Special Review

Maryland Health Care Commission

Security Monitoring of Patient Information Maintained by the
State-Designated Health Information Exchange

September 2017

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Warren G. Deschenaux
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

September 5, 2017

Senator Craig J. Zucker, Co-Chair, Joint Audit Committee
Delegate C. William Frick, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We conducted a review of the Maryland Health Care Commission's (MHCC) efforts to provide assurance as to the security and confidentiality of patient health care data collected and retained by the State-Designated Health Information Exchange (HIE). HIE is used by the Maryland health care community to share electronic health information for approximately 9.2 million individuals, and is maintained by an independent non-profit entity under an agreement with MHCC.

Our review disclosed that instead of obtaining a security and confidentiality review of HIE using industry-recognized authoritative guidance, MHCC engaged a certified public accounting (CPA) firm to conduct an annual performance audit of HIE. The audit objective was to assess whether the protected health information (PHI) and personally identifiable information (PII) obtained by HIE was processed, transmitted, and stored in a secure manner. However, unlike reports issued for reviews using recognized guidance (for example, a System and Organization Controls for Service Organizations (SOC) review under guidance issued by the American Institute of Certified Public Accountants), the performance audit report issued in May 2016 did not contain certain information regarding the review's scope and results. The report did not provide sufficiently detailed descriptions of the specific procedures and tests performed and related results to provide the necessary assurance that HIE participants' patient data were properly secured.

In addition, the performance audit report stated that the related audit included reviews of the SOC reports for contractors performing critical information technology services (such as hosting and infrastructure services) for HIE. However, the audit report did not address the scope of the SOC reviews, the testing performed, and the related results. As a result, MHCC lacked assurance

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

as to the security and confidentiality of the PHI and PII processed, retained, and transmitted by these contractors.

MDH's response to this audit, on behalf of MHCC, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this review by MHCC.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Scope, Objectives, and Methodology

We conducted a review of the Maryland Health Care Commission's (MHCC) efforts to provide assurance as to the security and confidentiality of data collected and retained by the State-Designated Health Information Exchange.

Effective October 29, 2009, MHCC entered into a memorandum of understanding with the Chesapeake Regional Information System for our Patients, Incorporated (CRISP) to become the State-Designated Health Information Exchange (HIE). CRISP is an independent 501(3)(c) corporation per the Federal Internal Revenue Code. As the State-Designated HIE, CRISP is responsible for building and maintaining a technical infrastructure to enable the Maryland health care community to appropriately and securely share electronic health information.

The purpose of our review was to determine if MHCC was ensuring that the sensitive protected health information and personally identifiable information received, retained, and transmitted by HIE was properly secured at all times. This review was performed in accordance with State Government Article, Section 2-1220 of the Annotated Code of Maryland.

Our review consisted of discussions with MHCC personnel, a review of the latest performance audit issued for the period covering April 1, 2015 to March 31, 2016, and other procedures as we deemed necessary to achieve our objectives. The results of our review are identified in Finding 1. Our review did not constitute an audit conducted in accordance with generally accepted government auditing standards. Our review was conducted during the period from February 2017 through April 2017.

MDH's response to this audit, on behalf of MHCC, is included as an appendix to this report. As prescribed in State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise MDH regarding the results of our review of its response.

Background Information

The Health–General Article of the Annotated Code of Maryland includes the provision for the creation of a State-designated health information exchange as per direction of the Maryland Health Care Commission (MHCC) and the Health Services Cost Review Commission.

Effective October 29, 2009, the MHCC entered into a memorandum of understanding with the Chesapeake Regional Information System for our Patients, Incorporated (CRISP) to become the State-Designated Health Information Exchange (HIE). CRISP is an independent 501(3)(c) corporation per the Federal Internal Revenue Code. As the State-Designated HIE, CRISP is responsible for building and maintaining a technical infrastructure to enable the Maryland health care community to appropriately and securely share electronic health information.

The Health-General Article further specifies that MHCC shall adopt regulations for the privacy and security of protected health information (PHI) obtained or released through an HIE. Furthermore, the Code of Maryland Regulations (COMAR) specifies that an HIE shall conduct an annual privacy and security audit to detect patterns of inappropriate access, use, maintenance, and disclosure of information that are in violation of COMAR and provide the findings of these audits to MHCC. In addition, COMAR also states that, at the request of MHCC, the HIE shall utilize a qualified third party to conduct an audit on the access, use, and disclosure of information through and the maintenance of information by the HIE.

The CRISP system database holds information on patients registered at Maryland health care organizations. We were advised that the CRISP Master Patient Index contained information related to approximately 9.2 million unique individuals as of March 2, 2017. We were advised that the CRISP query portal was accessed approximately 102,000 times each month and the notification system (which provides almost immediate notifications to primary care physicians and care coordinators when medical practices' patients are admitted to an emergency room, or are admitted to / discharged from a hospital) sends approximately 24,000 messages each day.

Six different contractors provided material information technology (IT) support services to CRISP. These support services include hosting and infrastructure, offsite data backup and management of CRISP application servers, network devices and a virtual production environment. CRISP was directly responsible for application and database security controls over its critical systems and for

ensuring that operating systems for servers supporting these systems were properly secured and hardened.

Findings and Recommendations

Finding 1
MHCC lacked assurance that sensitive information (including protected health information and personally identifiable information) obtained and maintained by the Chesapeake Regional Information System for our Patients (CRISP) was properly secured.

Analysis
MHCC lacked assurance that sensitive information (including protected health information and personally identifiable information) obtained and maintained by CRISP was properly secured.

Data Security Controls Directly Attributable to CRISP
The most recent performance audit report obtained by MHCC did not provide detailed descriptions of the specific procedures and tests performed and related results to ensure that the CRISP participants' patient data were properly secured. MHCC procured and obtained performance audits to ensure that CRISP participants' patient data were processed, transmitted, and stored by CRISP and its contractors in a secure manner in accordance with applicable laws and regulations. While the performance audit was conducted in accordance with the terms of the agreement between MHCC and an independent certified public accounting (CPA) firm and contained a number of findings and recommendations for improvements to controls, the auditor's work was not required to be conducted in accordance with certain industry-recognized authoritative guidance. MHCC advised us that, at the time of our review, CRISP had not been subject to any additional independent reviews.

At the time of our review, the most recent MHCC procured performance audit was conducted by a CPA firm covering the period from April 1, 2015 through March 31, 2016 and the related report was dated May 11, 2016. Our review disclosed that the report stated that the methodology of the performance audit included:

- tests and observations of system and process controls designed to ensure that CRISP participants' patient data were processed, transmitted, and stored in a secure manner;
- reviews of CRISP policies and procedures and its contractors' policies and System and Organization Controls for Service Organizations reports; and
- vulnerability scans of CRISP servers and network devices at hosted data centers.

Neither a System and Organization Controls for Service Organizations (SOC) independent review nor a Health Information Trust Alliance (HITRUST) independent review was conducted to address security, confidentiality and availability controls over CRISP. Instead, MHCC contracted for the aforementioned performance audit to assess controls implemented by CRISP. However, unlike in a SOC or HITRUST review, the description of the scope of the performance audit and the related test work performed was not detailed enough to allow MHCC to fully determine the extent to which patient data was secured. We noted that the performance audit report did not address database controls, such as access to critical database tables, as well as certain operating system security controls applicable to critical CRISP systems. A SOC review and report, for example, would have included a description of the database and operating system controls that existed at CRISP, a description of the testing performed, and the results of that testing.

Thus, these other types of independent reviews, which are conducted using industry-recognized authoritative guidance, would provide MHCC with greater assurance of data security. Specifically, both SOC reviews and HITRUST reviews are specifically designed to address security, confidentiality, and availability concerns for various entities including health information exchanges. These reviews and their associated standard type reports utilize a defined framework, which provides sufficient detail for certain trust principles (for example, security) over which controls should be reviewed and tested. Therefore, SOC or HITRUST reports should provide MHCC sufficient documentation and evidence of exactly what was reviewed, tested, and found. This information would allow MHCC to determine if the reviews performed properly addressed their concerns over the security and confidentiality of the CRISP participants' patient data.

The American Institute of Certified Public Accountants has issued guidance for auditing and reporting on reviews of service providers. This guidance encompasses several types of reviews and related SOC reports. A SOC 2 Type 2 review, which includes reviews of controls placed in operation and tests of operating effectiveness of these controls for the periods under review, could be tailored to include an evaluation of security, confidentiality, and availability over the CRISP system. The HITRUST common security framework (CSF), which was developed in collaboration with security professionals, is a widely adopted framework in the healthcare industry. The HITRUST CSF assurance program provides guidance for a common approach to managing security assessments.

Audits of CRISP Information Technology Support Services Contractors

Appendix A of the aforementioned performance audit report includes a statement that the performance audit encompassed a review of the CRISP contractors' SOC reports. However, the remainder of the report did not address the scope of these reviews, the testing performed, and the related results.

In addition, we determined that MHCC did not request, obtain, or review the SOC reports for the aforementioned contractors because MHCC personnel did not believe that they had the technical expertise to perform an effective review of these reports. As a result of these conditions, MHCC has no assurance that:

- there were SOC 2 Type 2 reports (or other independent type reports) for each of the aforementioned contractors for all recent periods,
- the scope of the SOC reviews were appropriate and included all relevant controls, and
- the extent of any deficiencies identified in these reports that could significantly and adversely impact the security and confidentiality over CRISP participants' patient data.

Recommendation 1

We recommend that MHCC

a. require, as allowed by COMAR, that CRISP obtain an independent annual review (such as a SOC 2 Type 2 or HITRUST review) for at least the security and confidentiality trust principles over CRISP applications, databases and operating systems that support critical CRISP systems;

b. obtain a copy of the related report, assess the report to ensure that its scope is sufficient, ensure that all critical deficiencies identified in the report are promptly corrected, document these assessments, and retain the documentation for future reference; and

c. obtain copies of the SOC reports (or other independent audit reports) for the aforementioned contractors, review these reports to ensure that the scope of the independent reviews were sufficient and ensure, via CRISP, that all critical deficiencies identified in these reports are promptly corrected, document these reviews and retain the documentation for future reference.

APPENDIX

MARYLAND
Department of Health

Larry Hogan, Governor · Boyd Rutherford, Lt. Governor · Dennis Schrader, Secretary

August 30, 2017

Mr. Thomas J. Barnickel III, CPA
Legislative Auditor
Office of Legislative Audits
301 W. Preston Street
Baltimore, MD 21201

Dear Mr. Barnickel,

Thank you for your letter regarding the draft audit report of the special review of the Maryland Health Care Commission. Enclosed is the Department's response and plan of correction that addresses each audit recommendation. I will work with the Commission to promptly address all audit exceptions. In addition, the OIG's Division of Audits will follow-up on the recommendations and responses to ensure compliance.

If you have any questions or require additional information, please do not hesitate to contact me at 410-767-4639 or Megan Davey Limarzi, Inspector General, at 410-767-5862.

Sincerely,

(COS/Acting)

Dennis R. Schrader
Secretary

Enclosure

cc: J. David Lashar, Chief of Staff
Ben Steffan, Executive Director, MHCC
Megan Davey Limarzi, Inspector General, MDH

Findings and Recommendations

Finding 1
MHCC lacked assurance that sensitive information (including protected health information and personally identifiable information) obtained and maintained by the Chesapeake Regional Information System for our Patients (CRISP) was properly secured.

Recommendation 1
We recommend that MHCC

a. require, as allowed by COMAR, that CRISP obtain an independent annual review (such as a SOC 2 Type 2 or HITRUST review) for at least the security and confidentiality trust principles over CRISP applications, databases and operating systems that support critical CRISP systems;

b. obtain a copy of the related report, assess the report to ensure that its scope is sufficient, ensure that all critical deficiencies identified in the report are promptly corrected, document these assessments, and retain the documentation for future reference; and

c. obtain copies of the SOC reports (or other independent audit reports) for the aforementioned contractors, review these reports to ensure that the scope of the independent reviews were sufficient and ensure, via CRISP, that all critical deficiencies identified in these reports are promptly corrected, document these reviews and retain the documentation for future reference.

Commission's Response

a The MHCC concurs with the recommendation. In future audits of the CRISP systems MHCC will conform with the recommendation to include in the scope of the audits the SOC 2 or HITRUST reviews. However, MHCC believes that ceding the direction of the review to CRISP in FY 2018 is premature. The MHCC will decide after completing the FY 2018 CRISP Privacy and Security Audit as a SOC 2 Type 2 review, whether responsibility for obtaining subsequent audits consistent with the recommendation will be delegated to CRISP or continue under the direction of MHCC.

b, c The MHCC concurs with these recommendations. Starting with the 2018 Privacy and Security Audit we will conduct a SOC 2 Type 2 review of

CRISP and obtain copies of CRISP vendors' SOC 2 Type 2 reports, assess the reports to ensure that its scope is sufficient, ensure – via CRISP - that all critical deficiencies identified in the report are corrected as soon as reasonably practicable based upon industry standards and best practices. MHCC will document these assessments and CRISP's remediation and documentation for future reference. Completion date for receiving the first CRISP SOC 2 Type 2 report is May 2018.

AUDIT TEAM

Stephen P. Jersey, CPA, CISA
Information Systems Audit Manager

R. Brendan Coffey, CPA, CISA
Information Systems Senior Auditor