ATMP Solutions

ATMP Solutions HIPAA/HITECH Assessment for:

Cogitate, Inc.

February 24,2012

ATMP Solutions HIPAA/HITECH Assessment

2011

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, ATMP Solutions. PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of ATMP Solutions, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of ATMP Solutions Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Changes or improvements may be made to the software described in this document at any time.

This is not a guarantee of compliance. This is a reasonable, best effort by ATMP Solutions to assist customers in identifying and remediating potential gaps in a company's compliance status. ATMP Solutions is reliant on the data provided by the customer. If this data is inaccurate, it is not the responsibility of ATMP Solutions. ATMP Solutionswill make every effort to validate information where ever possible, but the final output and compliance status is the responsibility of the customer.

Disclaimer

This HIPAA Report on Compliance does not address any of the following:

PART 412--PROSPECTIVE PAYMENT SYSTEMS FOR INPATIENT HOSPITAL SERVICES

PART 413--PRINCIPLES OF REASONABLE COST REIMBURSEMENT; PAYMENT FOR END–STAGE RENAL DISEASE SERVICES; OPTIONAL PROSPECTIVELY DETERMINED PAYMENT RATES FOR SKILLED NURSING FACILITIES

PART 422--MEDICARE ADVANTAGE PROGRAM

PART 495--STANDARDS FOR THE ELECTRONIC HEALTH RECORD TECHNOLOGY INCENTIVE PROGRAM

PART 13xxx - HEALTH INFORMATION TECHNOLOGY SUBTITLES A, B, C and D as pertaining to Prospective Payment systems, Medicare and Medicaid services, Miscellaneous Medicare and Medicaid Provisions, Incentive programs, Grants, Loans Funding, Research and Development Programs, Health care quality, Conditions on certain contacts as part of health care operations, and Relationships to other laws.

This service is focused on "assessments" for Business Associates. If the Business Associate's process and procedures requires any or all of the above previously mentioned sections, please review your requirements with ATMP Solutions as you may require a full HIPAA audit.

Document Control

This is a controlled document produced by ATMP Solutions. The control and release of this document is the responsibility of the ATMP Solutions' document owner. This includes any amendment that may be required.

Issue Control			
Document Reference	1.0	Project Number	Cogitate
Issue	1.0	Date	February 24, 2012
Classification	Final	Author	Joseph J. Dylewski
Document Title	ATMP Solutions HIPAA/HITECH Assessment		
Approved by	Joseph J. Dylewski		
Released by	Joseph J. Dylewski		

Owner Details	
Name	Joseph J. Dylewski
Office/Region	6323 Briarcliff Drive
Contact Number	(734)787-8758
E-mail Address	jdylewski@atmpgroup.com

Revision History			
Issue #	**Date**	**Author**	**Comments**
1.0	January 5, 2012	Joe Dylewski	Initial Findings
1.0	February 24, 2012	Joseph J. Dylewski	Final Attestation

Table of Contents

Executive Summary

ATMP Solutions conducted a review of the HIPAA assessment forms completed by Cogitate, Inc. between 12/01/11 and 2/01/12, with a principal location at: PO Box 980685, Ypsilanti, MI 48198.

ATMP Solutions has reviewed the assessment forms submitted by Cogitate, Inc. office and confirms that, based on this information; they (HAVE) met the minimum requirements for HIPAA and HITECH as per the published regulations for small business by HHS.

ATMP Solutions accomplished this by performing the following reviews:

- HIPAA Scoping and Discovery
- HIPAA Assessment
- HIPAA Report of Compliance (ROC)

All applicable controls were assessed between 12/01/11 and 2/01/12 and based solely upon the information provided by Cogitate, Inc.

Cogitate Business Description

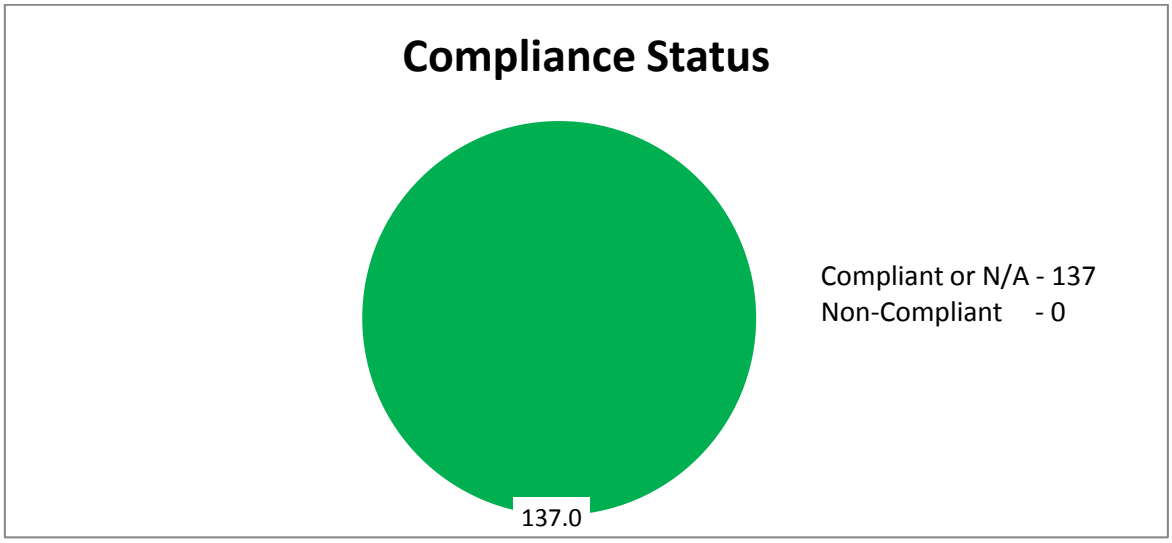
Cogitate, Inc., based in Ypsilanti, MI, provides a backup software solution, 9G Backup TM, that utilizes advanced encryption and spanning techniques. Cogitate, Inc. also offers technical and user support for their solution.

Description of Scope of Work and Approach Taken

ATMP assisted Cogitate in the development of a HIPAA compliance gap analysis and recommendation set. A three-phase approach was taken to develop this assessment. This three-phase approach consisted of Interviews and Account Provision, Preparation of a Gap Analysis and Recommendation Set, and Asset Delivery.

ATMP Solutions also assisted in the remediation services that followed the initial assessment. Included in these services were necessary policy templates, governance of gap remediation, and a final compliance review and attestation.

Overall Compliance Status: At Risk. 0 Non-Compliant Issues



Overall Risk Rating: Low. 0 Non-Compliant High risk items.

Compliance/Non-Compliance Attestation

All applicable controls were assessed between 12/01/11 and 2/01/12, and based upon the information provided, Cogitate was found to be **COMPLIANT** with the controls stipulated by the ATMP HIPAA version 1.2.1 at the time of this assessment.

Item	Safeguard	Standard	Implementation Specification	HIPAA Citation	Implementation	Attestation
3	Administrative	Security Management Process		164.308(a)(1)(i)	Required	Compliant
4			Risk Analysis	164.308(a)(1)(ii)(A)	Required	Compliant
5			Risk Management	164.308(a)(1)(ii)(B)	Required	Compliant
6			Sanction Policy	164.308(a)(1)(ii)(C)	Required	Compliant
7			Information Systems Activity Review	164.308(a)(1)(ii)(D)	Required	Compliant
8		Assigned Security Responsibility		164.308(a)(2)	Required	Compliant
9		Workforce Security		164.308(a)(3)(i)	Required	Compliant
10			Authorization and/or Supervision	164.308(a)(3)(ii)(A)	Addressable	Compliant
11			Workforce Clearance Procedure	164.308(a)(3)(ii)(B)	Addressable	Compliant
12			Termination Procedures	164.308(a)(3)(ii)(C)	Addressable	Compliant
13		Information Access Management		164.308(a)(4)(i)	Required	Compliant
15			Access Authorization	164.308(a)(4)(ii)(B)	Addressable	Compliant
16			Access Establishment and Modification	164.308(a)(4)(ii)(C)	Addressable	Compliant
17		Security Awareness Training		164.308(a)(5)(i)	Required	Compliant
18			Security Reminders	164.308(a)(5)(ii)(A)	Addressable	Compliant
19			Protection from Malicious Software	164.308(a)(5)(ii)(B)	Addressable	Compliant
20			Log-in Monitoring	164.308(a)(5)(ii)(C)	Addressable	Compliant
21			Password Management	164.308(a)(5)(ii)(D)	Addressable	Compliant
22		Security Incident Procedures		164.308(a)(6)(i)	Required	Compliant
23			Response and Reporting	164.308(a)(6)(ii)	Required	Compliant

Item	Safeguard	Standard	Implementation Specification	HIPAA Citation	Implementation	Attestation
24		Contingency Plan		164.308(a)(7)(i)	Required	Compliant
25			Data Backup Plan	164.308(a)(7)(ii)(A)	Required	Compliant
26			Disaster-Recovery Plan	164.308(a)(7)(ii)(B)	Required	Compliant
27			Emergency Mode Operation Plan	164.308(a)(7)(ii)(C)	Required	Compliant
28			Testing and Revision Procedures	164.308(a)(7)(ii)(D)	Addressable	Compliant
29			Applications and Data Criticality Analysis	164.308(a)(7)(ii)(E)	Addressable	Compliant
30		Evaluation		164.308(a)(8)	Required	Compliant
31		Business Associate Contracts and Other Arrangements		164.308(b)(1)	Required	Compliant
32			Written Contract	164.308(b)(4)	Required	Compliant
33	Physical	Facility Access Controls		164.310(a)(1)	Required	Compliant
34			Contingency Operations	164.310(a)(2)(i)	Addressable	Compliant
35		Facility Security Plan		164.310(a)(2)(ii)	Addressable	Compliant
36			Access Control and Validation Procedures	164.310(a)(2)(iii)	Addressable	Compliant
37			Maintenance Records	164.310(a)(2)(iv)	Addressable	Compliant
38		Workstation Use		164.310(b)	Required	Compliant
39		Workstation Security		164.310(c)	Required	Compliant
40		Device and Media Controls		164.310(d)(1)	Required	Compliant
41			Disposal	164.310(d)(2)(i)	Required	Compliant
42			Media Reuse	164.310(d)(2)(ii)	Required	Compliant
43			Accountability	164.310(d)(2)(iii)	Addressable	Compliant
44			Data Backup and Storage	164.310(d)(2)(iv)	Addressable	Compliant
45	Technical	Access Control		164.312(a)(1)	Required	Compliant
46			Unique User Identification	164.312(a)(2)(i)	Required	Compliant
47			Emergency Access Procedure	164.312(a)(2)(ii)	Required	Compliant

Item	Safeguard	Standard	Implementation Specification	HIPAA Citation	Implementation	Attestation
48			Automatic Logoff	164.312(a)(2)(iii)	Addressable	Compliant
49			Encryption and Decryption	164.312(a)(2)(iv)	Addressable	Compliant
50		Audit Controls		164.312(b)	Required	Compliant
51		Integrity		164.312(c)(1)	Required	Compliant
52			Mechanism to Authenticate Electronic PHI	164.312(c)(2)	Addressable	Compliant
53		Person or Entity Authentication		164.312(d)	Required	Compliant
54		Transmission Security		164.312(e)(1)	Required	Compliant
55			Integrity Controls	164.312(e)(2)(i)	Addressable	Compliant
56			Encryption	164.312(e)(2)(ii)	Addressable	Compliant

ATMP Solutions Overview

Applied Technology Methods and Practices (ATMP Solutions), a Michigan based company, has a proven model to ensure physicians, medical clinics and health systems are meeting HIPAA standards and implementing effective HIPAA management practices.

With increased federal regulation and evolving technology, medical practices and covered entities are mandated to comply with higher security standards for electronic protected health information, such as medical records and patient billing. Recognizing these challenges, ATMP Solutions provides critical services to help large health systems, insurance companies, home health agencies, long-term care facilities, medical billing companies, and physician practices assess their security risks and manage compliance with the Health Insurance Portability and Accountability (HIPAA) Act.

The HIPAA Security Compliance Assessment is an accurate and thorough analysis of an organization's current HIPAA compliance status. This includes a deep examination of electronic medical record management and software. ATMP Solutions conducts a Risk Assessment and Gap Analysis and assists in developing a remediation plan that leads to compliance.

Scoping Accuracy Validation

ATMP assisted Cogitate in the development of a HIPAA compliance gap analysis and recommendation set. A three-part approach was taken to develop this assessment. This three-part approach consisted of Interviews and Compliance Document Collection, Preparation of a Gap Analysis and Recommendation Set, and Asset Delivery.

ATMP Solutions has validated that the scope of this assessment, based on all information provided by Cogitate, Inc. and discovered by ATMP Solutions during the testing phases, is accurate and Cogitate, Inc. is taking steps to show reasonable effort to secure Cogitate, Inc.'s environment as it aligns with the HIPAA Privacy and Security model.

Cogitate Data Environment Overview

The scope of work for this assessment included the following environments:

- Applicable Networks
- Firewalls
- Routers
- Switches
- Servers
- Workstations
- Applications
- Network Connectivity and Transmission Links
- The following procedural reviews and technical discovery interviews were conducted
    - Existing HIPAA Privacy and Security Policies were manually reviewed
    - Physical security and privacy assessments of Cogitate, Inc. environments were conducted
    - Discovery interviews with both Management and their respective staff.

Interviewee List

ATMP Solutions interviewed the following people during the course of this assessment.

Name	Title	Organization	Topics Discussed
George Loescher	President	Cogitate, Inc.	Scope of Work Business Associates Compliance Assessment

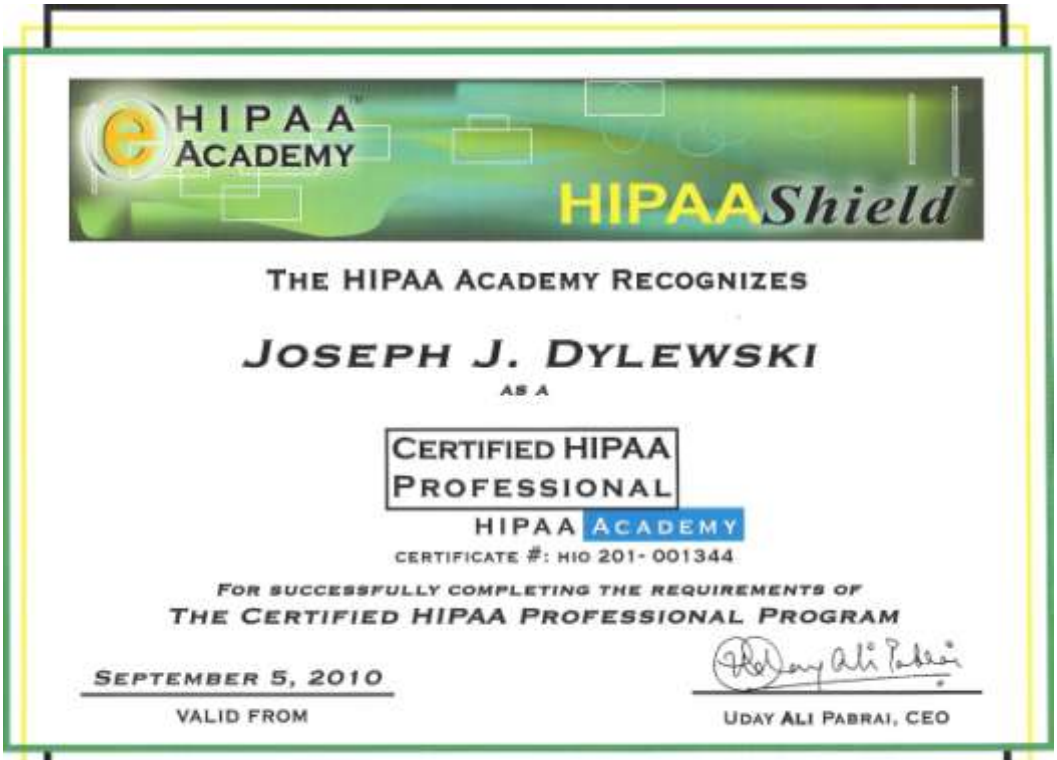
Build and Maintain a Secure HIPAA Environment

HIPAA compliance is not a one-time event. Once you have achieved HIPAA compliance, you are not finished with your efforts. You must now work to ensure your organization stays compliant. This may become challenging in an environment where there are many facilities in different locations, or where the organization is large and maintains constantly changing systems and networks.

The overall goal of HIPAA is to provide insurance portability, fraud enforcement, and administrative simplification for the healthcare industry. HIPAA was formed out of the growing concerns about keeping healthcare information private, the need to consolidate nonstandard healthcare data and transaction formats, as well as the general consensus to streamline healthcare operations and reduce the cost of providing healthcare services.

All systems must be protected from unauthorized access from non-trusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from non-trusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network

Appendix A - Assessor Certifications



HIPAA ACADEMY

HIPAAShield

THE HIPAA ACADEMY RECOGNIZES

JOSEPH J. DYLEWSKI

AS A

CERTIFIED HIPAA PROFESSIONAL

HIPAA ACADEMY

CERTIFICATE #: HIO 201- 001344

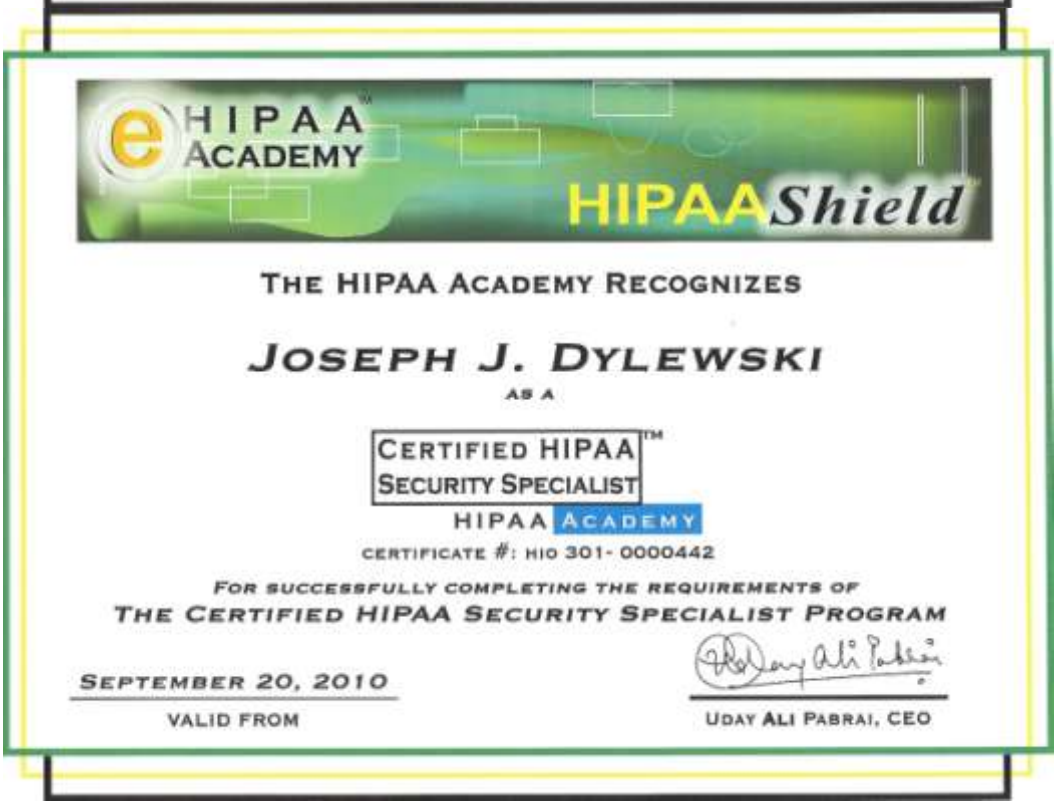
FOR SUCCESSFULLY COMPLETING THE REQUIREMENTS OF

THE CERTIFIED HIPAA PROFESSIONAL PROGRAM

SEPTEMBER 5, 2010

VALID FROM

UDAY ALI PABRAI, CEO



HIPAA ACADEMY

HIPAAShield

THE HIPAA ACADEMY RECOGNIZES

JOSEPH J. DYLEWSKI

AS A

CERTIFIED HIPAA™ SECURITY SPECIALIST

HIPAA ACADEMY

CERTIFICATE #: HIO 301- 0000442

FOR SUCCESSFULLY COMPLETING THE REQUIREMENTS OF

THE CERTIFIED HIPAA SECURITY SPECIALIST PROGRAM

SEPTEMBER 20, 2010

VALID FROM

UDAY ALI PABRAI, CEO