFR section 300.610 Confidentiality, the Secretary of Education shall take appropriate action, in accordance with section 444 of the General Education Provisions Act (GEPA), to ensure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by State educational agencies [SEA] and local educational agencies [LEA]. The implementation of the requirements of section 444 of the GEPA is delineated in 34 CFR section 99.2 (FERPA regulations). Pursuant to FERPA (20 U.S. Code section 1232g(a)(1)(A)), to be eligible for funds under any applicable program, the educational agency shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children. Both IDEA and FERPA give parents the right to have access to their children's education records, the right to seek amendments to the records, and the right to have some control over the disclosure of PII from the education records. Under FERPA, parents/students have specific rights regarding the release of such records and requires that institutions strictly adhere to these guidelines.

The District recognizes its responsibility in safeguarding student information, including PII in Student Educational Records, and has developed the following policies, procedures, and measures to comply with the applicable statutory and regulatory requirements:

- **School Board Policy 8330 – STUDENT RECORDS**, establishes M-DCPS' responsibility for maintaining, reviewing for accuracy, and restricting access to student records. The policy describes the two types of information—permanent and temporary—typically found in a student's cumulative record and provides guidance on access and transfer of student records, disclosure of information, and FERPA notification. At the school level, the school principal is responsible for the privacy and security of student records.
- **Student Educational Records Manual** – expands on School Board Policy 8330 and includes detailed procedures for maintaining, reviewing, and requesting Student Educational Records, including information on staff's periodic review

¹⁰ IDEA refers to FERPA in many instances for additional requirements and defines education records as those covered under 34 CFR Part 99, the regulations implementing FERPA.

of personal data collected on each student and annual notification to parents and students of their right to inspect those data.

- **School Operations Management Guide** – provides annual guidance to school principals that includes a wide range of Florida Statutes, School Board Policies and administrative directives, a “Year-At-A-Glance” calendar with workshops for the school year, a principal’s tasks list, and a faculty and staff acknowledgement form of multiple School Board policies, including Policy 8330.
- **Exceptional Student Education website** – provides a link to the Florida Department of Education, [IDEA] *Part B Notice of Procedural Safeguards for Parents of Student with Disabilities*, which includes information about a parent’s rights under the Act. The District has used this avenue to inform parents about the procedural safeguards under IDEA, as is required at least annually.
- **Agreement Form for Contracted Services (FM-2453)** – contains terms requiring the confidentiality of student records and compliance with FERPA.

Safeguards and Access to Student Records

The information maintained in a student’s cumulative record is categorized as either permanent or temporary and includes both PII and sensitive PII, which can be accessed by instructional and office staff. The table below provides examples of the data maintained for students according to the Student Educational Records Manual:

Permanent Information	Temporary Information
Student's full legal name	Health information, family background data, standardized test scores, etc.
Birthdate, place of birth, race, and sex	Reports of student services or exceptional student staffing committees
Last known address of the student	Correspondence from community agencies or private professionals
Name(s) of the student's parent(s) or guardian(s)	Driver education certificate
Name and location of last school attended	A list of schools attended

IDEA’s implementing regulation, 34 CFR § 300.623 Safeguards, prescribes that “[e]ach participating agency must protect the confidentiality of personally identifiable information at collection, storage, disclosure, and destruction stages.” Section 300.614 Record of Access, of the Regulation, and FERPA regulation 34 CFR § 99.32 What Recordkeeping Requirements Exist Concerning Requests And Disclosures?, require an educational agency to maintain a record of parties obtaining access to education records in its possession, including the name of the party, the date access was given, and the legitimate purpose for which access was given.

To evaluate the security and handling of student records, we selected and reviewed the student cumulative records of 240 ESE students from six schools and/or specialized centers with significant ESE populations from the South, Central, and North regions (40 students from each location). In addition, we interviewed school staff and observed the physical security of these records.

The following table and comments summarize our observations:

School	Student Records Storage & Security		Copies of Social Security Cards on File	No Record of Access Card on File	Records Accessed, No Consent on File
No. 1 (K-8 Center)	✓		11	9	0
No. 2 (K-8 Center)	✓		11	2	0
No. 3 (Specialized Center)	✓		16	2	0
No. 4 (Specialized Center)	✓		1	39**	0
No. 5 (Senior High)	✓		21	5	1*
No. 6 (K-8 Center)	✓		5	4	0
Total			65	61	1*

✓ = satisfactory

* Access to student record was granted to a government agency; however, evidence of consent or authority given by school administrator to the agency to access the record was not on file. Due to the lack of information on the Record of Access Card, we are unable to determine when access was granted or the school that provided access.

** The school maintains a single log in which activity for all student record files is recorded.

We found that student cumulative records were securely stored and access properly monitored. Records were stored in file cabinets located in either “staff-only areas” or secured rooms, with limited access to school personnel access. The file cabinets were unlocked during school hours and locked after hours.

Of the 240 student records we reviewed, 179 or 75% contained a Record of Access Card, whereas 61 or 25% did not. Our review of the Record of Access Cards disclosed a few instances when access was granted to someone other than the parent or eligible student and written consent was obtained in compliance with the applicable laws and regulations. We identified one Record of Access Card that indicated access to a student record was granted to a government agency, on an unknown date, with no evidence of written consent on file. The overwhelming majority of the Record of Access Cards reviewed contained no entry (i.e., blank). Therefore, we were unable to determine whether such student records were accessed in a compliant manner.

Throughout our review of the 240 records, we found a variety of information/documents, including copies of students and/or parents’ Social Security cards and students’ birth certificate, that were collected and maintained in the student record files.¹¹ In some instances, the documents did not contain a date of collection, making it impossible to determine when the information was collected. Moreover, the purpose for collecting the information was unclear.

A recommended best practice for reducing the risk of exposing PII and identity theft is not collecting too much data and only maintaining what is considered essential. In addition, the M-DCPS Student Educations Records manual states: *“to assure the students’ records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of the students, and to provide an opportunity for the correction or deletion of any inaccurate, misleading, or inappropriate data, the principal shall be responsible for establishing appropriate procedures for the periodic review of personal data collected on each student.”* In addition, during training sessions provided to school registrars and administrators, the removal of sensitive personal data from student records and not requesting or making copies of Social Security cards were discussed. During our discussions with schools administrators from the sampled schools, most indicated that student records are reviewed on an annual basis, and one school provided a checklist it uses to satisfy the review required by the Student Educations Records manual.

¹¹ Other records contained in the files included: personal and family data, health and immunization information, standardized test results, Individualized Education Program (IEP), student photos, correspondence to and from parents and/or guardians and school personnel, court order documents, psychological assessments, copies of driver’s license, passport information, immigration documents, parent consent/refusal forms, M-DCPS forms, and other similar data.

Procedural Safeguards – Notice to Parents

IDEA’s implementing regulation 34 CFR § 300.612 Notice to Parents, requires SEAs to provide notice to parents which fully informs them about the requirements of § 300.123¹², including “a description of all of the rights of parents and children regarding this information, and their rights under FERPA and implementing regulations in 34 CFR part 99.” FERPA and its implementing regulation, 34 CFR Part 99.7(a)(1), mandate that each educational agency annually notify parents or eligible students of their rights under the Act and Regulation.

To comply with the notification requirements of 34 CFR § 300.612, the Florida Department of Education (FDOE) has developed a document, *Part B – Notice of Procedural Safeguards for Parents of Student with Disabilities*, which is made available to parents through the department’s website. Through a link located on M-DCPS’ Office of Exceptional Student Education website, users are connected to the FDOE’s annual notification to parents. We learned from a District ESE administrator that the District has used this avenue to inform parents about the procedural safeguards under IDEA, as required, at least annually.

We reviewed the FDOE *Part B – Notice of Procedural Safeguards for Parents of Student with Disabilities* and found that some rights under FERPA and its implementing regulation, 34 CFR Part 99.7, were not included in the FDOE’s annual notification to parents. The omitted requirements are 34 CFR Part 99.7 subparagraphs (a)(3)(i) and (a)(3)(iii). However, the notice does contain a reference to the notice to parents of their rights under FERPA and 34 CFR Part 99.

To determine whether the omitted subparagraphs were included elsewhere in an alternate document, we asked the administration of the six sampled schools what means each school uses to provide the required annual notification to parents. The schools indicated that this is done through varying means, including either the school’s webpage or the Student Handbook.

We reviewed the documented source of notice used by each school, as indicated by the school administration, and found that none of the notices contained the two omitted requirements, as well as inconsistencies in the content of the notices, as reflected in the following table. The inconsistencies stem from the decentralized and unconnected approach the District uses to notify parents and eligible students.

¹² § 300.123 **Confidentiality of personally identifiable information.**

The State must have policies and procedures in effect to ensure that public agencies in the State comply with §§ 300.610 through 300.626 related to protecting the confidentiality of any personally identifiable information collected, used, or maintained under Part B of the Act.

FERPA Implementing Regulation - 34 CFR § 99.7 – What must an educational agency or institution include in its annual notification?

(Refer to Exhibit 1 for notification requirements (a)(1) through (b)(2))

The School’s Notice Contains This Requirement

School	(a)(1)	(a)(2)(i)	(a)(2)(ii)	(a)(2)(iii)	(a)(2)(iv)	(a)(3)(i)	(a)(3)(ii)	(a)(3)(iii)	(b)(1)	(b)(2)
No. 1 (K-8 Center)	✓	✓	✓	✓	X	X	X	X	✓	X
No. 2 (K-8 Center)	✓	✓	✓	✓	✓	✓	✓	X	✓	✓
No. 3 (Specialized Center)	✓	✓	✓	✓	✓	X	✓	X	✓	✓
No. 4 (Specialized Center)	✓	✓	✓	✓	✓	X	✓	X	✓	✓
No. 5 (Senior High)	✓	✓	✓	✓	X	X	X	X	✓	✓
No. 6 (K-8 Center)	✓	✓	✓	✓	X	X	X	X	✓	✓

✓ = satisfactory

X = not satisfactory

§99.7 What must an educational agency or institution include in its annual notification?

(a)(1) Each education agency or institution shall annually notify parents of students currently in attendance, or eligible student currently in attendance, of their rights under the Act and this part.

(2) The notice must inform parents or eligible students that they have the right to:

(i) Inspect and review the student's education records;

(ii) Seek amendment of the student's education records that the parent or eligible student believes to be inaccurate, misleading, or otherwise in violation of the student's privacy rights;

(iii) Consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that the Act and §99.31 authorize disclosure without consent; and

(iv) File with the Department a complaint under §99.63 and 99.64 concerning alleged failures by the educational agency or institution to comply with the requirements of the Act and this part.

(3) The notice must include all of the following:

(i) The procedure for exercising the right to inspect and review education records.

(ii) The procedure for requesting amendment of records under §99.20

(iii) If the educational agency or institution has a policy of disclosing education records under §99.31(a)(1), a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.

(b) An educational agency or institution may provide this notice by any means that are reasonably likely to inform the parents or eligible students of their rights.

(1) An educational agency or institution shall effectively notify parents or eligible students who are disabled.

(2) An agency or institution of elementary or secondary education shall effectively notify parents who have a primary or home language other than English.

Since the District relies on the FDOE's annual notification to parents (IDEA) to satisfy the required annual notification to parents under FERPA, according to District ESE staff, and neither the FDOE's annual notification nor the other notification to parents used by the six sampled schools includes all of the FERPA-required elements, the District is non-compliant as it relates to the FERPA annual notification to parents requirements.

In addition to the measures stated above, the District also provides guidance regarding parental notification in the M-DCPS Student Educational Records manual. The manual states: *“Each school must provide to parents and eligible students annual notification of their right to inspect and review educational records. The notification should be distributed at the beginning of the school year and must be available in the language of the parent or eligible student... the exact nature of the letter and the procedures for its delivery may be determined by the principal.”*

We performed auditing procedures at the six sampled schools to determine the extent of each school’s compliance with the annual parental notification requirements stated in the manual. Those procedures included comparing the notices, typically found in student/parent handbooks, each school claims it uses to the requirements delineated in the M-DCPS Student Educational Records manual for consistency (Exhibit 2) and inquiring of school administrators about the annual notice. Our audit tests found that the notices in effect at each school sampled did not contain all the requirements detailed in the M-DCPS Student Educational Records manual. The following table summarizes the results of our tests. Moreover, the guidelines contained in M-DCPS Student Educational Records manual do not include all of the elements required by FERPA for the annual notification to parents.

M-DCPS STUDENT EDUCATIONAL RECORDS MANUAL SECTION IV. PUBLIC NOTIFICATION (Refer to Exhibit 2 for the Public Notification Requirements A through H)								
School	The Notice Satisfies This Requirement							
	A	B	C	D	E	F	G	H
No. 1 (K-8 Center)	✓	X	✓	X	X	X	X	✓
No. 2 (K-8 Center)	✓	✓	✓	✓	✓	X	✓	✓
No. 3 (Specialized Center)	✓	✓	✓	✓	✓	✓	✓	✓
No. 4 (Specialized Center)	✓	✓	✓	✓	✓	✓	✓	✓
No. 5 Senior High	✓	X	✓	X	X	X	X	✓
No. 6 (K-8 Center)	✓	X	✓	X	X	X	X	✓

✓ = satisfactory X = not satisfactory

Exhibit 2

M-DCPS STUDENT EDUCATIONAL RECORDS - IV. PUBLIC NOTIFICATION	
Each school must provide to parents and eligible students annual notification of their right to inspect and review student educational records. The notification should be distributed at the beginning of the school year and must be available in the language of the parent or eligible student. A sample letter, for use in the PK-12 program, in English, Spanish, and Haitian Creole (see pages 26-28) has been provided; however, the exact nature of the letter and the procedures for its delivery may be determined by the principal.	
Regardless of the form and style of the notification, the following points must be included:	
A.	A description of the limits placed on access to student educational records.
B.	The procedures established for parents and eligible students to have access to the records for inspection and review.
C.	The provision and condition for the right and the waiver of access.
D.	The procedures established for challenging the content of educational records.
E.	Notification of the right to file a complaint with the Family Policy Compliance Office and the address of that office.
F.	Notification of the right to obtain a copy of the official policy of Miami-Dade County Public Schools pertaining to the Family Educational Rights and Privacy Act .
G.	The categories of information designated as "directory information" (see VI, section A, page 9-10). In this regard, notification must also be made that the parent or eligible student will be given a reasonable period of time to inform the institution that a part or all the "directory information" should not be released without the appropriate prior consent. The objection should be noted by flagging the record on the ISIS - Student Information - Miscellaneous Information screen through the "Unsolicited Literature" flag or on the VACS - Student Information biographical screen. Provisions for granting requests for lists of "directory information" data must also be included.
H.	The conditions under which the rights accorded to the parents are transferred to the students . (See V, section C, page 9).

Procedural Safeguards – Record for Public Inspection

IDEA § 300.623(d) requires each participating agency to maintain, for public inspection, a current listing of the names and positions of those employees within the agency who may have access to personally identifiable information. Based on the auditing procedures performed, we found no evidence of the District’s compliance with this requirement.

Safeguards Over Employee and Retiree Sensitive Information

The R&B HIPAA Privacy and Security Policy states that PII and PHI will be kept in a secure manner, including turning records containing PII and PHI face down, while being used and filing away such records in locked storage overnight or when not in use. The Policy also stated that privacy filter screens will be used on all PC monitors and protected information will not be shared with other office staff unless they are directly involved with the issue at hand.

We performed auditing procedures to test the workforce compliance with these appropriate safeguards. The procedures included observing the layout of the work area where PII and PHI are routinely handled by R&B staff members and other on-site representatives. These procedures were performed during normal working hours and after the close of the workday.

Our tests found that computer monitors were equipped with privacy filter screens, computers were either turned off or locked, storage cabinets were locked, each workstation was equipped with a paper shredder, and trash cans contained no documents containing PII or PHI. We also found that most of the desks inspected did not have records containing PII or PHI lying around on them or notes containing user names or password.

However, our tests also found that the physical layout of the work area was not adequately conducive to preventing the unintentional disclosure of sensitive information to persons not authorized to have access to such information. The office layout features a total of six individual offices divided along two opposite perimeter walls, four open cubicles divided along the other two opposite perimeter walls, and an open area of abutting desks in the center of the work space. This layout leaves the majority of the work area without physical privacy barriers.

Additionally, through our audit observations, we found unsecured boxes and files containing many records of employees and retirees' PII and PHI were either stored on or around some workstations. This condition increases the risk of exposure and breach of sensitive information, because persons who might not be authorized to handle PII and PHI that are in the possession of R&B can access the work area after hours.

RECOMMENDATIONS:

2.1 To limit the exposure to unauthorized use or disclosure of sensitive information, including PII and PHI, we recommend School-site administrators ensure that the periodic review of student records, required by the guidance contained in the Student Educational Records manual, be diligently performed and:

- a) Information deemed to be no longer needed to provide services to students is disposed, pursuant to FERPA guidelines.**
- b) Images of students and parents' Social Security cards are not kept in the student cumulative file. Images of parents' Social Security cards found on file should be immediately destroyed. Images of students' Social Security cards found on file should be destroyed after the number is verified to be correct in the District Student Information System.**
- c) A Record of Access Card is kept on file for every student cumulative file.**

Responsible Department:

School Operations

Management Response: *A Weekly Briefing was disseminated outlining Board Policy 8330 Student Records and notifying Principals that Social Security Cards are not to be duplicated or filed in students cums pursuant FERPA guidelines.*

Additionally, Principals instructed registrars to review all cums and remove and destroy all images of students and parent Social Security cards in accordance to FERPA guidelines.

Lastly, School Operations instructed all Principals identify a designee to review all Cumulative Records for information deemed to be no longer needed to provide services to students be disposed, pursuant to FERPA guidelines.

2.2 To ensure full compliance with FERPA, the District should develop a common, uniform notice containing all required elements for annually notifying parents or eligible students of their rights to inspect and review students' educational records. The District may determine an appropriate means of providing this notice.

Responsible Department: School Operations

Management Response: *School Operations will provide a universal Student/Parent Handbook that provides all of the required elements to promote a positive school climate. Included in the Parent/Student Handbook will be annual notification to parents on their rights to inspect and review students' educational records in accordance with The Family Educational Rights and Privacy Act (FERPA).*

2.3 District administration should implement the necessary safeguards to comply with IDEA § 300.623(d) requirement of maintaining a current listing of the names and positions of those District employees who may have access to personally identifiable information for public inspection.

Responsible Department: School Operations

Management Response: *School Operations directed Principals to maintain a current listing of the names and positions of those employees who may have access to personally identifiable information for public inspection. The lists will be maintained at the school and respective Region. School will update as necessary and submit revisions on an annual basis to their region*

2.4 R&B should provide refresher training to its staff members and other on-site representatives on the security provisions contained in its HIPAA Privacy and Security Policy to promote aware of and adherence to these policies that are designed to protect sensitive information that is in R&B’s custody. In addition, R&B administration should conduct periodic reviews of staff’s and other on-site representatives’ compliance with these provisions. R&B should consider strategies to improve the physical security of the general work area.

Responsible Department:

Office of Risk and Benefits Management

Management Response: *The Office of Risk and Benefits Management required all employees to complete an accredited, two part HIPAA training in September 2016. The training covered HIPAA Privacy for Covered Entities, and HIPAA Information Security Standards as of 2016. The Office’s vendors are also required by RFP and contract to provide HIPAA training to all their employees. The Office’s leadership team performed a HIPAA Compliance walkthrough in October 2016, which identified opportunities for improvement. Moving forward, random unannounced information security reviews will be performed to assure that the appropriate practices are consistently followed.*

The Office of Risk and Benefits Management will review several office layout options and related costs to improve the physical security of the general work area. Until the Office is moved to its permanent location, these options, including the purchase of individual cubical type accommodations will be carefully evaluated. The Office is also evaluating an electronic filing system in an effort to reduce the amount of paper records.

3. THE EXTENT AND NATURE OF TRAINING IN THE HANDLING AND SAFEGUARDING OF PII AND PHI R&B STAFF RECEIVES IS INSUFFICIENTLY DOCUMENTED

Training is a vital piece of an organization's internal controls and ensures that employees have the necessary knowledge and skills to carry out their duties. According to HIPAA Privacy Rule, Part 164 Subpart E, 164.530 (b)(1), an entity must train all members of its workforce on its policies and procedures with respect to PHI, as necessary and appropriate for the members of the workforce to carry out their functions within the organization. Section 164.530(b)(2)(ii) of the Regulation requires the entity to document the training that has been provided to its workforce.

To satisfy our audit objective, we performed various auditing procedures, as described in the following sections, to determine the extent of training provided to the R&B staff and on-site insurance representatives, regarding procedures for handling and safeguarding PII and PHI.

Training Provided to Staff of the Office of Risk and Benefits Management

We inquired of R&B's management and staff about whether they receive training related to procedures for handling and safeguarding PII and PHI. R&B management replied that R&B staff primarily handles PII data, while the on-site insurance representatives handle PHI data and ongoing in-house training is provided during staff meetings and targeted towards the employee's assigned role. Of the four R&B staff members interviewed, three who handle PII information stated that the training is primarily limited to updates on regulations and procedures, via staff meetings or emails.

To determine the nature and breadth of the said training, we requested that R&B management provide to us documentary evidence of the subject matter discussed during these informal training meetings, such as, sign-in sheets, agendas, handouts, memos, meeting notes, topic sheets, emails, or any other documents. The documentary evidence we received from R&B consisted of Microsoft Outlook meeting notifications emailed to staff, none of which mentioned training sessions in the subject line or body of the document.

Due to the lack of corroborating evidence, we are unable to determine the extent and type of training in the area of PII and PHI provided to R&B staff. The lack of documentary evidence on the extent and nature of training provided makes the District non-compliant with the applicable HIPAA regulations and increases the risk of exposure to the District, as this could weaken the District's position in the event of a breach and/or challenges or claims emanating from any such incident. In addition, documenting and/or certifying the training provided or received is consistent with internal controls and best practices.

Training Provided to On-site Insurance Representatives

According to R&B management, on-site representatives of healthcare companies that provide such services to M-DCPS receive training directly from their respective company. We interviewed seven on-site representatives, who all stated they receive HIPAA training directly from their company. All of the on-site representatives also indicated that updates on regulations and procedures are sometimes provided by R&B via staff meetings.

To corroborate the assertions of the on-site representatives, we requested that they provide to us documentary evidence of the training, such as, sign-in sheets, agendas, handouts, manuals, or any other documents. Three of the five companies provided their HIPAA Privacy and/or Security Policy and Procedures manual (Manuals), while the remaining two did not, asserting that the information is proprietary. We reviewed the Manuals received and verified that employees are required to receive training for the purpose of understanding and complying with HIPAA Privacy and Security Rules. In addition, we received a copy of an on-site representative's "transcript reports," listing the courses she completed for 2014 and 2015, which included "2015 Enterprise Privacy and Security Training" and "Information Security and Privacy Awareness Training 2014."

Based on our tests, it is evident that the on-site representatives of companies providing healthcare services to M-DCPS are trained in the handling and safeguarding of PHI and PII. The nature and extent of training in this area provided by three of these companies to their on-site representatives was documented and verified; however, we were unable to make a similar determination for the remaining two companies due to the denial of access to requested information.

RECOMMENDATION:

- 3.1 We recommend that R&B maintain written documentation of training provided to all of its staff members and the on-site representatives of health services providers on the handling and safeguarding of PII and PHI to comply with the requirements of the HIPAA administrative safeguards.**

Responsible Department:

Office of Risk and Benefits Management

Management Response: *The Office's written documentation of training provided to all Risk Management employees which was completed in September 2016, is available upon request. Risk and Benefits Management believes documentation to be sufficient, but guidance from the Office of Management Audits is welcome.*

4. R&B POLICIES AND PROCEDURES CAN BE STRENGTHENED TO ADDRESS THE REQUIREMENTS OF THE HIPAA PRIVACY RULE

The School Board acknowledges that its self-insured group health plans shall comply with HIPAA Privacy Rule and all implementing Federal regulations. Through the promulgation of School Board Policies 1419.01, 3419.01, and 4419.01, the Board authorized the R&BO “to develop, propose to the Board, and implement the Board approved internal policies and procedures for the group health plan(s) relating to the use and disclosure of protected health information.” The policies granted authority to the R&BO to bring into effect the actions required by the HIPAA administrative procedures.

The Office of Risk and Benefits (R&B) Management Procedures and Guidelines, includes the HIPAA Privacy and Security Policy authorized by the School Board. The policy indicates the Board-granted authority for its development and identifies the Risk and Benefits Officer as the privacy official of the group health plans. The policy specifically identifies the following six components to follow for compliance with applicable Federal and State Laws and Board policies, as they relate to HIPAA:

1. Security – provides guidelines for staff members’ access to, use, and disposal of PII and PHI (physical security).
2. Acceptable Use – stresses confidentiality of, and limited access to PII and PHI based on their intended use.
3. Disclosure – provides guidance regarding the disclosure of PHI and consent requirements.
4. Request for Amendment – indicates the process for requesting the amendment of PHI.
5. Coordination of Privacy Law – provides information on the Gramm-Leach Bliley Act.
6. Florida Statutes – presents a list of Florida Statutes that may require the reporting of PHI under certain circumstances, without consent.

We completed a comparative analysis of the R&B HIPAA policy, District policies, and 45 CFR Part §164, Subpart E—Privacy of Individually Identifiable Health Information, which disclosed that the R&B policy was lacking several standards and requirements of the HIPAA regulations’ Administrative Requirements. (See Appendix A)

Given that R&B's HIPAA policy was authorized by the Board and intended to represent the District's internal policy for ensuring compliance with the HIPAA Privacy Rule, the omission of specific guidance in the policy creates an instance of non-compliance and increases potential exposure of the imposition of civil monetary penalty.

RECOMMENDATION:

4.1 In order to fulfill the Board's directive for the development of an internal policy to ensure the District's compliance with the HIPAA Privacy Rules, we recommend that the R&BO review R&B's existing HIPAA Privacy and Security Policy and amend it, to include all relevant requirements of the HIPAA Privacy Rules and implementing regulations.

Responsible Department:

Office of Risk and Benefits Management

Management Response: *In addition to the existing HIPAA Privacy and Security Policy, the Office will develop a HIPAA Privacy and Security Employee Handbook to address the issues identified in Appendix A.*

5. THE DISTRICT IS COMPLIANT WITH SAFEGUARDING DATA STORED IN COPIERS REMOVED FROM SERVICE, BUT COULD STRENGTHEN ITS POLICY ON SAFEGUARDING DATA STORED IN COMPUTERS WHEN DISPOSED

In an effort to ensure the protection of PII and PHI, M-DCPS has adopted and implemented various safeguards to provide guidance on the disposition of computers and other technical equipment. This is particularly important due to the permanent storage of student and employee PII and PHI in computers and copier machines with hard drives, and these equipment typically having “a life” after being surplus by M-DCPS.

Pursuant to School Board Policy 7310 – Disposition of Surplus Property, once Board-owned equipment are deemed to be obsolete, uneconomical, inefficient, or serve no useful function, they are disposed through either a sale, auction, or donation. Therefore, individuals possessing surplus equipment containing “unwiped” hard drives and the ability to access the hard drives can view the information stored on the hard drives, including images of all documents that were previously copied or printed on the copier machines.

The following are some of the steps M-DCPS takes to ensure protection of personal identifiable/health information:

- **M-DCPS Network Security Standard:**

Section 2.0 – The Network Security Standard applies to employees and vendors with access to M-DCPS computer resources.

Section 4.1.2 (13) - Any computers or networking devices removed from service in the District must have the hard drives degaussed, re-formatted, or otherwise cleared of software and data before they can be sold, given away or disposed of.

Section 4.1.2 (14) – Copier and printer technology has evolved to the point where there is wireless communication to these devices from computers and hard drives/solid state memory within the device may hold copies of all documents printed/copied/faxed. This means that wireless transmissions of confidential data whether printed or copied, can be intercepted and hard drives containing PII/PHI can be accessed. Although the bids and contracts may specify that hard drives be removed or degaussed by the vendor when the machines is being taken out of the District use, local supervisors should confirm that this has been done.

- **Bid #033-KK11** – M-DCPS contract for multifunctional devices, copying equipment, service and supplies for the period January 2011 through January 2016 required the vendor to “remove any stored copy/print/scan job data from each units memory at no charge to the District.” The bid instructs vendors, “At a minimum to

minimum to provide a form indicating a data security device has been installed on the machine/device. The vendor should also provide a third party certificate verifying the data security device removes any data stored on the multiple functional product (MFP).” According to the Chief Procurement Officer, upon expiration of the aforementioned bid, M-DCPS currently is “piggy backing” on another government agency contract for the same type of services that include the securing of hard drives.

- **School Board Policy 7310 – Disposition of Surplus Property**

Section C.2.a. – An appropriate Outgoing Controlled Equipment form is to be used to record any request for disposition of a described item of property and to record the review and approval by two (2) persons.

- **Weekly Briefings** – Multiple weekly briefings to M-DCPS employees during fiscal years 2011-12, 2012-13, and 2014-15 included procedures on the proper handling and disposing of hard drives of district-owned and leased copiers and computers.

To assess the extent of compliance with the abovementioned safeguards to satisfy our audit objectives, we visited six schools with high ESE student enrollment belonging to the South, Central, and North Region Offices and Specialized Centers, and R&B. Our objectives included assessing the following:

- The proper handling of hard drives for all computers and leased and owned copier equipment disposed during fiscal years 2014-15 and 2015-16.
- Verifying whether the current lease agreements for copiers at the seven sites were obtained through bid #033-KK11 or included data a security clause for the handling of hard drives and PII/PHI similar to the clause contained in said bid.

Based on our audit testing, we concluded that the privacy and security provision of Bid #033-KK11, pertaining to the proper handling of hard drives contained in district-owned and leased copiers, was being complied with.

The following table summarizes of our observations pertaining to photocopying machines that were operated or disposed by the seven sampled locations during FYs 2014-15 and 2015-16:

Copiers With Hard Drives (District-Owned and Leased) Operated or Disposed at the Seven Sampled District Locations During FYs 2014-15 and 2015-16					
School	District-Owned Copiers (Disposed)		Leased Copiers (Operated)		
	Reported on Outgoing Controlled Equipment form (FM 1670)	Hard Drive Reported Removed	Number of Leased Copiers Tested	Lease Agreement Includes PII/PHI Safeguards	Removal of Copier Hard Drive Documented if Copier Was Replaced
No. 1 (K-8 Center)	None	N/A	0	N/A	N/A
No. 2 (K-8 Center)	None	N/A	1	1	N/A
No. 3 (Specialized Center)	1	Yes	0	N/A	N/A
No. 4 (Specialized Center)	None	N/A	0	N/A	N/A
No. 5 (Senior High)	5*	Yes	0	N/A	N/A
No. 6 (K-8 Center)	None	N/A	0	N/A	N/A
R&B	1	Yes	3	3	N/A

* = Two (2) out of the five (5) copiers reported did not contain a hard drive. Also, we were unable to determine whether one (1) other copier had a hard drive. According to the school IT technician, the copier did not have a hard drive; however, we were unable to confirm this assertion.

The results of our tests of safeguards over District-owned computers was inconclusive, in the context of our audit objectives. According to the IT technicians we interviewed, they are aware of the NSS degaussing requirements and options to remove hard drive data. However, we noted there is a lack of uniform procedures. The technicians stated that they generally either destroy the computer hard drives or erase the data on the hard drives and reuse them. At one school, we were able to observe an inventory of hard drives that were removed from surplus computers and intended for re-use, according to the IT technician. We requested proof of the degaussing of the hard drives of surplus computers from the other IT technicians, since we did not have access to those machines or their hard drives, but were provided none. According to the IT technicians, they are not required to document that the hard drives were degaussed. Therefore, without access to specifically identified disposed computers and there being no record of the action taken by the IT technicians, we were unable to verify, with certainty, that data is removed from computer hard drives when the equipment is disposed, in compliance with the District’s NSS.

The following table summarizes our observations pertaining to district-owned computers reported as disposed by t seven sampled locations during FYs 2014-15 and 2015-16. We noted that the computers reported on the Outgoing Controlled Equipment form (FM-1670) were “controlled property,” valued at \$1,000 or greater. However, due to the lack of information, we were unable to determine whether this accounts for all computers, including those costing less than \$1,000, which would also require proper handling of their hard drives when the property is disposed.

District-Owned Computers Disposed During FYs 2014-15 and 2015-16		
School & District Office	Number of Computers	
	Reported on Outgoing Controlled Equipment form (FM-1670)	Reported as degaussed [ⓧ]
No. 1 (K-8 Center)	0	0
No. 2 (K-8 Center)	32	0
No. 3 (Specialized Center)	44	0
No. 4 (Specialized Center)	0	0
No. 5 Senior High	19	0
No. 6 (K-8 Center)	30	0
R & B District Office	0	0
Total	125	0

[ⓧ] M-DCPS Network Security Standard and School Board Policy 7310 do not require documentation of the degaussing of hard drives.

Leaving PII/PHI data on computers can expose both individuals and organizations to identity theft and fraud and violates federal law. To determine the likelihood that the above computers reported on the Outgoing Controlled Equipment forms might contain PII and/or PHI, we queried the Property Accounting system to identify the probable use of the computers assigned an active property control number.¹³ Of the 125 computers, 117 had active property control numbers. The results of the query revealed that five computers were most likely assigned to school administrators and/or main office personnel, based on their room assignment, and 14 other computers were located in the school library. We were unable to determine the probable use of the remaining 98 computers. Since we did not have access to the disposed computers noted above, we were unable to determine whether any PII/PHI was contained on the hard drives.

Although the conditions noted above might not specifically bear upon strict convergence of the audit scope—compliance with HIPAA Privacy Rule and IDEA Confidentiality requirements—they do, however, bear upon the requirement of the Rules for agencies to develop policies and procedures to protect the privacy and confidentiality of individual’s PII and PHI at all stages, including at their disposal. Although the District has policies and procedures in place for safeguarding data stored on electronic equipment at the time of their disposal, an integral part of an effective plan includes documenting compliance, which is also a requirement of the HIPAA Privacy Rule. This important element is missing from the District’s NSS, its policy for safeguarding data stored on computers at the time of their disposal, and makes it difficult for the District to prove compliance with its policy.

¹³ Tangible property costing \$1,000 or greater is assigned a Property Control Number and tracked in the Property Accounting System.

RECOMMENDATIONS:

5.1 In order to document compliance with the actions required by the District's Network Security Standard, as part of the data removal policy, we recommend that:

- a) The NSS be revised to specifically require the degaussing or removal and destruction of computer and copier hard drives be properly documented before these equipment are disposed.**

Responsible Department: Information Technology Services

Management Response: *The NSS has been revised to include language that addresses this recommendation. The revisions are currently going through the approval process.*

- b) The Outgoing Controlled Equipment form (FM 1670) be modified to include a field to record the occurrence of this action.**

Responsible Department: Office of the Controller

Management Response: *The Office of the Controller will revise The Outgoing Controlled Equipment form (FM 1670) adding a field to denote that the hard drives have been removed or degaussed.*

5.2 We recommend that property disposal procedures for technical equipment require a final inspection to confirm that all data is removed/degaussed from hard drives. This process would be independent from the degaussing process and will ensure the removal of data from computer hard drives. This is a necessary step to verify that confidential data are not released.

Responsible Department: Information Technology Services

Management Response: *The school site administrator will request, through our Incident Management System (HEAT), the degaussing of device(s). The completed HEAT ticket will notify the requester when this action is completed. The HEAT ticket number should be referenced on FM 1670 to show the degaussing is complete. A Weekly Briefing will be sent explaining this process.*

6. INFORMATION SYSTEM'S ACCESS PROTOCOL CAN BE STRENGTHENED TO PREVENT EXPOSURE OF PII AND PHI

Information technology controls are essential to an agency's plan for securing and safeguarding the confidentiality of sensitive information, as required by HIPAA Privacy and Security Rules and IDEA Confidentiality provisions. A well designed plan will prevent or limit unauthorized access to and exposure of PII and PHI. The plan, through its implementing policies and procedures, should include user access being appropriately assigned and limited to ensure the security of employee and student information.

During our audit, guided "Open Enrollment" sessions for employee health benefits were offered by R&B for Fall 2015 and Spring 2016, at various locations. We observed some of the sessions, November 30, 2015, May 2, 2016, and May 5, 2016. These sessions were staffed by R&B representatives offering personalized assistance in healthcare plans and other employee benefits. Enrollment activity was completed electronically using computers set-up by R&B at each of the sites visited.

During the observation of November 30th, employees were asked to log-in to their "employee portal" for SAP access in order to view and make changes to their fringe benefits. We observed that at the end of each session, some employees logged-out of their portal, while others were logged-out by an R&B representative. We inquired of the representative regarding the inconsistency, and she replied that she logs-out for each employee she assists to avoid any "mix-up" that may lead to making benefit changes to the wrong employee. To expand on this concern, we performed tests, involving introducing various scenarios, to determine the potential impact emanating from the stated condition. These tests were performed on individual workstations in our office in an effort to duplicate the conditions noted through our observations during Open Enrollment.

Our tests identified certain technical flaws in the information system that may result in the exposure of sensitive information, including PII and PHI of an individual, when the Health Benefit application was accessed by an employee. The risk appears to be limited to situations where computer workstations either are shared or could be accessed by more than one user.

For security reasons, we have omitted specific details about the technical flaws and the various scenarios applied during our testing of the system from this report. However, we discussed and formally communicated those conditions and scenarios, in detail, to management in a separate document.

The Chief Information Security Officer, Information Technology Services (ITS), proposed a few solutions to address the conditions noted above. Although these proposed solutions may

mitigate the conditions noted, the risk of unauthorized access to employee information and systems applications has not been addressed to a satisfactory resolution.

RECOMMENDATIONS:

6.1 Because of the risk of potential exposure of employees and retirees' sensitive information, R&B should develop and communicate a strategy for mitigating this risk in preparation for future Open Enrollment sessions until the matter is satisfactorily resolved. The strategy may include, among other things, requiring mandatory authentication and signoff/logout by each employee when being assisted by an R&B representative during guided Open Enrollment sessions.

Responsible Department: Office of Risk and Benefits Management

Management Response: *The District's enrollment process requires that employees log-off after completing their open enrollment, to prevent exposing PHI and PII information. The Office will work with ITS and the Board's third party administrators to evaluate additional security enhancing options that are available to the District. To further minimize risks, the District has purchased cyber liability coverage with coverage limits of \$10 million per claim/annual aggregate subject to a \$250,000 self-insured retention.*

6.2 ITS should analyze the condition further and implement reasonable solutions that will eliminate the existing risk.

Responsible Department: Information Technology Services

Management Response: *Currently, all users are automatically logged off applications after 20 minutes. In addition, Section 5.1.3 of the Network Security Standards states the following: "Users are responsible for all activity associated with their user-id. When a user is finished using a computer or will be leaving the computer unattended, they must log off or lock the computer (CTRL-ALT-OELETE, Lock Computer) to prevent their account from being compromised. This is particularly important for teachers - leaving their account open on the computer may provide students and other unauthorized users with access to their grade book, e-mail account, personal information on the District Portal, and other sensitive/confidential applications and data (see 4.1.1.10)." However, in addition to the above-mentioned best practices, ITS has developed a solution that will log users out of SAP when they close the browser. This solution is scheduled to be implemented in early February 2017. ITS will continue to watch for any new risks.*

7. SERVICE ORGANIZATION REPORT RELEVANT TO SECURITY, CONFIDENTIALITY, AND PRIVACY SHOULD BE OBTAINED FROM SOME VENDORS PROVIDING HEALTHCARE SERVICES, AND CONTRACTS SHOULD BE IN PLACE FOR ALL HEALTHCARE VENDORS

The Service Organization Control (SOC) report obtained by R&B from one of the vendors providing health benefit services to the District is adequate for complying with financial statement reporting purposes. However, the SOC report, namely SOC 2 Type 2, which reports on internal controls over the service organization’s information system relevant to security, availability, processing integrity, confidentiality, or privacy and their operating effectiveness, is not obtained by R&B.

In addition, while the District maintains executed contracts with two of the five vendors providing some form of health insurance services to the District and/or its employees, it does not have executed contracts with the remaining three vendors.

The major goal of the HIPAA Privacy and Security Rules is to assure that individuals’ health information is properly protected and that covered entities creating, receiving, maintaining, or transmitting such information in electronic form (e-PHI) are protecting it accordingly. Therefore, it is important for an organization to ensure that PHI and PII data are collected, accessed, shared, and disposed of properly.

In administering M-DCPS’ comprehensive fringe benefits program, which includes health, life, disability, dental, and vision coverage for all benefit eligible employees, their eligible dependents, and retirees, R&B partners with various hired service providers, all of whom have on-site representatives to provide assistance. The District employees’ personal and health information is maintained on these companies’ information systems. The following are the companies with on-site representatives on M-DCPS property:

- Cigna
- FBMC
- United Healthcare - Dental/Vision
- Delta Dental
- Davis Vision

SOC Reports

We asked R&B administrations for copies of the SOC report provided by each of the companies referenced above and the contract executed between the companies and M-DCPS

to determine whether there is an administrative or Third Party Administrator (TPA) service relationship and the need for a SOC report to be obtained by the school district¹⁴. A copy of the Cigna and FBMC contracts was provided by R&B. We reviewed the contracts and determined that these two companies provide administrative services for M-DCPS, which categorizes them as TPAs and therefore, M-DCPS obtaining a SOC 2 report from each would be vital in demonstrating HIPAA compliance related to security and privacy for the outsourced functions.

R&B administration indicated to us that they currently only require Cigna and Gallagher Bassett (GB)¹⁵ to submit a SOC 1 report annually, which is also provided to the external auditors during their audit of M-DCPS’ financial statements. Copies of these reports were provided to us, along with the corresponding Bridge/Gap letters for interim reporting. R&B also indicated that they have not requested SOC 2 reports from any of the aforementioned companies (See table below). However, they indicated that going forward, R&B will require all TPAs and insurance vendors to provide a SOC 1 report.

Companies	Report Type	
	SOC 1	SOC 2
Cigna	✓	X
FBMC	X	X
United Healthcare - Dental/Vision	NA	NA
Delta Dental	NA	NA
Davis Vision	NA	NA
Gallagher Bassett (GB) *	✓	X

✓ = Provided by vendor

X = Not provided by vendor

NA = Not Applicable; vendor is not a TPA

* = Not audited - outside of scope

¹⁴ According to the American Institute of Certified Public Accountants (AICPA), SOC 1, 2 and 3 reports are designed to provide transparency around the internal controls of service organizations’ (organizations that operate information systems and provide information system services to other entities) information systems and to help build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant. The types of report and their purpose are as follows:

- **SOC 1** – A report on controls at a service organization relevant to the user organization’s financial reporting.
- **SOC 2** – A report to evaluate a service organization’s information system relevant to security, availability, processing integrity, confidentiality, or privacy.
- **SOC 3** – A report similar to SOC 2, but does not detail the testing performed and is meant to be used as marketing material.

There are two types of SOC 1 and 2 reports: Type 1, reports on management’s description of a service organization’s system and the suitability of the design of controls; and Type 2, reports on management’s description of a service organization’s system and the suitability of the design and operating effectiveness of controls.

¹⁵ GB handles Workers’ Compensation claims management and is outside the scope of our audit.

A SOC 2, Type 2 report provides assurance on the description, suitability of design, and operating effectiveness of a TPA’s information systems relevant to security, confidentiality, availability, processing integrity, and privacy. Since the District entrusts sensitive information, including PHI and PII, to TPAs, it is essential to have a level of assurance that such information will be handled with proper care.

SOC Report Comparison

	Who Are the Users	Why	What
SOC 1®	Users’ controller’s office and user auditors	Audits of f/s Controls	relevant to user financial reporting
SOC 2®	Management Regulators Others	GRC programs Oversight Due diligence	Concerns regarding security, availability, processing integrity, confidentiality or privacy
SOC 3®	Any users with need for confidence in service organization’s controls	Marketing purposes; detail not needed	Easy-to-read report on controls

Source: AICPA

No Service Contract or Agreement

As stated previously, we requested copies of the contracts between M-DCPS and the companies (United Healthcare, Delta Dental, and Davis Vision) providing dental and vision insurance to District employees. R&B indicated that M-DCPS does not have a contractual agreement with these vendors since they only sell insurance products and provide a benefit to District employees. Instead, R&B provided a Request for Proposal (RFP), which shows the scope of work, expectations, and requirements from vendors offering dental and vision benefit plans to District employees. The RFP indicates that assistance for dental and vision benefits to District employees entails the convenience of having in-house services such as claims data inquiry, customer service, and verification of employee coverage. The results of the RFP were presented to the School Board, however, we did not receive any documentation to indicate that further actions to establish a contractual relationship between M-DCPS and the respondents selected to provide benefits to the District’s employees and retirees had occurred.

Additional inquiries of the School Board Attorney’s Office revealed that the said RFP was processed, but a written contract or agreement was not executed. According to management, the relationship between M-DCPS and the subject companies are governed by the companies’ responses to the RFP.

Although this matter does not specifically relate to the scope of our audit, determining the adequacy of internal controls and safeguards to assure the District's compliance with HIPAA Privacy Rule and IDEA Confidentiality requirements and protecting PHI or PII, it is an otherwise important control deficiency and should be addressed.

RECOMMENDATIONS:

7.1 To strengthen its safeguards over PHI and PII, we recommend the District require all Service Organizations providing health benefit administrative services to M-DCPS to submit SOC 1 and SOC 2 reports to R&B. This will provide assurance that the TPAs used by the District: 1) possess the necessary internal controls on their information systems to prevent financial misstatements and 2) provide the appropriate level of security, availability, processing integrity, confidentiality, and privacy of sensitive information.

Responsible Department: Office of Risk and Benefits Management

Management Response: *The Office of Risk and Benefits management will request the existing third party service administrators to voluntarily furnish SOC 2, type 2, audit reports for the duration of their existing bid periods and will include this requirement in future request for proposals (RFP) to incorporate them in the contracts.*

7.2 The District administration should execute contracts with all vendors providing healthcare services to District employees.

Responsible Department: Office of Risk and Benefits Management

Management Response: *The Office of Risk and Benefits Management is in the process of finalizing and executing all pending contracts.*

APPENDIX A: SUMMARY OF THE COMPLETENESS OF R&B'S POLICY TO ENSURE COMPLIANCE WITH THE RELEVANT REQUIREMENTS OF THE HIPAA PRIVACY RULE

Rule Section	Rule Description	Contained in R&B Policy		Remarks
		Yes	No	
Subpart E—Privacy of Individually Identifiable Health Information				
§ 164.530	Administrative requirements.			
§ 164.530(a)(1)	<p><i>Standard: Personnel designations.</i> (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.</p> <p>(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by §164.520.</p>	✓	✓	R&B policy manual does not designate a person to receive complaints. See Finding No. 4.
§ 164.530(2)	<i>Implementation specification: Personnel designations.</i> A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.	✓		
§ 164.530(b)(1)	<i>Standard: Training.</i> A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.		✓	R&B staff members queried stated that they received training on the handling of PHI & PII; however, training program is not contained

APPENDIX A: SUMMARY OF THE COMPLETENESS OF R&B'S POLICY TO ENSURE COMPLIANCE WITH THE RELEVANT REQUIREMENTS OF THE HIPAA PRIVACY RULE

Rule Section	Rule Description	Contained in R&B Policy		Remarks
		Yes	No	
				in R&B policy manual. See Finding No. 4.
§ 164.530(b)(2)(ii)	<i>Implementation specifications: Training.</i> A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.		✓	Training of R&B staff is not documented. See Finding No. 3.
§ 164.530(c)(1)	<i>Standard: Safeguards.</i> A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.	✓		
§ 164.530(2)(i)	<i>Implementation specification: Safeguards.</i> A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.	✓		
§ 164.530(2)(ii)	A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.	✓		
§ 164.530(d)(1) and (2)	<i>Standard: Complaints to the covered entity.</i> A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of		✓	R&B policy manual does not contain a complaint process. Neither was the required process found

APPENDIX A: SUMMARY OF THE COMPLETENESS OF R&B'S POLICY TO ENSURE COMPLIANCE WITH THE RELEVANT REQUIREMENTS OF THE HIPAA PRIVACY RULE

Rule Section	Rule Description	Contained in R&B Policy		Remarks
		Yes	No	
	<p>this subpart.</p> <p>(2) <i>Implementation specification:</i> Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.</p>		✓	<p>elsewhere in District policy. See Finding No. 4.</p> <p>A process to document complaints is not in place. See Finding No. 4.</p>
§ 164.530(e)(1)	<p><i>Standard: Sanctions.</i> A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart...</p>		✓	<p>R&B policy manual does not address this standard. School Board policies authorizing the development and implementation of HIPPA privacy policy, 1419.01, 3419.01, and 4419.01 indemnifies the R&BO for monetary civil penalties imposed for violating the HIPAA Privacy and Security Rules. The District's anti-fraud policy,</p>

APPENDIX A: SUMMARY OF THE COMPLETENESS OF R&B'S POLICY TO ENSURE COMPLIANCE WITH THE RELEVANT REQUIREMENTS OF THE HIPAA PRIVACY RULE

Rule Section	Rule Description	Contained in R&B Policy		Remarks
		Yes	No	
				8700, imposes sanction on employees who disclose confidential information. See Finding No. 4.
§ 164.530(e)(2)	<i>Implementation specification: Documentation.</i> As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.	N/A	N/A	Refer to preceding remark and Finding No. 4.
§ 164.530(f)	<i>Standard: Mitigation.</i> A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.		✓	R&B policy manual does not address mitigation strategy. School Board Policy 8351 provides mitigation for breach of electronic PHI cover under the HIPAA Security Rule. See Finding No. 4.
§ 164.530(g)	<i>Standard: Refraining from intimidating or retaliatory acts.</i> A covered entity— (1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any		✓	R&B policy manual does not address this standard. See Finding No. 4.

APPENDIX A: SUMMARY OF THE COMPLETENESS OF R&B'S POLICY TO ENSURE COMPLIANCE WITH THE RELEVANT REQUIREMENTS OF THE HIPAA PRIVACY RULE

Rule Section	Rule Description	Contained in R&B Policy		Remarks
		Yes	No	
	process provided for by this subpart, including the filing of a complaint under this section...			
§ 164.530(h)	<i>Standard: Waiver of rights.</i> A covered entity may not require individuals to waive their rights under §160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.		✓	R&B policy manual does not address this standard. See Finding No. 4.
§ 164.530(i)(1)	<i>Standard: Policies and procedures.</i> 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...	✓		
§ 164.530(2)	<i>Standard: Changes to policies or procedures.</i> (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart...	✓		
§ 164.530(3)	<i>Implementation specification: Changes in law.</i> Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure.	✓		

APPENDIX A: SUMMARY OF THE COMPLETENESS OF R&B'S POLICY TO ENSURE COMPLIANCE WITH THE RELEVANT REQUIREMENTS OF THE HIPAA PRIVACY RULE

Rule Section	Rule Description	Contained in R&B Policy		Remarks
		Yes	No	
§ 164.530(j)(1)	<p><i>Standard: Documentation.</i> A covered entity must: (i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;</p> <p>(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and</p> <p>(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.</p>	✓	✓	Action such as training provided to staff members is not documented, as required. See Finding No. 3.
§ 164.530(j)(2)	<p><i>Implementation specification: Retention period.</i> A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.</p>	✓	✓	R&B policy manual does not address this implementation specification. See Finding No. 4.

APPENDIX B: SUMMARY OF COMPLIANCE WITH RELEVANT IDEA CONFIDENTIALITY REQUIREMENTS

Rule Section	Rule Description	Compliant		Remarks
		Yes	No	
Confidentiality of Information				
§ 300.613(a)	Access rights. Each participating agency must permit parents to inspect and review any education records relating to their children that are collected, maintained, or used by the agency under this part...	✓		
§ 300.614	Record of access. Each participating agency must keep a record of parties obtaining access to education records collected, maintained, or used under Part B of the Act (except access by parents and authorized employees of the participating agency), including the name of the party, the date access was given, and the purpose for which the party is authorized to use the records.		✓	See Finding No. 2.
§ 300.622(a)	Consent. Parental consent must be obtained before personally identifiable information is disclosed to parties, other than officials of participating agencies in accordance with paragraph (b)(1) of this section, unless the information is contained in education records, and the disclosure is authorized without parental consent under 34 CFR part 99.	✓		
§ 300.623(a)	Safeguards. Each participating agency must protect the confidentiality of personally identifiable information at collection, storage, disclosure, and destruction stages.	✓		

APPENDIX B: SUMMARY OF COMPLIANCE WITH RELEVANT IDEA CONFIDENTIALITY REQUIREMENTS

Rule Section	Rule Description	Compliant		Remarks
		Yes	No	
§ 300.623(b)	Safeguards. One official at each participating agency must assume responsibility for ensuring the confidentiality of any personally identifiable information.	✓		
§ 300.623(c)	Safeguards. All persons collecting or using personally identifiable information must receive training or instruction regarding the State’s policies and procedures under §300.123 and 34 CFR part 99.		✓	Training is provided to school registrars. ESE staff handling PII at a Specialized Center did not receive training. See Finding No. 1.
§ 300.623(d)	Safeguards. Each participating agency must maintain, for public inspection, a current listing of the names and positions of those employees within the agency who may have access to personally identifiable information.		✓	See Finding No. 2.
§ 300.624(a)	Destruction of information. The public agency must inform parents when personally identifiable information collected, maintained, or used under this part is no longer needed to provide educational services to the child.	✓		

MANAGEMENT'S RESPONSE

Miami-Dade Schools Police Department

MEMORANDUM

IAM/2016-17#183
December 20, 2016
IAM/305-757-7708

TO: Trevor Williams, Assistant Chief Auditor
Office of Management and Compliance Audits


FROM: Ian Moffett, Chief of Police
Miami-Dade Schools Police Department

SUBJECT: ADMINISTRATIVE RESPONSE – AUDIT OF ESE & ESE RISK BENEFITS (IDEA & HIPAA) COMPLIANCE

This memorandum serves as a response to the relevant findings in the Audit of ESE & Risk Benefits (IDEA & HIPAA) Compliance. Miami-Dade Schools Police Department (MDSPD) has taken corrective action by way of removing a link from Miami-Dade Schools Police (MDSPD) website that included a vendor that sells various products for identity/credit protection that might have incorrectly lead the user to assume that Miami-Dade County Public Schools recommended or endorsed the products.

MDSPD has also provided the Office of Management and Compliance with a Public Service Announcement (PSA) script with the goal of providing information to parents regarding how to reduce the possibility their child may become a victim of identity theft. The script was also shared with Ms. Daisy Gonzalez Diego, Chief Communications Officer. The PSA is in the process of being filmed and edited and will be found on the MDSPD website by January 21, 2017. MDSPD recently hired part time hourly staff to conduct such functions since we did not previously possess the personnel nor resources to produce this item. Once completed, a link to the video will be provided to the Office of Management and Compliance Audits.


IAM/caf

School Operations

MEMORANDUM

February 8, 2017

TO: Jose Montes de Oca, Chief Auditor
Office of Management and Compliance Audits

FROM: Valtena G. Brown, Deputy Superintendent/Chief Operating Officer 
School Operations

SUBJECT: **SCHOOL OPERATIONS RESPONSE TO AUDIT OF ESE & RISK BENEFITS (IDEA & HIPAA) COMPLIANCE**

School Operations has reviewed the audit exceptions cited in the 2016-2017 fiscal year audit report of the audit of ESE and Risk Benefits (IDEA & HIPAA) compliance report. The following preventive actions will be taken through School Operations for the following recommendations:

RECOMMENDATIONS:

2.1 To limit the exposure to unauthorized use or disclosure of sensitive information, including PII and PHI, we recommend school-site administrators ensure that the periodic review of student records, required by the guidance contained in the Student Educational Records manual, be diligently performed and:

- a) Information deemed to be no longer needed to provide services to students be recommended for disposed, pursuant FERPA guidelines.
- b) Images of students' and parents' Social Security cards are not kept in the student cumulative file. Images of parents' Social Security cards found on file should be immediately destroyed. Images of students' Social Security cards found on file should be destroyed after the number is verified to be correct in the District Student Information system.
- c) A Record of Access Card is kept on file for every student cumulative file.

A Weekly Briefing was disseminated outlining Board Policy 8330 Student Records and notifying Principals that Social Security Cards are not to be duplicated or filed in students' cumulative files pursuant FERPA guidelines.

Additionally, Principals instructed registrars to review all cumulative files and remove and destroy all images of students and parent Social Security cards in accordance to FERPA guidelines.

Lastly, School Operations instructed all Principals identify a designee to review all Cumulative Records for information deemed to be no longer needed to provide services to students be disposed, pursuant to FERPA guidelines.

2.2 To ensure full compliance with FERPA, the District should develop a common, uniform notice containing all required elements for annually notifying parents or eligible students of their rights to inspect and review students' educational records. The District may determine an appropriate means of providing this notice.

School Operations will provide a universal Student/Parent Handbook that provides all of the required elements to promote a positive school climate. Included in the Parent/Student Handbook will be annual notification to parents on their rights to inspect and review

students' educational records in accordance with The Family Educational Rights and Privacy Act (FERPA).

2.3 District administration should implement the necessary safeguards to comply with IDEA 330.623(d) of maintaining a current listing of the names and positions of those District employees who may have access to personally identifiable information for public inspection.

School Operations directed Principals to maintain a current listing of the names and positions of those employees who may have access to personally identifiable information for public inspection. The lists will be maintained at the school and respective Region. School will update as necessary and submit revisions on an annual basis to their Region.

If you have any questions, please contact me at 305 995-2938.

VGB:cg
M084

cc:
Region Superintendents
Ms. Cynthia Gracia
Region Directors

Office of Risk and Benefits Management

MEMORANDUM

January 11, 2017

TO: Mr. Jose Montes de Oca, Chief Auditor
Management Audits

FROM: Judith M. Marte, Chief Financial Officer
Financial Services

BY: Michael G. Fox, Risk and Benefits Officer
Risk and Benefits Management



2017 JAN 12 AM 8:47
MANAGEMENT AND
OPERATIONS AUDITS

SUBJECT: AUDIT OF ESE & RISK BENEFIT (IDEA & HIPAA) COMPLIANCE

Following are the administration's responses to the Audit of ESE & Risk Benefit (IDEA & HIPAA) Compliance:

2. EXTENSIVE SAFEGUARDS TO PROTECT CONFIDENTIAL STUDENT INFORMATION ARE IN PLACE, BUT ADDITIONAL MEASURES ARE NEEDED TO LIMIT EXPOSURE OF STUDENT'S, EMPLOYEE'S AND RETIREE'S SENSITIVE INFORMATION

2.4 MANAGEMENT'S RESPONSE

The Office of Risk and Benefits Management required all employees to complete an accredited, two part HIPAA training in September 2016. The training covered HIPAA Privacy for Covered Entities, and HIPAA Information Security Standards as of 2016. The Office's vendors are also required by RFP and contract to provide HIPAA training to all their employees. The Office's leadership team performed a HIPAA Compliance walkthrough in October 2016, which identified opportunities for improvement. Moving forward, random unannounced information security reviews will be performed to assure that the appropriate practices are consistently followed.

The Office of Risk and Benefits Management will review several office layout options and related costs to improve the physical security of the general work area. Until the Office is moved to its permanent location, these options, including the purchase of individual cubical type accommodations will be carefully evaluated. The Office is also evaluating an electronic filing system in an effort to reduce the amount of paper records.

3. THE EXTENT AND NATURE OF TRAINING IN THE HANDLING AND SAFEGUARDING OF PII AND PHI R&B STAFF RECEIVES IS INSUFFICIENTLY DOCUMENTED

3.1 MANAGEMENT'S RESPONSE

The Office's written documentation of training provided to all Risk Management employees which was completed in September 2016, is available upon request. Risk and Benefits Management believes documentation to be sufficient, but guidance from the Office of Management Audits is welcome.

4. R&B POLICIES AND PROCEDURES CAN BE STRENGTHENED TO ADDRESS THE REQUIREMENTS OF THE HIPAA PRIVACY RULE

4.1 MANAGEMENT'S RESPONSE

In addition to the existing HIPAA Privacy and Security Policy, the Office will develop a HIPAA Privacy and Security Employee Handbook to address the issues identified in Appendix A.

6. INFORMATION SYSTEM'S ACCESS PROTOCOL CAN BE STRENGTHENED TO PREVENT EXPOSURE OF PII AND PHI

6.1 MANAGEMENT'S RESPONSE

The District's enrollment process requires that employees log-off after completing their open enrollment, to prevent exposing PHI and PII information. The Office will work with ITS and the Board's third party administrators to evaluate additional security enhancing options that are available to the District. To further minimize risks, the District has purchased cyber liability coverage with coverage limits of \$10 million per claim/annual aggregate subject to a \$250,000 self-insured retention.

7. SERVICE ORGANIZATION REPORT RELEVANT TO SECURITY, CONFIDENTIALITY, AND PRIVACY SHOULD BE OBTAINED FROM SOME VENDORS PROVIDING HEALTHCARE SERVICES AND CONTRACTS SHOULD BE IN PLACE FOR ALL HEALTHCARE VENDORS

7.1 MANAGEMENT'S RESPONSE

The Office of Risk and Benefits management will request the existing third party service administrators to voluntarily furnish SOC 2, type 2, audit reports for the duration of their existing bid periods and will include this requirement in future request for proposals (RFP) to incorporate them in the contracts.

7.2 MANAGEMENT'S RESPONSE

The Office of Risk and Benefits Management is in the process of finalizing and executing all pending contracts.

Any questions should be directed to Mrs. Judith M. Marte, Chief Financial Officer, Financial Services, at 305 995-1958, or Mr. Michael G. Fox, Risk and Benefits Officer, Office of Risk and Benefits Management, at 305 995-7155.

JMM:mgf
M041

Information Technology Services



Miami-Dade County Public Schools

giving our students the world

Superintendent of Schools
Alberto M. Carvalho

Miami-Dade County School Board

Dr. Lawrence S. Feldman, Chair
Dr. Marta Pérez, Vice Chair
Dr. Dorothy Bendross-Mindingall
Susie V. Castillo
Dr. Steve Gallon III
Perla Tabares Hantman
Dr. Martin Karp
Lubby Navarro
Mari Tere Rojas

February 2, 2017

Mr. Jose Montes de Oca, Chief Auditor
Office of Management and Compliance Audits
1450 N.E. 2 Avenue, Room 415
Miami, FL 33132

2017 FEB - 2 AM 10: 29
MANAGEMENT AND
COMPLIANCE AUDITS

Dear Mr. Montes de Oca:

Below are the Office of Academics and Transformation's management responses regarding the findings and recommendations stemming from the Audit of ESE & Risk Benefits (IDEA & HIPAA) Compliance.

If you have any questions, please contact Ms. Marie Izquierdo, Chief Academic Officer, Office of Academics and Transformation, at 305 995-1451, or Ms. Deborah Karcher, Chief Information Officer, Division of Information Technology Services, at 305 995-3750.

Sincerely,

Marie Izquierdo, Chief Academic Officer
Office of Academics and Transformation

MI:kh
L045

cc: Ms. Deborah Karcher

School Board Administration Building • 1450 N.E. 2nd Avenue • Miami, Florida 33132
305-995-1000 • www.dadeschools.net

Audit of ESE & Risk Benefits (IDEA) & HIPAA) Compliance
Office of Academics and Transformation
Management Responses

5.1 In order to document compliance with the actions required by the District's Network Security Standard, as part of the data removal policy, we recommend that:

a) The NSS be revised to specifically require the degaussing or removal and destruction of computer and copier hard drives be properly documented before these equipment are disposed.

Responsible Department: Information Technology Services

Management Response:

The NSS has been revised to include language that addresses this recommendation. The revisions are currently going through the approval process.

5.2 We recommend that property disposal procedures for technical equipment require a final inspection to confirm that all data is removed/degaussed from hard drives. This process would be independent from the degaussing process and will ensure the removal of data from computer hard drives. This is a necessary step to verify that confidential data are not released.

Responsible Department: Information Technology Services

Management Response:

The school site administrator will request, through our Incident Management System (HEAT), the degaussing of device(s). The completed HEAT ticket will notify the requester when this action is completed. The HEAT ticket number should be referenced on FM 1670 to show the degaussing is complete. A Weekly Briefing will be sent explaining this process.

6.2 ITS should analyze the condition further and implement reasonable solutions that will eliminate the existing risk.

Responsible Department: Information Technology Services

Management Response:

Currently, all users are automatically logged off applications after 20 minutes. In addition, Section 5.1.3 of the Network Security Standards states the following: "Users are responsible for all activity associated with their user-id. When a user is finished using a computer or will be leaving the computer unattended, they must log off or lock the computer (CTRL-ALT-DELETE, Lock Computer) to prevent their account from being compromised. This is particularly important for teachers – leaving their account open on

the computer may provide students and other unauthorized users with access to their grade book, e-mail account, personal information on the District Portal, and other sensitive/confidential applications and data (see 4.1.1.10).” However, in addition to the above-mentioned best practices, ITS has developed a solution that will log users out of SAP when they close the browser. This solution is scheduled to be implemented in early February 2017. ITS will continue to watch for any new risks.

Office of the Controller

Connie Pou
Controller
Suite 664
Tel. 995-2001

Daisy Naya
Assistant Controller
General Accounting
Suite 664
Tel. 995-2025

Odalis Garces
District Director
Payroll Department
Suite 614
Tel. 995-1641

Eric F. Ojeda
District Director
Accounts Payable
Suite 602
Tel. 995-1604

TO: Mr. Jose F. Montes de Oca,
Chief Auditor, Office of Management
and Compliance Audits

DATE: January 17, 2017

MEMO: CP-059

FROM: Connie Pou, C.P.A. *CP*
Controller

**SUBJECT: RESPONSE TO THE INTERNAL AUDIT REPORT – ESE & RISK
BENEFIT (IDEA & HIPAA) COMPLIANCE**

Attached is the response to the above mentioned audit report.

If you need further information, please do not hesitate to contact me at 305-995-2001.

CP:bjz

Attachment

cc: Mrs. Judith M. Marte
Mr. Trevor Williams

M
E
M
O
R
A
N
D
U
M



**INTERNAL AUDIT REPORT – ESE & RISK BENEFIT (IDEA & HIPAA)
COMPLIANCE**

RECOMMENDATIONS:

5.1 In order to document compliance with the actions required by the District's Network Security Standard, as part of the data removal policy, we recommend that:

- b) The Outgoing Controlled Equipment form (FM 1670) be modified to include a field to record the occurrence of this action.

RESPONSE:

The Office of the Controller will revise The Outgoing Controlled Equipment form (FM 1670) adding a field to denote that the hard drives have been removed or degaussed.

Anti-Discrimination Policy

Federal and State Laws

The School Board of Miami-Dade County, Florida adheres to a policy of nondiscrimination in employment and educational programs/activities and strives affirmatively to provide equal opportunity for all as required by:

Title VI of the Civil Rights Act of 1964 - prohibits discrimination on the basis of race, color, religion, or national origin.

Title VII of the Civil Rights Act of 1964 as amended - prohibits discrimination in employment on the basis of race, color, religion, gender, or national origin.

Title IX of the Education Amendments of 1972 - prohibits discrimination on the basis of gender.

Age Discrimination in Employment Act of 1967 (ADEA) as amended - prohibits discrimination on the basis of age with respect to individuals who are at least 40.

The Equal Pay Act of 1963 as amended - prohibits gender discrimination in payment of wages to women and men performing substantially equal work in the same establishment.

Section 504 of the Rehabilitation Act of 1973 - prohibits discrimination against the disabled.

Americans with Disabilities Act of 1990 (ADA) - prohibits discrimination against individuals with disabilities in employment, public service, public accommodations and telecommunications.

The Family and Medical Leave Act of 1993 (FMLA) - requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to "eligible" employees for certain family and medical reasons.

The Pregnancy Discrimination Act of 1978 - prohibits discrimination in employment on the basis of pregnancy, childbirth, or related medical conditions.

Florida Educational Equity Act (FEEA) - prohibits discrimination on the basis of race, gender, national origin, marital status, or handicap against a student or employee.

Florida Civil Rights Act of 1992 - secures for all individuals within the state freedom from discrimination because of race, color, religion, sex, national origin, age, handicap, or marital status.

Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA) - prohibits discrimination against employees or applicants because of genetic information.

Boy Scouts of America Equal Access Act of 2002 – no public school shall deny equal access to, or a fair opportunity for groups to meet on school premises or in school facilities before or after school hours, or discriminate against any group officially affiliated with Boy Scouts of America or any other youth or community group listed in Title 36 (as a patriotic society).

Veterans are provided re-employment rights in accordance with P.L. 93-508 (Federal Law) and Section 295.07 (Florida Statutes), which stipulate categorical preferences for employment.

In Addition:

School Board Policies 1362, 3362, 4362, and 5517 - Prohibit harassment and/or discrimination against students, employees, or applicants on the basis of sex, race, color, ethnic or national origin, religion, marital status, disability, genetic information, age, political beliefs, sexual orientation, gender, gender identification, social and family background, linguistic preference, pregnancy, and any other legally prohibited basis. Retaliation for engaging in a protected activity is also prohibited.

INTERNAL AUDIT REPORT

**Audit of ESE & Risk Benefits (IDEA & HIPAA)
Compliance**



MIAMI-DADE COUNTY PUBLIC SCHOOLS
Office of Management and Compliance Audits
1450 N.E. 2nd Avenue, Room 415
Miami, Florida 33132
Telephone: (305)995-1318 ♦ Fax: (305)995-1331
<http://mca.dadeschools.net>
