An Independent Evaluation of the HIPAA Programs

Privacy, Security, and Breach Notification

Prepared For

Management & Medical Consulting Services (MMCS)

March 21, 2017

Prepared by

John Cathey, MBA, CBCP, PMP

Principal Consultant, tw-Security

john.cathey@tw-Security.com

tw Security
Healthcare Information Security

6108 W. 121st Street, Overland Park, KS 66209
(o) 913-696-1573 | tom.walsh@tw-Security.com
www.tw-Security.com

Evaluation of the HIPAA Programs

Purpose

The clients ("Covered Entities") of MMCS may want to obtain some type of reasonable assurances that the policies, procedures, plans, safeguards, and controls implemented at MMCS are based upon a risk analysis as well as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The intent of this validation letter is to provide a mechanism to quickly and efficiently respond to inquiries on the status of compliance and to help MMCS clients make an informed business decision.

Status

Based upon an independent, nontechnical evaluation conducted by tw-Security in December 2016, it is our professional opinion that **MMCS meets the applicable provisions of the HIPAA Privacy, Security, and Breach Notification Rule**. Our opinion is based upon the level of maturity at MMCS where the following three things were demonstrated:

1) An awareness of the applicable requirements,
2) Observation or proof of a practice being followed, and
3) Documented evidence to support compliance.

Our evaluation benchmarks were derived from our knowledge and experience in using the standards and implementation specifications in the HIPAA Privacy, Security, and Breach Notification Rules and the criteria from the *HIPAA Audit Program Protocol,* the same audit test procedures used by the Office for Civil Rights (OCR) for evaluation of HIPAA compliance for covered entities. At this time, there is no audit protocol specifically written for business associates.

The risk analysis, based on the methodology outlined by the National Institute of Standards and Technology (NIST), was conducted for IT infrastructure, virtual worker, and operational practices.

Evaluation Process

The evaluation was conducted through scheduled interviews structured to document security controls and policies that were already in place. The risk analysis conducted by tw-Security documented the reasonably anticipated threats, existing security controls in place to address those threats, and the remaining vulnerabilities identified. Suggestions were made for additional security safeguards and controls as well as any noted gaps in compliance. A prioritized action plan was created to:

- Address risk remediation and compliance gaps
- Ensure that resources were allocated
- Track start and completion dates

Some sample documents were also provided to help complete certain tasks within the plan. Additional support services were provided by tw-Security to help MMCS complete the majority of the tasks in the prioritized action plan and answer questions that arose.

Results

The items identified in this assessment represent low to medium risks. Even though the remaining risk items are within normal risk tolerances, remediation activities are planned to address these findings. A prioritized action plan was prepared by tw-Security to address the team's recommendations for improvement and to address any remaining findings.

It is the opinion of this consulting team that there are no significant compliance gaps.

However, compliance is an ongoing effort. Any third-party evaluation is based upon the organization's status at any given point in time. Also, evaluations are subject to inherent limitations.

The report prepared by tw-Security is intended solely for the benefit and use of MMCS. tw-Security assumes no liability for any issues that may arise in the future. Questions regarding the evaluation process or report of findings may be directed to:

Sheryl Lemons
Management & Medical Consulting Services LLC.
33637 US Highway 280, Suite C
Childersburg, Alabama 35044
Main: 256-346-3611
Email: sheryl@managementmed.com

Staffing

Tom Walsh, CISSP, tw-Security Founder and Managing Partner, is a nationally recognized expert in healthcare information security and a Certified Information Systems Security Professional (CISSP). Tom is a well-known leader and educator in healthcare information security. In addition to numerous articles, he has co-authored four books published by the American Medical Association (AMA), American Health Information Management Association (AHIMA) and Healthcare Information and Management Systems Society (HIMSS) as well as presented at the HIMSS Annual Conference, the largest health IT event in the industry, for 15 consecutive years. Tom is an active member and contributor to HIMSS and AHIMA at both local and national levels.

Tom has over 24 years of information security experience. In addition to leading tw-Security, Tom has been the information security consultant for several healthcare organizations including

hospitals and business associates. Prior to starting his healthcare consulting business in 2003, Tom's experience included being the first information security manager for a large, multi-hospital healthcare system in Kansas City.

Mark Dill, CISM, CRISC, is a Partner and Principle Consultant for tw-Security. Mark retired from a long successful career as the Director of Information Security for Cleveland Clinic. At Cleveland Clinic, Mark was responsible for the deployment of information security and disaster recovery best practices and compliance with HIPAA, PCI, and Internal Control Effectiveness/SOX regulations and standards. In December of 2015, *Health Data Management* recognized Mark as one of the "50 Top Healthcare IT Experts". In 2014, Mark was recognized by *HealthcareInfoSecurity.com* as one of the most influential people in healthcare information security. Mark contributes to local, regional and national efforts supporting information security program advancements and discipline. Mark was recently appointed to the Advisory Board for Information Security Media Group. Mark is an author and frequent speaker at national, regional and local conferences, notably HIMSS and AHIMA.

John Cathey, MBA, CBCP, PMP, a tw-Security Principal Consultant has a long and diverse background in Information Technology. Since 1990 he has been focused in the areas of security and disaster recovery, the last 18 years dedicated to tactical disaster recovery, business impact analysis, high availability strategies design and implementation. He gained his rich experiences in the following positions; Senior Manager for Ernst and Young, Manager, Professional Services for SunGard Availability Services and Senior Engagement Manager for IBM. John was the architect and implementation specialist for a New York City investment firm on an advanced failover recovery system that was successfully executed during the World Trade Center tragedy on September 11, 2001. All professional certifications are up to date and a member in good standing. John is currently preparing for the Healthcare Information Security and Privacy Practitioner (HCISSP) exam.