Celebrating 60 years
Established 1952
HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

MDdatacor
CLINICAL DATA, QUALITY OUTCOMES

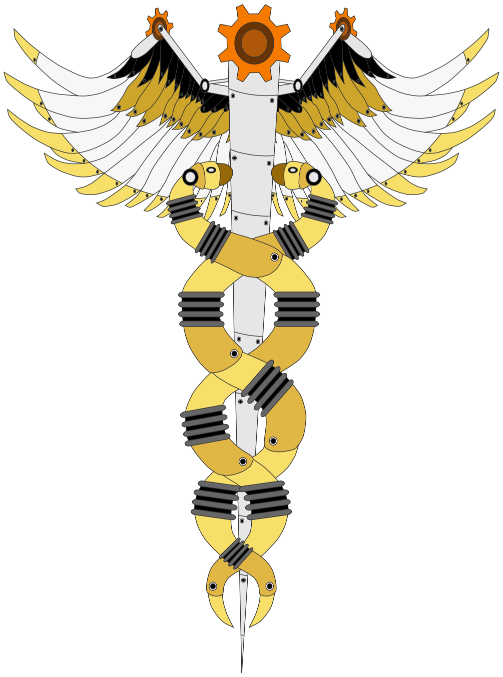
# Healthcare IT Company Seeks Transparency into Controls

*World-class report confirms solid data security processes*

## All-Around Peace of Mind: MDdatacor Efficiently Meets HIPAA Privacy and Security Requirements with SOC 2 Assurance Reporting

### Background

Established in 2001, MDdatacor transforms healthcare practices to improve quality of care and patient outcomes while reducing costs. They accomplish this mission through innovative data-aggregation technology, clinical program integration and patient-centered medical home programs.



A growing number of health plans across the country have recognized the value of MDdatacor's solutions, and in late 2011, Noridian Mutual Insurance Company completed an acquisition of the company.

### Challenges

As the company has grown, so have the regulatory hurdles through which healthcare entities must jump. "The HITECH Act has spurred all of our customers to be more engaged in the evaluation and scrutiny of privacy and security measures implemented by their business associates," says Fiona Clark, MDdatacor's VP of Operations. "We wanted to be proactive in demonstrating our company's rigorous controls."

Even more pressing, the firm was negotiating a contract with a large health plan – their largest customer at that point – that had included in its business associate agreement a clause requiring an audit of MDdatacor's internal controls.

MDdatacor's leaders also needed this information for their own peace of mind, despite the strain on the financial and human resources it would place on the small company.

"Everything was on the line," says Kimberly Greaves, MDdatacor's general counsel. "In the event of a major breach, healthcare IT companies face monumental compliance costs and loss of customer trust. MDdatacor felt compelled to take steps to verify that it was doing all that it reasonably could to mitigate risks, protect its customers and ensure future success of the company."

### Organization

MDdatacor, Inc.
**www.mddatacor.com**

### Industry

Healthcare IT
Healthcare Practice Transformation

### Challenges

- ○ MDdatacor's desire to provide absolute transparency into privacy and security controls
- ○ Needed assurance that company is complying with HIPAA Privacy and Security Rules and general industry standards for protecting customers' PHI

### Solution

Service Organization Control 2 Report based on Generally Accepted Privacy Principles

### GAME - CHANGER

The HA&W team thoroughly educated MDdatacor about the new SOC reporting structure, explaining the rigor and transparency provided by management's system description and assertion (required components of a SOC 2 report), and the credibility and high level of assurance inherent in the independent auditor's opinion backed by recognized professional standards.

## The Solution

At the time MDdatacor began this search, the only available solution was a SAS 70 audit, the report that gained prominence in the last decade as a way to improve the efficiency of financial statement audits. However, this report would have been insufficient for MDdatacor's situation, since it does not address the operational and compliance risks that are at the heart of healthcare entities' concerns.

But another option was just being introduced to the market by the American Institute of Certified Public Accountants ("AICPA"). In 2010, the AICPA released a new service organization control ("SOC") reporting structure that helps business associates and covered entities more comprehensively address their governance needs. One of these options, known as SOC 2, was designed specifically to provide a high level of transparency into controls around privacy, confidentiality, security, availability and/or processing integrity.

While Greaves and Clark had been in discussions with several public accounting firms about SOC reporting, one stood out.

**Habif, Arogeti & Wynne ("HA&W") had been referred to the company by its law firm, due to the firm's leadership in the area of IT assurance. As immediate ex-chairperson of the AICPA Information Technology Executive Committee, Partner Dan Schroeder had been involved in validating the SOC framework and leading SOC education nationally.**

They also showed how the AICPA's new Generally Accepted Privacy Principles ("GAPP"), the set of criteria used to perform a SOC 2 examination on privacy, would demonstrate compliance with HIPAA Privacy and Security. This was a key component of MDdatacor's decision to embrace SOC 2.

> **"I didn't want to go through an audit that didn't cover a vast majority of what the HIPAA Privacy and Security regulations require."**

**Kimberly Greaves**
MDdatacor's general counsel

The MDdatacor team conducted significant due diligence over the course of a year to ensure that both HA&W and the SOC 2 framework would meet the company's high standards. After a series of meetings with HA&W and creating in-depth documents that mapped HIPAA Privacy and Security criteria directly to GAPP criteria, MDdatacor was confident they had categorical evidence that a SOC 2 examination on the Privacy Principle would demonstrate compliance with the HIPAA Privacy and Security Rules, including required and addressable implementation specifications.

## The Implementation

As with any implementation, all did not go as planned. Always working to improve and enhance its products and services, MDdatacor had several concurrent major projects as well as changes to the corporate structure of the company, all of which contributed to a longer-than-expected timeline for the audit. But everyone understood that the deadline for delivery of the SOC 2 report was firm and did what was necessary to meet it.

**HA&W was instrumental in helping MDdatacor cross that finish line. Schroeder and his team provided a detailed roadmap and guidance on how best to structure controls and the system description to fulfill the SOC 2 requirements, and they made sure MDdatacor had no audit testing surprises.**

HA&W provided a detailed audit program for all the controls in advance of testing so MDdatacor could best anticipate and plan for evidence they would need to provide, reducing delays.

HA&W also was flexible and accommodating, meeting every deadline and delivering the report on time to help MDdatacor meet its commitment to proving the security of its data.

## The Results

### Improved Efficiency

The SOC 2 report is a vastly more efficient way to respond to customer requests for evidence of privacy and security measures. Instead of addressing requests one-by-one, which can take days and tie up hundreds of hours of human resources, Clark is able to satisfy customer requests for proof of transparency with a copy of the SOC 2 report.

Greaves estimates that the cost of the SOC 2 audit was far less than the human resource costs that would have been incurred to satisfy multiple clients' demands for in-person audits and customized questionnaires.

### Ahead of the Curve

"Being able to share the SOC 2 report also demonstrates to customers that MDdatacor is serious and proactive in regard to security," Greaves says.

While other assurance reporting options claim to fulfill HIPAA compliance needs, "they may be showing only part of the picture," and they lack the credibility and substance of a SOC 2 report conducted by independent auditors, she says.

The robust, comprehensive and credible SOC 2 report, on the other hand, is "a positive in contract negotiations, when we're trying to earn trust," she adds.

### All-Around Peace of Mind

The most significant benefit of the SOC 2 reporting process has been the reassurance that it gives to management that they are doing the right things to protect PHI.

"You don't know if you really have your house in order until you verify these things with some level of certainty," Greaves says.

The report also provides a roadmap to all MDdatacor employees. In fact, new employees are immediately given the 110-page SOC 2 report to help them understand how the company operates and how it protects PHI.

All IT and operational decisions are now made through the lens of how they will impact the company's control environment related to security and privacy.

> **"Security and privacy are top-of-mind for all MDdatacor employees. When we go about our daily tasks, we know we're making decisions based on the security and privacy policies and procedures we have in place. It has given us all-around peace of mind."**

**Fiona Clark**
MDdatacor's VP of Operations

## RESULTS

Ability to quickly and efficiently respond to requests for evidence of privacy and security controls – almost immediately with virtually no effort, versus hundreds of hours over weeks or more to complete questionnaires and audits.

Prospective clients quickly gain confidence in MDdatacor's control environment.

MDdatacor management has quantifiable verification that customers' PHI is appropriately protected consistent with HIPAA and HITECH requirements.

## CONTACT

**Dan Schroeder**
**Partner**
770-353-8379
Dan.schroeder@hawcpa.com

Celebrating 60 years

Established 1952

HA&W

HABIF, AROGETI & WYNNE, LLP

Certified Public Accountants and Business Advisors

**Habif, Arogeti & Wynne, LLP**
Five Concourse Parkway ○ Suite 1000 ○ Atlanta, Georgia 30328
404.892.9651 ○ www.hawcpa.com
An Independent Member of Baker Tilly International