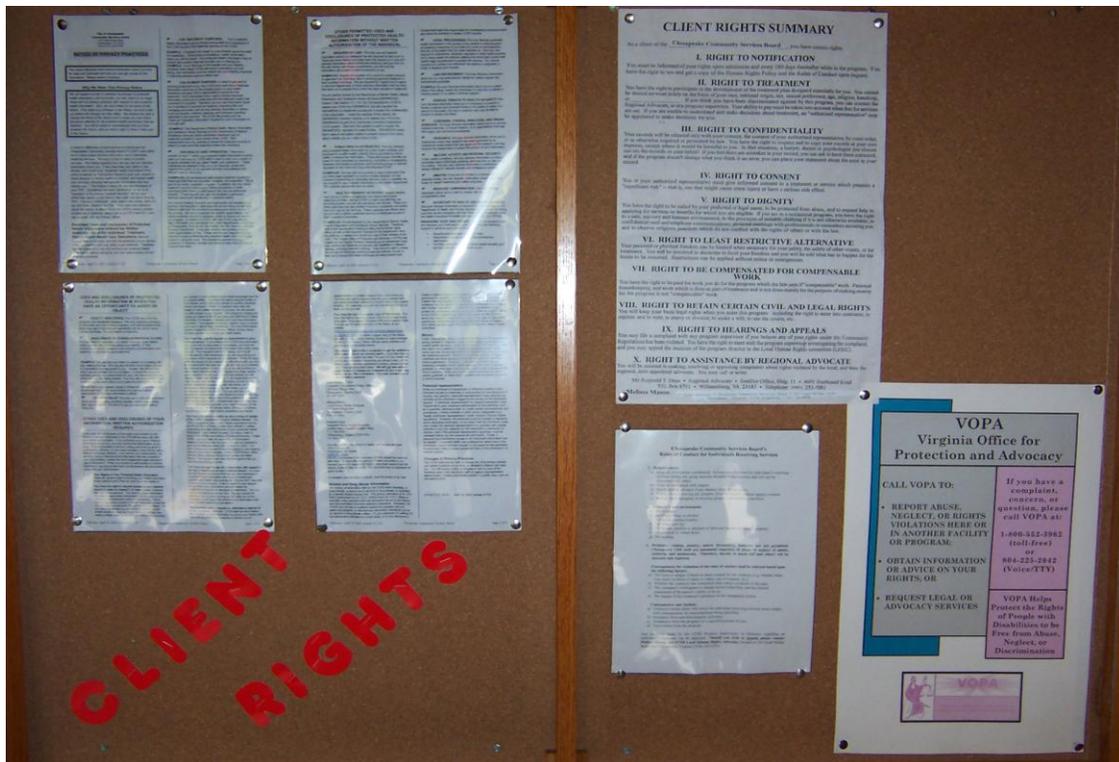


Chesapeake VIRGINIA

COMMUNITY SERVICES BOARD

PERFORMANCE AUDIT



FISCAL YEAR 2005

CITY OF CHESAPEAKE, VIRGINIA
AUDIT SERVICES DEPARTMENT

Audit Services Department
306 Cedar Road
P.O. Box 15225
Chesapeake, Virginia 23328
(757) 382-8511
Fax (757) 382-8860

September 15, 2005

The Honorable Dalton S. Edge and
Members of the City Council
City of Chesapeake
City Hall – 6th Floor
Chesapeake, Virginia 23328

Dear Mayor Edge and Members of the City Council:

We have completed our review of the Chesapeake Community Services Board (CCSB) for the period July 1, 2004 to June 30, 2005. Our review was conducted for the purpose of determining whether CCSB was in full compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and other policy and procedures requirements. The review was conducted in accordance with Government Auditing Standards and included such tests of records and other audit procedures as we deemed necessary in the circumstances.

CCSB provided comprehensive community-based services and support to Chesapeake residents with mental health, mental retardation, and/or substance abuse services needs. For FY 2005, CCSB had an operating budget of \$13,306,495 with over 150 full-time positions. CCSB funding sources included federal, state, and City funds, and client payments. CCSB must comply with applicable federal, state and City laws and regulations. One such federal law, HIPAA, was enacted in 1996 to improve the Medicare and Medicaid programs by encouraging the development of a health information system through the establishment of standards and requirements to facilitate the exchange, and to protect the privacy and security, of certain health information. Specifically, the U.S. Department of Health & Human Services issued and enforced the HIPAA regulations that required that covered entities, such as CCSB, meet transaction and code sets standards by October 16, 2002, privacy standards by April 14, 2003, and security standards by April 20, 2005.

Based on our review and analysis, we have determined that CCSB had made significant and substantial progress in implementing the comprehensive HIPAA standards. Specifically, CCSB had been very effective in meeting the requirements of HIPAA regulations concerning transactions and code sets and privacy of its clients' protected health information and had made substantial progress in meeting the HIPAA security standards. However, we did identify several areas that CCSB

needed to address to assure itself of HIPPA compliance. Specifically, CSSB needed to finalize Business Associate agreements with the Departments of Finance and Information Technology and with the City Treasurer. Also, the City had not developed a risk analysis methodology and written policies and procedures, and had not completed disaster recovery backup requirements to fully implement the HIPAA security standards.

This report, in draft, was provided to CCSB officials for review and response. Their comments have been considered in the preparation of this report. These comments have been included in the Managerial Summary, the Audit Report, and Appendix A. CCSB management and staffs were very helpful throughout the course of this audit, and we appreciate their courtesy and cooperation on this assignment.

Sincerely,

A handwritten signature in cursive script that reads "Jay Poole".

Jay Poole
City Auditor
City of Chesapeake, Virginia

C: Dr. Clarence V. Cuffee, City Manager
Candace Waller, Executive Director of Community Services Board

Managerial Summary

A. Objective, Scope, and Methodology

We have completed our review of the Chesapeake Community Services Board (CCSB) for the Fiscal Year (FY) 2005. Our review was conducted for the purpose of determining whether CCSB was in full compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and other policy and procedures requirements. The review was conducted in accordance with Government Auditing Standards and included such tests of records and other audit procedures as we deemed necessary in the circumstances.

CCSB provided comprehensive community-based services and support to Chesapeake residents with mental health, mental retardation, and/or substance abuse services needs. For FY 2005, CCSB had an operating budget of \$13,306,495 with over 150 full-time positions. CCSB funding sources included federal, state, and City funds, and client payments. CCSB must comply with applicable federal, state and City laws and regulations. One such federal law, HIPAA, was enacted in 1996 to improve the Medicare and Medicaid programs by encouraging the development of a health information system through the establishment of standards and requirements to facilitate the exchange, and to protect the privacy and security, of certain health information. Specifically, the U.S. Department of Health & Human Services issued and enforced the HIPAA regulations that required that covered entities, such as CCSB, meet transaction and code sets standards by October 16, 2002, privacy standards by April 14, 2003, and security standards by April 20, 2005.

To determine how well CCSB complied with the HIPAA requirements and standards relating to transactions and code sets, privacy, and security, we reviewed the federal law and corresponding regulations, state requirements, and CCSB policies and procedures. We discussed and documented information from CCSB management and staff and associated City department's officials that related to HIPAA privacy and security requirements. Also, we reviewed, analyzed, and obtained the status of CCSB implementation of report recommendations of KPMG's July 2004 Executive Summary entitled "City of Chesapeake, Fire and Community Services Departments, HIPAA Security Standards – Gap Analysis and Strategy Planning Engagement". In addition, we reviewed CCSB administrative and operational processes, documentation, and reports pertaining to quality assurance, reimbursement, budget, privacy, security, and client recordation.

We reviewed Quality Management Services chart review results and follow-up audits conducted in FY 2004 and 2005 to determine the quality of the reviews and the level of compliance with HIPAA standards and CCSB policy and procedures. In

addition, we judgmentally selected 5 of 10 supervisors in CCSB's mental health, mental retardation, and substance abuse programs and reviewed their FY 2005 audit results of staffs' client charts for compliance with HIPAA privacy and the related CCSB policy and procedures. Finally, we reviewed documentation to determine the status of CCSB implementing two recommendations presented in our June 2002 report entitled, "Service Practices of the Community Services Board, Preliminary Review".

Major Observations and Conclusions

Based on our review and analysis, we have determined that CCSB had made significant and substantial progress in implementing the comprehensive HIPAA standards. Specifically, CCSB had been very effective in meeting the requirements of HIPAA regulations concerning transactions and code sets and privacy of its clients' protected health information and had made substantial progress in meeting the HIPAA security standards. However, we did identify several areas that CCSB needed to address to assure itself of HIPAA compliance. Specifically, CCSB needed to finalize Business Associate agreements with the Departments of Finance and Information Technology and with the City Treasurer. Also, the City had not developed a risk analysis methodology and written policies and procedures, and had not completed disaster recovery backup requirements to fully implement the HIPAA security standards.

This report, in draft, was provided to CCSB officials for review and response. Their comments have been considered in the preparation of this report. These comments have been included in the Managerial Summary, the Audit Report, and Appendix A. CCSB management and staffs were very helpful throughout the course of this audit, and we appreciate their courtesy and cooperation on this assignment.

B. HIPAA Privacy and Security Issues

As previously noted, we have determined that CCSB had made significant and substantial progress in complying with the comprehensive HIPAA standards. Specifically, CCSB has been very effective in meeting the requirements of HIPAA regulations concerning transactions and code sets and privacy of its clients' protected health information. In addition, it has made substantial progress in meeting the HIPAA security standards. However, we did identify several areas that CCSB needed to address to assure itself of HIPAA compliance. Specifically, CCSB needed to finalize the Business Associate agreements with the Departments of Finance and Information Technology and with the City Treasurer. Also, the City had not developed a risk analysis methodology and written policies and procedures, and has not met disaster recovery backup requirements to fully implement the HIPAA security standards. (See additional details and analysis concerning the HIPAA security standards in Appendix B).

HIPAA Privacy Issues

1. Memorandum of Understanding with Business Associates

Finding – CCSB had not finalized a Memorandum of Understanding with three of its Business Associates - the Departments' of Finance and Information Technology and the City Treasurer – as required by HIPAA.

Recommendation – CCSB should seek approval of individual Memorandum of Understanding with the City's Departments' of Finance and Information Technology and with the City Treasurer as Business Associates.

Response - The Memorandums of Understanding with the Departments of Finance and Information Technology have been finalized and signed as of 8/31/05. The Deputy City Attorney is working with the City Treasurer's attorney to finalize this MOU, and we hope to have this completed within a month.

2. Quality Assurance Checklist

Finding - The Infant Intervention Service did not use the approved CCSB agency Quality Assurance Checklist when doing its supervisory audits of staffs' client charts.

Recommendation - CCSB should assure itself that all program supervisors use the approved Quality Assurance Review Checklist form when performing audits of staffs' client charts.

Response - The program supervisor for Infant Intervention Services has a completed quality assurance checklist that includes all the universal, standardized criteria of the agency including those individualized for the unique stream of funding received in that program area. Please see attached checklist. (*Audit Services did not include the checklist in this Report.*) During the annual audit of Infant Intervention Services, scheduled September 2005, the QA Office staff will assure that the program supervisor is utilizing the standardized section of the Quality Assurance Review Checklist.

HIPAA Security Issues

1. Risk Analysis Methodology

Finding – The City had not developed a risk analysis methodology to determine the risks and vulnerabilities to clients' electronic protected health information.

Recommendation - To ensure the safeguard of client's electronic protected health information, CCSB should assist the Department of Information Technology to expeditiously move towards completion of the outsourcing process for developing a risk analysis.

Response - As of 5/12/05, CCSB has not created a Risk Analysis methodology to determine the risks and vulnerabilities to electronic protected health information. Thus no documentation exists. Prior to May 2005 the City's Information Technology Department approved a Management Analyst position and was in the process of conducting interviews. The Analyst was to do the risk assessment to identify technical and non-technical threats and vulnerabilities to electronic protected health information. However, on 5/12/05, the CCSB MIS Administrator said that they would not hire a management analyst to do this work but would outsource the work regarding the creation, performance and documentation of a risk assessment during the next fiscal year (2006). In addition the outsourced company would implement a process to perform periodic updates to the risk analysis. The MIS Administrator indicated that they would follow the NIST guide exclusively to create the risk assessment. The RFP has been written to contract for the services of a Risk Manager. Once this position has been outsourced we will be able to move forward with the risk analysis and implement a risk methodology that will bring us into compliance with HIPAA.

2. Written Policies and Procedures

Finding – CCSB had not developed written policies and procedures for several administrative and physical safeguards concerning HIPAA security.

Recommendation – CCSB should establish written policies and procedures as required by the HIPAA security standards.

Response - Due to limited resources in funding and staff, have not been able to further develop and complete HIPAA security policies and procedures.

3. Disaster Recovery Plan Requirements

Finding – CCSB had not completed HIPAA disaster recovery plan requirements for electronic protected health information.

Recommendation – CCSB should work with the City to address its disaster recovery plan needs, hardware and software services, and identify a temporary alternate location.

Response - The CCSB by nature of services provided could continue to function and capture data on paper, the consumers charts are keep in paper mode thereby allowing the clinical staff to have access to pertinent data. Any long term lost of the computer resources in excess of two weeks would disable the CCSB's ability to bill its payers, and access to the City Financial System would not be available thereby restricting ability to properly pay employees. However if the disaster event is City wide, where emergency shelters are open, all clinical staff are required to man those sites so the CCSB would not be able to provide services to consumers until the shelter were closed. The CCSB MIS Administrator will meet with the City's Information Technology Communications Coordinator in late September 2005 to discuss a cooperative effort in the event of disaster.

CHESAPEAKE COMMUNITY SERVICES BOARD

PERFORMANCE AUDIT

FISCAL YEAR 2005

Table of Contents

<u>Contents</u>	<u>Page</u>
A. Objective, Scope, and Methodology	1
B. HIPAA Privacy and Security Issues	4
Appendix A – Responses from Chesapeake Community Services Board Officials	
Appendix B – HIPAA Security Standards, Gap Analysis and CCSB Status, as of June 30, 2005	

A. Objectives, Scope, and Methodology

We have completed our review of the Chesapeake Community Services Board (CCSB) for the Fiscal Year (FY) 2005. Our review was conducted for the purpose of determining whether CCSB was in full compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and other policy and procedures requirements. The review was conducted in accordance with Government Auditing Standards and included such tests of records and other audit procedures as we deemed necessary in the circumstances.

CCSB provided comprehensive community-based services and support to Chesapeake residents with mental health, mental retardation, and/or substance abuse services needs. CCSB services included 24 hour-a-day emergency services and outpatient services to mental health clients; mental retardation services including infant intervention and case management services; and vocational training; and substance abuse services including individual, group, and family counseling and treatment. CCSB was governed by a twelve-member community-based board appointed by the City Council. CCSB employed an Executive Director, an Assistant Director, and Fiscal, Quality Assurance, and Management Information Systems Administrators; Clinicians, Nurses, Counselors, and other medical specialists and support staff.

For FY 2005, CCSB had an operating budget of \$13,306,495 with over 150 full-time positions. CCSB funding sources included federal, state, and City funds, and client payments. CCSB must comply with applicable federal, state and City laws and regulations. One such federal law, HIPAA, was enacted in 1996 to improve the Medicare and Medicaid programs by encouraging the development of a health information system through the establishment of standards and requirements to facilitate the exchange, and to protect the privacy and security, of certain health information. Specifically, the U.S. Department of Health & Human Services issued and enforced the HIPAA regulations that required that covered entities, such as CCSB, meet transactions and code sets standards by October 16, 2002, privacy standards by April 14, 2003, and security standards by April 20, 2005.

Major Observations and Conclusions

Based on our review and analysis, we have determined that CCSB had made significant and substantial progress in implementing the comprehensive HIPAA standards. Specifically, CCSB had been very effective in meeting the requirements of HIPAA regulations concerning transactions and code sets and privacy of its clients' protected health information and had made substantial progress in meeting the HIPAA security standards. However, we did identify several areas that CCSB needed to address to assure itself of HIPAA compliance. Specifically, CCSB needed to finalize Business Associate agreements with the Departments of Finance and Information Technology and with the City Treasurer. Also, CCSB had not developed a risk analysis methodology and written policies and procedures, and had not completed disaster

recovery backup requirements to fully implement the HIPAA security standards. (See additional details and analysis concerning the HIPAA security standards in Appendix B).

This report, in draft, was provided to CCSB officials for review and response. Their comments have been considered in the preparation of this report. These comments have been included in the Managerial Summary, the Audit Report, and Appendix A. CCSB management and staffs were very helpful throughout the course of this audit, and we appreciate their courtesy and cooperation on this assignment.

Methodology

To determine how well CCSB complied with the HIPAA requirements and standards relating to transactions and code sets, privacy, and security, we reviewed the federal law and corresponding regulations, state requirements, and CCSB policies and procedures. We discussed and documented information from CCSB management and staff and associated City department's officials that related to HIPAA privacy and security requirements. Also, we reviewed, analyzed, and obtained the status of CCSB implementation of report recommendations of KPMG's July 2004 Executive Summary entitled "City of Chesapeake, Fire and Community Services Departments, HIPAA Security Standards – Gap Analysis and Strategy Planning Engagement". In addition, we reviewed CCSB administrative and operational processes, documentation, and reports pertaining to quality assurance, reimbursement, budget, privacy, security, and client recordation.

We reviewed Quality Management Services chart review results and follow-up audits conducted in FY 2004 and 2005 to determine the quality of the reviews and the level of compliance with HIPAA standards and CCSB policy and procedures. In addition, we judgmentally selected 5 of 10 supervisors in CCSB's mental health, mental retardation, and substance abuse programs and reviewed their FY 2005 audit results of staffs' client charts for compliance with HIPAA privacy and the related CCSB policy and procedures. Finally, we reviewed documentation to determine the status of CCSB implementing two recommendations presented in our June 2002 report entitled, "Service Practices of the Community Services Board, Preliminary Review".



Authorized staff accessing the Management Information System Center where electronic protected client health information was stored.



CCSB Chart Room where clients' charts were filed.

B. HIPAA Privacy and Security Issues

As previously noted, we have determined that CCSB had made significant and substantial progress in complying with the comprehensive HIPAA standards. Specifically, CCSB has been very effective in meeting the requirements of HIPAA regulations concerning transactions and code sets and privacy of its clients' protected health information. In addition, it has made substantial progress in meeting the HIPAA security standards. However, we did identify several areas that CCSB needed to address to assure itself of HIPAA compliance. Specifically, CCSB needed to finalize the Business Associate agreements with the Departments of Finance and Information Technology and with the City Treasurer. Also, CCSB had not developed a risk analysis methodology and written policies and procedures, and has not met disaster recovery backup requirements to fully implement the HIPAA security standards. (See additional details and analysis concerning the HIPAA security standards in Appendix B).

HIPAA Privacy Issues

1. Finding – CCSB had not finalized a Memorandum of Understanding with three of its Business Associates - the Departments' of Finance and Information Technology and the City Treasurer – as required by HIPAA.

The HIPAA Privacy Rules required that, if a “covered entity” such as CCSB had “business associates” that performed services on behalf of the “covered entity” and received protected health information about clients of the “covered entity” in the course of performing those services, the “covered entity” must enter into a written Business Associate Agreement in which the business associate agrees not to disclose the protected health information it received from the “covered entity” except to the extent permitted under the agreement, consistent with the business associate’s services on behalf of the “covered entity,” and then only as allowed under the HIPAA Privacy Rules. Further, if the “covered entity” and the “business associate” were governmental entities, the requirement for a Business Associate Agreement could be satisfied through a Memorandum of Understanding between the government entities. Without a Business Associate Agreement or a Memorandum of Understanding, the covered entity was not authorized under the HIPAA Privacy Rule to disclose protected health information to the Business Associate without the prior written authorization of the client.

However, CSSB had been successful in finalizing a number of Memorandums of Understanding with City departments and its vendors. The City’s Departments of Finance and Information Technology and the City Treasurer were Business Associates that had no approved Memorandum of Understanding with CCSB. The Finance Department’s Office of Risk Management (Risk Management) received information from CCSB about any incident occurring within CCSB, or involving CCSB clients that had the potential for creating a financial obligation or liability for CCSB. Risk Management was responsible for arranging for investigations of such incidents and contacting appropriate insurers and other parties to address and resolve actual and potential claims arising out of such incidents. In addition, from time to time CCSB may purchase services or

products for a client, resulting in the name of the client appearing on the purchasing documents from CCSB. Such purchasing documents were processed by the Finance Department on behalf of CCSB. In performing these duties on behalf of CCSB, the Finance Department performed the functions of a Business Associate.

The City's Information Technology department received protected health information on clients from CCSB that it submitted to the Virginia Department of Taxation for Debt Set-Off collection. The Department of Taxation for Debt Set-Off collects delinquent payments from income tax returns. CCSB's Management Information System department created a text file of clients that were to be submitted for Debt Set-Off collection. The text file contained protected health information including client's name, address, date of birth, social security number, and self-pay balance and balance to collect from the state. The file was created and downloaded from CCSB's BTI AS400 system to a CD and transported to the City's Information Technology Department for transmission along with other claim data from the city to the state.

Finally, the City Treasurer's Office staff entered data into the state system that allowed the use of the Set-Off Debt system. The previously mentioned client's protected health information had to be disclosed to the Treasurer by CCSB staff for this process to occur. The City Treasurer also had access to electronic fund transfers from payers to CCSB; e.g., Virginia Department of Medical Assistance Services, which include protected health information such as the client's social security number for payments on client accounts. Personal payments such as checks made on behalf of the client were also processed through the Treasurer's Office.

This situation occurred because the other departments had not yet returned the signed agreements. Without a Memorandum of Understanding between CCSB and the above three City entities, or prior written authorization from each client, CCSB was not authorized and was not fully compliant with the HIPAA Privacy Rule to disclose individual client protected health information.

Recommendation – CCSB should seek approval of individual Memorandum of Understanding with the City's Departments' of Finance and Information Technology and with the City Treasurer as Business Associates.

CCSB should expeditiously seek approval of a Memorandum of Understanding with the City's Departments' of Finance and Information Technology and with the City Treasurer as Business Associates. The Memorandum of Understanding would state that the Business Associate agreed not to disclose the protected health information it received from CCSB except to the extent permitted under the agreement, consistent with the Business Associate's services on behalf of CCSB. CCSB may wish to seek the assistance of the City Attorney's Office to obtain the Memorandum of Understanding.

Response - The Memorandums of Understanding with the Departments of Finance and Information Technology have been finalized and signed as of 8/31/05. The Deputy City Attorney is working with the City Treasurer's attorney to finalize this MOU, and we hope to have this completed within a month.

2. Finding - The Infant Intervention Service did not use the approved CCSB agency Quality Assurance Checklist when doing its supervisory audits of staffs' client charts.

CCSB Policy and Procedures for Quality Assurance required that program supervisors semiannually conduct audits of staffs' client charts in their program. The program supervisors utilized the criteria included in CCSB agency quality assurance audit checklist when doing their chart reviews. The checklist had several HIPAA criteria including an Accounting Log. Human Rights regulations (12VAC35-115-80©(3)) required that whenever confidential information was disclosed without a client's consent, CSSB was required to put in the client's service record an Accounting Log that included a written notation of: the information disclosed, the name of the person who received it, the purpose of the disclosure, and the date of the disclosure.

We reviewed the results of five program supervisors' audits of staffs' client charts including the audit performed by the Infant Intervention Service supervisor. Between July 1, 2004 and December 2004, the Infant Intervention Service supervisor did 19 quality assurance audits of her staffs' client charts. However, the chart review form used to perform and record the audit results was not the Quality Assurance Review form approved by Quality Assurance. The supervisor stated that the Quality Assurance Review form she used to perform the audits was revised to meet additional state program requirements and that the Accounting Log criteria was inadvertently omitted from the form. Because the audit did not include a review of the Accounting Log form in the client charts, CCSB has no assurance that the client charts had been properly documented for the Accounting Log criteria.

Recommendation - CCSB should assure itself that all program supervisors use the approved Quality Assurance Review Checklist form when performing audits of staffs' client charts.

To assure itself that client charts have the proper documentation, CCSB should restate the policy requirement that all program supervisors use the approved Quality Assurance Review Checklist form, including the Accounting Log criteria when performing audits of staffs' client charts. CCSB should continue to monitor the results of the supervisory reviews for HIPAA and policy compliance.

Response - The program supervisor for Infant Intervention Services has a completed quality assurance checklist that includes all the universal, standardized criteria of the agency including those individualized for the unique stream of funding received in that program area. Please see attached checklist. (*Audit Services did not include the checklist in this Report.*) During the annual audit of Infant Intervention Services, scheduled September 2005, the QA Office staff will assure that the program supervisor is utilizing the standardized section of the Quality Assurance Review Checklist.

HIPAA Security Issues

1. Finding – The City had not developed a risk analysis methodology to determine the risks and vulnerabilities to clients’ electronic protected health information.

Within HIPAA administrative safeguards, there was a requirement to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. This analysis was to result in the creation of a risk management plan to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

In FY 2005 the City developed a position description and attempted twice to hire a person to develop a risk analysis, and to direct its implementation and identification of policy and procedures needed to guide CCSB and Fire’s EMS HIPAA Security compliance as determined by the KPMG Gap Analysis. However, the interview panel could not identify a candidate that it deemed suitable. Thus, the position remained vacant. Subsequently, the HIPAA Oversight Committee leadership, which consisted of the Information Technology Director, CCSB Executive Director, and the Fire Chief, went with an alternate recommendation to develop an RFP to contract for these services.

Because a risk analysis had not been developed, CCSB had not implemented and documented a risk management plan that addressed security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. As a result, it also had not complied with HIPAA security standards. Although CCSB appeared to show reasonable diligence in attempting to meet HIPAA standards, CCSB needs to assure itself that it is expeditiously developing a risk analysis and will implement its results.

Recommendation - To ensure the safeguard of client’s electronic protected health information, CCSB should assist the Department of Information Technology to expeditiously move towards completion of the outsourcing process for developing a risk analysis.

The safeguard of client’s electronic protected health information has been a high priority for CCSB. Thus, CCSB should assist Information Technology in expeditiously moving towards completion of the outsourcing process for developing a risk analysis. From the result of the risk analysis, CCSB should implement and document an information security program that would include the following components: risk assessment/analysis, policy management, governance/compliance, security awareness and training, monitoring, incident response, and reporting.

Response - As of 5/12/05, CCSB has not created a Risk Analysis methodology to determine the risks and vulnerabilities to electronic protected health information. Thus, no documentation exists. Prior to May 2005, the City’s Information Technology Department approved a Management Analyst position and was in the

process of conducting interviews. The Analyst was to do the risk assessment to identify technical and non-technical threats and vulnerabilities to electronic protected health information. However, on 5/12/05, the CCSB MIS Administrator said that they would not hire a management analyst to do this work but would outsource the work regarding the creation, performance and documentation of a risk assessment during the next fiscal year (2006). In addition the outsourced company would implement a process to perform periodic updates to the risk analysis. The MIS Administrator indicated that they would follow the NIST guide exclusively to create the risk assessment. The RFP has been written to contract for the services of a Risk Manager. Once this position has been outsourced we will be able to move forward with the risk analysis and implement a risk methodology that will bring us into compliance with HIPAA.

2. Finding – CCSB had not developed written policies and procedures for several administrative and physical safeguards concerning HIPAA security.

HIPAA security safeguards required covered entities to write reasonable and appropriate policies and procedures to comply with the HIPAA standards that required preventing, detecting, containing, and correcting security violations; controlling physical access to its electronic information systems and facilities; and providing technical access only to those persons or software programs that have been granted access rights.

While CCSB had made significant progress in implementing administrative safeguards in workforce security, information access management and security awareness, it had not established written policies and procedures for many of these safeguards. Specifically, CCSB had not implemented policies and procedures to;

- ensure that all staff had appropriate access to electronic information,
- require approval authority,
- review staff access privileges for client's protected health information,
- respond in the event of notification of a new high-risk virus threat,
- control access to the new building,
- degauss hardware and magnetic tapes prior to re-use, and
- track the location of magnetic tapes that contain electronic protected health information.

CCSB was required to comply with HIPAA security standards by April 20, 2005. However, the significant staff time and money that was needed to implement and document these safeguards had delayed their completion. Without written policies and procedures in the above areas, CCSB could not assure that clients' electronic protected health information was not being compromised.

Recommendation – CCSB should establish written policies and procedures as required by the HIPAA security standards.

CCSB should establish written policies and procedures to comply with the HIPAA security standards. These policies and procedures should provide consistent direction and guidance to prevent, detect, contain, and correct security violations; control physical access to its electronic information systems and facilities; and provide technical access only to those persons or software programs that have been granted access rights.

Response - Due to limited resources in funding and staff, have not been able to further develop and complete HIPAA security policies and procedures.

3. Finding – CCSB had not completed HIPAA disaster recovery plan requirements for electronic protected health information.

The HIPAA Security regulations required that a contingency plan be established and implemented that included appropriate policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damaged systems that contain electronic protected health information. As part of CCSB disaster recovery plan for computer services, the plan relied on the movement of critical personnel and system applications to a selected alternate computer center site.

CCSB had a disaster recovery plan for its total operations and also an individual disaster recovery plan for its computer services. While CCSB computer services recovery plan stated that the essential business functions that were supported by computer services, if affected by a major disruption, would resume within 12 days after a disaster declaration and movement to the selected alternate computer center, CCSB has no designated alternate site for its critical business functions operations and its computer services. CCSB indicated that acquiring an alternate site with redundant systems would be very costly and was not being considered at this time.

We discussed whether there was an opportunity for CCSB to work with the City to acquire an alternate location and redundancy systems. CCSB indicated that there could be some benefit for establishing an alternate location with the City. However, CCSB used systems and applications that were generally different than the City. CCSB had different operating systems, software applications (AS400 and BTI), and e-mail systems than the City, although they use the City's financial system software.

Similarly, while the City had recognized the need for redundancy mainframe systems and servers, the City had not yet identified an alternate location or redundancy for its mainframe systems/applications and systems' servers located in the Information Technology building. Presently, there was no formal process ongoing to identify an alternate location or establish redundant systems for the City's computer functions. Finally the City's Information Technology Department indicated that it would coordinate closely with CCSB on any emergency operations/disaster recovery requirements associated with HIPAA security compliance.

As a substitute for an alternate site, the KPMG's Gap Analysis recommended that CCSB establish quick shipped vendor agreements for critical hardware and software services in case a major disruption occurred at the current computer services location. However, no vendor agreements have been initiated.

A major disruption in CCSB computer services could adversely impact or compromise client files that include electronic protected health information, telecommunications, network servers, e-mail, purchasing, accounts payable and receivable, payroll, and general ledger functions.

Recommendation – CCSB should work with the City to address its disaster recovery plan needs, hardware and software services, and identify a temporary alternate location.

An alternate location and redundancy of computer systems/applications for CCSB should be pursued in conjunction with the City and its need for a comparable facility. If budgetary constraints prevent the purchase of an alternate location with redundancy systems, CCSB should consider establishing quick shipped vendor agreements for critical computer hardware and software services and identify a temporary alternate location.

Response - The CCSB by nature of services provided could continue to function and capture data on paper, the consumers charts are keep in paper mode thereby allowing the clinical staff to have access to pertinent data. Any long term lost of the computer resources in excess of two weeks would disable the CCSB's ability to bill its payers, and access to the City Financial System would not be available thereby restricting ability to properly pay employees. However if the disaster event is City wide, where emergency shelters are open, all clinical staff are required to man those sites so the CCSB would not be able to provide services to consumers until the shelter were closed. The CCSB MIS Administrator will meet with the City's Information Technology Communications Coordinator in late September 2005 to discuss a cooperative effort in the event of disaster.

APPENDIX A

RESPONSE FROM CHESAPEAKE

COMMUNITY SERVICES BOARD

OFFICIALS

CHESAPEAKE COMMUNITY SERVICES BOARD RESPONSES for Fiscal Year 2005
PERFORMANCE AUDIT
Conducted by the City of Chesapeake Audit Services Department

B. HIPAA Privacy and Security Issues

HIPAA Privacy Issues

1. Memorandum of Understanding with Business Associates

Finding – CCSB had not finalized a Memorandum of Understanding with its Business Associates - the Departments' of Finance and Information Technology and the City Treasurer – as required by HIPAA.

Recommendation – CCSB should seek approval of individual Memorandum of Understanding with the City's Departments' of Finance and Information Technology and with the City Treasurer as Business Associates.

Response - The Memorandums of Understanding with the Departments of Finance and Information Technology have been finalized and signed as of 8/31/05. The Deputy City Attorney is working with the City Treasurer's attorney to finalize this MOU, and we hope to have this completed within a month.

2. Quality Assurance Checklist

Finding - The Infant Intervention Service did not use the approved CCSB agency Quality Assurance Checklist when doing its supervisory audits of staffs' client charts.

Recommendation - CCSB should assure itself that all program supervisors use the approved Quality Assurance Review Checklist form when performing audits of staffs' client charts.

Response - The program supervisor for Infant Intervention Services has a completed quality assurance checklist that includes all the universal, standardized criteria of the agency including those individualized for the unique stream of funding received in that program area. Please see attached checklist. (*Audit Services did not include the checklist in this Report.*) During the annual audit of Infant Intervention Services, scheduled September 2005, the QA Office staff will assure that the program supervisor is utilizing the standardized section of the Quality Assurance Review Checklist.

HIPAA Security Issues

1. Risk Analysis Methodology

Finding – CCSB had not developed a risk analysis methodology to determine the risks and vulnerabilities to clients' electronic protected health information.

Recommendation - To ensure the safeguard of client's electronic protected health information, CCSB should assist the Department of Information Technology to expeditiously move towards completion of the outsourcing process for developing a risk analysis.

Response - As of 5/12/05, CCSB has not created a Risk Analysis methodology to determine the risks and vulnerabilities to electronic protected health information. Thus no documentation exists. Prior to May 2005 the City's Information Technology Department approved a Management Analyst position and was in the process of conducting interviews. The Analyst was to do the risk assessment to identify technical and non-technical threats and vulnerabilities to electronic protected health information. However, on 5/12/05, the CCSB MIS Administrator said that they would not hire a management analyst to do this work but would outsource the work regarding the creation, performance and documentation of a risk assessment during the next fiscal year (2006). In addition the outsourced company would implement a process to perform periodic updates to the risk analysis. The MIS Administrator indicated that they would follow the NIST guide exclusively to create the risk assessment. The RFP has been written to contract for the services of a Risk Manager. Once this position has been outsourced we will be able to move forward with the risk analysis and implement a risk methodology that will bring us into compliance with HIPAA.

2. Written Policies and Procedures

Finding – CCSB had not developed written policies and procedures for several administrative and physical safeguards concerning HIPAA security.

Recommendation – CCSB should establish written policies and procedures as required by the HIPAA security standards.

Response - Due to limited resources in funding and staff, have not been able to further develop and complete HIPAA security policies and procedures.

3. Disaster Recovery Plan Requirements

Finding – CCSB had not completed HIPAA disaster recovery plan requirements for electronic protected health information.

Recommendation – CCSB should work with the City to address its disaster recovery plan needs, hardware and software services, and identify a temporary alternate location.

Response - The CCSB by nature of services provided could continue to function and capture data on paper, the consumers charts are kept in paper mode thereby allowing the clinical staff to have access to pertinent data. Any long term loss of the computer resources in excess of two weeks would disable the CCSB's ability to bill its payers, and access to the City Financial System would not be available thereby restricting ability to

properly pay employees. However, if the disaster event is City wide, where emergency shelters are open, all clinical staff are required to man those sites so the CCSB would not be able to provide services to consumers until the shelter were closed. The CCSB MIS Administrator will meet with the City's Information Technology Communications Coordinator in late September 2005 to discuss a cooperative effort in the event of disaster.

APPENDIX B

HIPAA SECURITY STANDARDS GAP ANALYSIS AND CCSB STATUS AS OF JUNE 2005

**HIPAA REGULATORY REQUIREMENTS
KPMG'S HIPAA SECURITY STANDARDS GAP ANALYSIS
CCSB RESPONSE AND STATUS
AS OF JUNE 2005**

ADMINISTRATIVE SAFEGUARDS

Security Management Process – 164.308(a)(1)(i) – Implement policies and procedures to prevent, detect, contain, and correct security violations.

A-1.1 Risk Analysis Gap (Required – High – Red)*: Although a policy that reserves CCSB's right to conduct periodic information security risk assessments has been implemented, a documented and standardized risk assessment methodology and process has not been established and/or adopted by CCSB.

KPMG Risk Analysis Recommendation: Adopt or create a standard risk analysis methodology (e.g., NIST Risk Management Guide for Information Technology System) should be used as a starting point and tailored to meet the needs of CCSB. Perform and document an initial Risk Analysis of threats and vulnerabilities (technical and non-technical) to electronic protected health information. Implement a process to perform periodic (e.g., annual) updates to the Risk Analysis based on changes in the technology environment.

Status: As of June 2005, CCSB has not developed a risk analysis methodology to determine the risks and vulnerabilities to electronic protected health information. Thus, no documentation exists. The City, in FY 2005, developed a position and attempted twice to hire a person to develop a risk analysis, and to direct its implementation and identification of policy and procedures needed to guide CCSB and Fire's EMS HIPAA Security compliance as determined by the KPMG Gap Analysis. However, the interview panel could not identify a candidate it deemed suitable. Thus, the HIPAA Committee, consisting of the Information Technology Director, CCSB Executive Director, and the Fire Chief did not hire anyone, but instead decided to write an RFP to outsource the work regarding the creation, performance and documentation of a risk assessment to identify technical and non-technical threats and vulnerabilities to electronic protected health information. The outsourcing process will be handled by the City's Department of Information Technology and would start at the beginning of FY 2006. In addition, the outsourced consultant would implement a process to perform periodic updates to the risk analysis. CCSB indicated that they would request that the winning bidder would follow the NIST guide exclusively to create the risk analysis.

A-1.2 Risk Management Gap (Required – High – Red): A formal documented security program, including additional policies, standards and guidelines does not exist. Information Technology personnel or end users handling electronic protected health information do not have an authoritative source to reference for security policy or procedural issues.

KPMG Risk Management Recommendation: Document and implement an information security program based on the results of Risk Analysis (A-1.1). At a minimum, the program should include the following components: Risk Assessment/Analysis, Policy Management, Governance/Compliance, Security Awareness and Training, Monitoring, Incident Response, and Reporting. Full time resources should be hired to develop and implement this program. Virtual teams should be utilized to assist with the technical aspects.

Status – CCSB has not done a risk analysis and thus has not documented and implemented an information security program based on the results of a risk analysis.

Assigned Security Responsibility – 164.308(a)(2) – Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

A-2.0 Assigned Security Responsibility Gap (Required – Medium – Yellow): Although the Information System Manager has been identified as CCSB's Security Official, this has not been indicated in a formal document describing the Security Officer's job description.

KPMG Assigned Security Responsibility Recommendation: Include in the job description for the IS Manager the functions of Disaster Recovery Planning coordination and Information Security (including the HIPAA Security Officer), such as: Risk Assessment/Analysis, Policy Management, Governance/Compliance, Security Awareness and Training, and Disaster Recovery Testing and Coordination. The Information System Manager is currently operating in a number of these capacities informally (e.g., she wrote the existing Disaster Recovery plan). An assessment of her capacity to handle any remaining tasks needs to be performed.

Status: The Executive Director has rewritten the job description to include the HIPAA Security Officer duties. However, the Executive Director has not yet forwarded the job description to Human Resources for approval, and thus the additional functions have not been finalized.

Workforce Security – 164.308(a)(3)(i) – Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

A-3.1 Authorization and/or Supervision Gap (Addressable – Medium – Red): An employee's supervisor approval is not obtained for granting access to computer resources, including the LAN, Lotus Notes, BTI/HHS and other specific applications containing electronic protected health information.

KPMG Authorization and/or Supervision Recommendation: Develop and implement a policy and process to capture authorization for access to electronic protected health information. An employee's supervisor should sign off either a hardcopy or email form before access to electronic protected health information is granted on the LAN, Lotus Notes, and/or BTI/HSS. The City's 'Computer User Account Request Form' should be leveraged to expedite the process and drive consistency between the two Information Technology groups.

Status: CCSB has implemented a Computer User Request form that must be filled out by the employee's supervisor before the user can be added to the LAN, AS400 and/or Lotus Notes systems. The form also specifies what type of access is needed. However, no written policy and procedures exist.

A-3.2 Workforce Clearance Procedures Gap (Addressable – Low – Yellow): Although role-based exists within Lotus Notes and BTI/HSS, the ability to access/inquire all electronic protected health information is currently granted to the majority individuals who have system access, regardless of business need, and is in conflict with the 'Need to Know' section in the *Information System Access Policy*.

KPMG Workforce Clearance Procedures Recommendation: Review access privileges for all user accounts for the LAN, Lotus Notes, and BTI/HSS. Restrict access privileges to the Lotus Notes, and BTI/HSS based on the business needs of users. The strategy for restricting access base on 'Need to Know' will be documented in a manner that is appropriate given the business requirements of CCSB system end users.

Status: CCSB has implemented a Computer User Request form that must be filled out by the employee's supervisor before the user can be added or removed from the system. The form also specifies what type of access is needed. However, no written policy and procedures exist.

A-3.3 Termination Procedures Gap (Addressable – Medium – Red): Documented procedures do not exist to ensure that all system and building access privileges that an employee was granted by CCSB are revoked upon termination.

KPMG Termination Procedures Recommendation: Document and implement procedures for end user groups to notify the Management Information System department for removal of access privileges upon employee termination or transfer. Forms and procedures from the access request process (see A-3.1) could be leveraged to expedite this issue and facilitate consistency/ease of use.

Status: CCSB has developed a Computer User Request form that must be filled out by the supervisor of the employee that was being terminated or transferred. The form must be provided to the Management Information System department for the employee's removal from the systems and building access privileges upon termination or transfer. However, no written policy and procedures exist.

Information Access Management – 164.308(a)(4)(i) – Implement policies and procedures for authorizing access to electronic protected health information that are consistent with subpart E of this part.

A-4.2 Access Authorization Gap (Addressable – Medium – Red): Approval of the employee's supervisor is not obtained for access authorization to computer resources, including the LAN, Lotus Notes, BTI/HSS and other specific application containing electronic protected health information.

KPMG Access Authorization Recommendation: Develop and implement a policy and process to capture authorization for access to electronic protected health information. An employee's supervisor should sign off either a hardcopy or email form before access to electronic protected health information, is granted on the LAN, Lotus Notes, and/or BTI/HSS. The City's 'Computer User Account Request Form' should be leveraged to expedite the process and drive consistency between the two IT groups.

Status: CCSB has implemented a Computer User Request form that must be filled out by the employee's supervisor before the user can be added or removed from the system. The form also specifies what type of access is needed. However, no written policy and procedures exist.

A-4.3 Access Establishment and Modification Gap (Addressable – Medium – Red): The approval of the employee's supervisor is not obtained for access authorization or modification. A formal policy and procedure to modify employee computer access rights does not exist.

KPMG Access Establishment and Modification Recommendation: Develop and implement a policy and process to capture authorization for access to electronic protected health information. An employee's supervisor should sign off either a hardcopy or email form before access to electronic protected health information, is granted on the LAN, Lotus Notes, and/or BTI/HSS. The City's 'Computer User Account Request Form' should be leveraged to expedite the process and drive consistency between the two Information Technology groups.

Status: As stated in A-4.2, CCSB has implemented a Computer User Request form that must be filled out by the employee's supervisor before the user can be added or removed from the system. The form also specifies what type of access is needed. However, no written policy and procedures exist.

Security Awareness and Training – 164.308(a)(5)(i) – Implement a security awareness and training program for all members of its workforce (including management).

A-5-1 Security Reminders Gap (Addressable – Low – Yellow): A formal security awareness program with periodic reminders for CCSB personnel does not exist.

KPMG Security Reminder Recommendation: Develop a formal security awareness presentation to educate new and existing employees, particularly to those who have access to electronic protected health information. Deliver half hour security presentation 'briefings' to the individual CCSB end user departments in department meetings or other appropriate forums. Topic of the presentation should include; 'Who We Are and What We Do' for Management Information System area of CCSB? Why Securing Information (particularly electronic protected health information) is Important? How End Users Can Contribute to a More Secure Environment? (e.g., use appropriate access request forms, don't use standard email confidential data, don't download software from the Internet, etc.), and What Resources are Available for Help" (e.g., policies, contact information, etc.) Provide access to information technology related policies and standards on the Intranet or similar means. Notify end user of current information technology security issues in quarterly broadcast emails. An internet or other electronic means for internal communication of CCSB business and/or Management Information System issues exists. 'Global' email distribution email distribution list exists to broadcast messages to the end user community. Opportunities to leverage future City Information Technology implementation exist.

Status: CCSB has received FY 2005 funds to purchase HIPAA Security Awareness Training courses.

A-5.2 Protection from Malicious Software Gap (Addressable – Low – Yellow): Documented procedures have not been developed to receive and act upon new and high-risk virus threats.

KPMG Protection from Malicious Software Recommendation: Develop response procedures in the event of notification of a new high-risk virus threat. (Additional details in A-6.1)

Status: CCSB has protection from malicious software and has approved funding to increase the protection of CCSB computer system. CCSB uses McAfee Antivirus and has a Policy Server that automatically updated each computer on CCSB network. However no written policy and procedures exist.

A-5.3 Log-in Monitoring Gap (Addressable – Low – Yellow): Application level audit logs, access reports, or security incident tracking reports are not generated nor reviewed on a regular basis in order to proactively detect unauthorized access to electronic protected health information. Upon initial logon to the LAN, a popup box notification does not exist notifying user that CCSB may monitor their computer use.

KPMG Log-in Monitoring Recommendation: Audit logging item addressed jointly with A-1.4. Develop a network level popup box that is pushed to end users upon initial log-in, notifying them that CCSB may monitor their computer use. The verbiage of the popup box that notifies users that the City may monitor computer use can be leveraged to expedite the process and drive consistency between the two Information Technology groups.

Status: This was implemented but, caused a major network failure, whereby the users lost the ability to log on to the system. It was disabled until the cause could be identified and a fix could be implemented. CCSB plans to open a service ticket with Microsoft, so that they can provide technical assistance with setting up a pop-up prior to logging on to the network.

Contingency Plan – 164.308(a)(7)(i) – Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrences (for example fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

A-7.2 Disaster Recovery Plan Gap (Required – Medium – Yellow): The *Disaster Recovery Plan for Computer Services* is partially reliant on an alternate computer center site, which has not been identified in the document.

KPMG Disaster Recovery Plan Recommendation: Evaluate, identify and consider alternate processing environment options (e.g., alternate buildings with excess capacity or vendor quick ship agreement, etc). Update disaster recovery plan with pertinent information. Perform testing procedures to ensure alternate processing functions are effectively working. Funding for alternate processing options is limited. Only the most critical systems will be recovered in the event of a disaster.

Status: CCSB has no alternate site identified due to infrastructure and budget constraints. CCSB could continue servicing clients; the clients charts are keep in paper mode thereby allowing the clinical staff to have access to pertinent data. However, any long term loss of the computer resources in excess of two weeks would disable CCSB's ability to bill its payers, prevent access the City's Financial System, and thus would restrict its ability to pay employees. However if the disaster event was City wide, where emergency shelters were open, all clinical staff would be required to man those sites so CCSB would not be able to provide services to its clients until the shelter were closed.

A-7.3 Emergency Mode Operations Plan Gap (Required – Medium – Yellow): Emergency mode operations are not documented in a disaster recovery/business continuity plan or any operational procedures.

KMPG Emergency Mode Operations Plan Recommendation: Evaluate, identify and consider alternate processing environment options (e.g., alternate buildings with excess capacity or vendor quick ship agreement, etc.) Update disaster recovery plan with pertinent information. Perform testing procedures to ensure alternate processing functions effectively. Funding for alternate processing options is limited. Only the most critical systems will be recovered in the event of a disaster.

Status: CCSB has no alternate site identified due to infrastructure and budget constraints. CCSB could continue servicing clients; the clients charts are keep in paper mode thereby allowing the clinical staff to have access to pertinent data. However, any long term loss of the computer resources in excess of two weeks would disable CCSB's

ability to bill its payers, prevent access the City's Financial System and thus would restrict its ability to pay employees. However, if the disaster event was City wide, where emergency shelters are open, all clinical staff would be required to man those sites so CCSB would not be able to provide services to its clients until the shelter were closed.

A-7.4 Test and Revision Procedures (Addressable – Low- Yellow): Documented procedures are not enforced.

KPMG Test and Revision Procedures Recommendation: This item addressed jointly with A-7.2 as follows; Evaluate, identify and consider alternate processing environment options (e.g., alternate buildings with excess capacity or vendor quick ship agreement, etc). Update disaster recovery plan with pertinent information. Perform testing procedures to ensure alternate processing functions effectively. Funding for alternate processing options is limited. Only the most critical systems will be recovered in the event of a disaster.

Status: This item was contingent on outsourcing for the development of a Risk Analysis.

A-7.5 Applications and Data Criticality Analysis (Addressable – Medium – Yellow): The criticality of applications is not reviewed on a periodic basis in support of CCSB's *Disaster Recovery Plan for computer Services*.

KPMG Application and Data Criticality Analysis Recommendation: Formalize the application criticality framework to include system owner input on the following topics to create a system ranking "score" (e.g., 1-3, 1 being most critical - recovered first, etc.): Data Sensitivity (e.g., electronic protected health information), Interdependencies on other systems, Recovery Time Objective, Recovery Point Objective. Identify system owners to assign criticality score and maintain criticality as changes are made to systems that could impact the criticality of the system. Assumptions – System owners can be identified for all appropriate environments. System owners become aware (through the Management Information System Manager) of their responsibility to periodically update the application criticality.

Status: This item is dependent on outsourcing the development of a Risk Analysis and Risk Management Program.

Business Associate Contracts and Other Arrangements – 164.308(b)(1) – A covered entity, in accordance with 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314(a) that the business associate will appropriately safeguard the information.

A-9.1 Written Contract or Other Arrangement Gap (Required – Medium – Yellow): There is a discrepancy between CCSB's list of identified business associates and the City Attorney's. The following identified business associates have not signed a Business

Associate Agreement: Hib, Rogal & Hamelton, Lab Corp, and SPSA. Memorandums of Understanding have not been drafted or signed. Further assurance is not obtained for service providers that are critical to operations.

KPMG Written Contract or Other Arrangement Recommendation: Ensure Business Associate Agreements and Memorandum of Understandings on file with City Attorney match current documentation held at CCSB. Draft Memorandum of Understandings to be signed by identified governmental business associates, including identified City departments. Based on the risk analysis, obtain or conduct the following assurance from business associates based on the level of risk assigned: HIGH – Obtain/Review a Statement of Auditing Standards Number 70 (SAS 70) Report from the business associates., MEDIUM – Conduct yearly meetings with the management of business associates and walk through the organization’s internal control process., and LOW – Obtain a signed Business Associate Agreements or Memorandum of Understandings from the business associate. Inventory of Business Associates are maintained by City Attorney and updated via discussions with CCSB on a periodic basis.

Status: The HIPAA Privacy Officer was working with the City Attorney’s Office to ensure that all Business Associate Agreements are in place.

PHYSICAL SAFEGUARDS

Facility Access Controls process – 164.310(a)(1) – Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.

P-1.1 Contingency Operations (Addressable – Low - Yellow): The *Disaster Recovery Plan for Computer Services* does not specifically address limiting physical access to electronic protected health information during a disastrous event.

KPMG Risk Analysis Recommendation: This item is addressed jointly with A-7.2 as followed. Evaluate, identify and consider alternate processing environment options (e.g., alternate buildings with excess capacity or vendor quick ship agreements, etc.). Update disaster recovery plan with pertinent information. Perform testing procedures to ensure alternate processing functions effectively. Assumptions: Funding for alternate processing options is limited. Only the most critical systems will be recovered in the event of a disaster.

Status: This item was contingent on outsourcing for the development of a Risk Analysis.

P-1.2 Facility security Plan (Addressable – Low – Yellow): Since the construction of the new building has not been completed, policies and procedures have not been finalized.

KPMG Risk Analysis Recommendation: As construction of the new CCSB building nears completion, documented procedures controlling building access should be finalized.

Status: CCSB has implemented a Prox Card Security System, however, no documented procedures for controlling access has been established.

P-1.3 Access Control and Validation Procedures (Addressable – Low – Yellow): Since the construction of the new building has not been completed, policies and procedures have not been finalized.

KPMG Risk Analysis Recommendation: As construction of the new CCSB building nears completion, documented procedures to validate a person's building access based on his/her job requirements should be finalized. Assumptions: The City's future documentation can be leveraged to expedite the process and drive consistency between the two IT groups.

Status: Policies and procedures will not be written until a Risk Manager is hired.

Device and Media Controls process – 164.310(d) – Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

P-4.2 Media Re-use (Required – High – Red): The savvy computer user could access electronic protected health information that was previously stored on the workstation if the hard drive is not reformatted before it is transferred. By not degaussing magnetic tapes prior to re-use, the integrity of the data stored on the off-line media may be compromised. No procedures have been documented.

KPMG Risk Analysis Recommendation: Document and implement procedures to degauss hardware and magnetic tapes, on which electronic protected health information resides, prior to re-use. Assumptions: Time required for ongoing degaussing of magnetic tapes dependent on amount of electronic protected health information data written to off-line media.

Status: The HIPAA Committee has FY 2006 funding approved for CCSB to purchase a degaussing machine to clean tapes and hard drives prior to re-using. However, CCSB has no written policy and procedures on this subject.

P-4.3 Accountability (Addressable – Low – Yellow): A formal method of tracking the location of magnetic tapes does not exist.

KPMG Risk Analysis Recommendation: Develop and implement a documented procedure that tracks the location of magnetic tapes containing electronic protected health information. Assumptions: The current off-site procedures will simply be

augmented (adding another column to the backup tracking spreadsheet) to include physical location of the media.

Status: No written procedures and their implementation have been done to track the location of magnetic tapes with electronic protected health information.

P-4.4 Data Backup and Storage (Addressable - Low – Plaid Green): The documented policy and procedure is not enforced.

KPMG Risk Analysis Recommendation: This item is addressed jointly with A-7.1 as followed. Review current documented policies and procedures. Analyze the impact to determine if implementing the current policies and procedures will be more effective than altering current schedule. Dependant on impact and Risk Analysis (see A-1.1) modify the schedule and/or policy and procedures documentation. Assumptions: Additional physical media may be required for storage of backup data in the event the current policies and procedures (i.e., retention, etc.) are implemented.

Status: CCSB has FY 2005 funding approved to purchase additional media.

TECHNICAL SAFEGUARDS

Access Control process – 164.312(a)(1) – Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted appropriate access rights.

T-1.1 Unique User Identification (Required – High - Red): Although role-based security exists within BTI/HSS, the ability to access (i.e., add, read, modify) electronic protected health information is currently granted to individuals who do not have a business need. Additionally, electronic protected health information is being shared amongst clinicians within the Lotus Notes system. Identifying and tracking user identity cannot be accomplished with generic user identifications.

KPMG Risk Analysis Recommendation: Review the Lotus Notes and BTI/HSS applications for generic user identification. Analyze which operational functions require the use of generic user identification (e.g., batch jobs, system identifications, etc.). Document the approved use of these generic user identifications and implement a mitigating control such as restricted functions e.g., no direct log-in with batch process identification, etc. Remove and/or modify all appropriate generic user identifications based on the review and analysis. Assumptions: There is no compelling business need for end users to utilize generic identifications to access systems containing electronic protected health information.

Status: CCSB does not and can not have role based security for most of its programs because of cross disability clients (i.e., mental retardation or mental health clients that were drug users). However, as discussed above (A-6.1), the Infant

Intervention database does not have to be used (cross disability programs) by other programs' staff, and thus only CCSB Infant Intervention staff have access to the database. CCSB no longer uses generic identifications (meaning more than one person using the same identification to log on to the system). All staff now have unique identifications for entering program systems. Finally, CCSB does not have written policy and procedures on this subject.

T-1.2 Emergency Access Procedure (Required – Medium - Yellow): *The Disaster Recovery Plan for Computer Services* is partially reliant on an alternate computer center site, which has not been identified to date.

KPMG Risk Analysis Recommendation: This item is addressed jointly with A-7.2 as stated below. Evaluate, identify and consider alternate processing environment options (e.g., alternate buildings with excess capacity or vendor quick ship agreements, etc.). Update disaster recovery plan with pertinent information. Perform testing procedures to ensure alternate processing functions effectively. Assumptions: Funding for alternate processing options are limited. Only the most critical systems will be recovered in the event of a disaster.

Status: CCSB has no alternate site identified due to infrastructure and budget constraints. CCSB could continue servicing client; the clients charts are keep in paper mode thereby allowing the clinical staff to have access to pertinent data. However, any long term loss of the computer resources in excess of two weeks would disable CCSB's ability to bill its payers, prevent access the City's Financial System, and thus would restrict its ability to pay employees. However, if the disaster event was City wide, where emergency shelters are open, all clinical staff would be required to man those sites so CCSB would not be able to provide services to its clients until the shelter were closed.

T-1.3 Automatic Logoff (Addressable – Low – Yellow): Workstations are not built to automatically lock users out of the workstation and/or network after a period of inactivity.

KPMG Risk Analysis Recommendation: Configure and test automatic workstation lockouts/screen saver passwords after a predetermined period of time on the LAN (e.g., 5-1- minutes of inactivity). Assumptions: Users do not have the ability to disable the LAN lockout/screen saver password locally on their individual workstation.

Status: Users are reminded to lock their computer before walking away from them. They are cautioned as to the consequences of not doing this. The AS400 does automatically log off users after 30 minutes of inactivity and Lotus Notes log off after 15 minutes. Presently CCSB was exploring how to automatically log off the Microsoft Network.

T-1.4 Encryption and Decryption (Addressable – Low – Red): Mechanisms to encrypt and decrypt do not exist. The *Acceptable Encryption Policy* does not identify data elements to be encrypted.

KPMG Encryption and Decryption Recommendation: Determine if current vendor application solutions are feasible in the current technology environment. Investigate an operating software upgrade to the LAN that includes file system encryption capabilities. Based on the investigation, consider implementing an operating software upgrade for the LAN, or document the need not to implement file storage encryption due to lack of practicality in the environment and the existence of mitigating controls (e.g., physical access, logical security, etc.). Assumptions: Costs of software upgrades may not be practical for CCSB. Future access control enhancements may appropriately mitigate the risk for this addressable implementation specification.

Status: CCSB has \$31,000 in FY 2005 funding approved to purchase encryption software.

Integrity processes – 164.312(c)(1) – Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

T-3.1 Mechanism to Authenticate Electronic Protected Health Information (Addressable – Medium – Red): Although role-based security exists within Lotus Notes and BTI/HSS, the ability to access (i.e., add, read, modify) electronic protected health information is currently not limited to only an individual employee's client caseload. Additionally, when clients are transferred between clinicians for treatment, their electronic protected health information is placed within a database in Lotus Notes for the new clinician's reference. Transmission of electronic protected health information data to the Commonwealth of Virginia is not authenticated via any corroborative mechanisms such as digital signatures. It is unclear whether the transmission of electronic protected health information data to Professional Management Group (PMG) is authenticated via any corroborative mechanisms such as digital signatures. No document policies and procedures exist.

KPMG Risk Analysis Recommendation: This item is addressed jointly with A-3.2 as followed. Review access privileges for all user accounts for the LAN, Lotus Notes, and BTI/HSS. Restrict access privileges to the Lotus Notes and BTI/HSS based on the business needs of users. Assumptions: The strategy for restricting access based on "Need to Know" will be documented in a manner that is appropriate given the business requirements of CCSB system end users.

Follow up with PMG to evaluate the means used to authenticate data transmissions. Based on this evaluation, implement authentication process or document mitigating controls. Assumptions: Costs of software upgrades may not be practical to implement within the PMG environment. Future access control and additional manual reconciliation enhancements may appropriately mitigate the risk for this addressable implementation specification.

Status: This item is dependent on outsourcing for the development of a Risk Analysis and a Risk Management Program. Additionally CCSB requested and was

approved funding to gain additional technical assistance for BTI to set up its electronic billing thereby removing PMG as its clearinghouse.

Person or Entity Authentication process - 164.312(d) – Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

T-4.0 Person or Entity Authentication (Required – Medium – Yellow): Since the construction of the new CCSB building has not been completed, policies and procedures have not been finalized.

KPMG Risk Analysis Recommendation: This item is addressed jointly with P-1.2 as followed. As construction of the new CCSB building nears completion, documented procedures controlling building access should be finalized.

Status: CCSB has installed a Prox card system which restricted employee from having physical access to areas that they do not need to have access to. This system records the areas and time an employee has accessed a specific area. Additionally CCSB has installed an external security monitoring system and has employed full security guard to patrol and limit access to the building. However, no written documentation exists.

Transmission Security process – 164.312(e)(1) – Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

T-5.1 Integrity Controls (Addressable – Low – Yellow): Confirmation does not contain information pertaining to the accuracy or completeness of the data transmission. No documented policies and/or procedures exist.

KPMG Risk Analysis Recommendation: Evaluate means to assure the data integrity of transmissions to PMG. Based on evaluation, implement the data integrity process of data transmissions or document mitigating controls. Assumptions: Costs of software upgrades may not be practical to implement within the PMG environment. Future access control and additional manual reconciliation enhancements may appropriately mitigate the risk for this addressable implementation specification.

Status: CCSB has \$31,000 in FY 2005 funding approved to purchase encryption software.

T-5.2 Encryption (Addressable – Medium – Red): Electronic protected health information is traversing the Internet to Information Technology in clear text. Electronic protected health information is being couriered on a CD-ROM in clear text.

KPMG Risk Analysis Recommendation: Follow up with PMG to evaluate the means used to encrypt data transmissions. Analyze and evaluate with the City's

Information Technology Department and Direct Marketing the use of encryption software (e.g., ABI-Coder or PGP) for email and/or attachments and CD-ROMs containing electronic protected health information. Assumptions: ABI-Coder would be used to encrypt attachments only, not the content/body of the email message itself.

Status: CCSB has FY 2005 funding approved to purchase encryption software.

Legend:

*Required - Safeguard is required.

*Addressable – Assess whether the specification is reasonable and appropriate in the environment, given its contribution to protecting electronic protection health information. Based on the assessment, the covered entity must implement (if reasonable and appropriate) OR document why the specification is not reasonable and appropriate AND implement an equivalent security measure.

*Priority – High, Medium, or Low.

*Color Code – Plaid Green (Denotes safeguard in place – but inconsistent with documented policy); Yellow (Denotes safeguard partially in place or undocumented); Red (Denotes safeguard not in place).