# Audit of HIPAA compliance for BAA of Utah DOH

2016-02

July 18, 2017

Utah Office of
Inspector General

**Gene Cottrell**
Inspector General

July 18, 2017

To: Utah Department of Health

Please see the attached report, Audit of HIPAA compliance for BAA of the Utah DOH**,** (Report 2016-02). An Executive Summary is included at the inception of this report. The objectives and scope of the audit are explained on page 2 of this report.

Sincerely,

Gene Cottrell
Inspector General
Utah Office of Inspector General

cc: Joseph Miner, Nathan Checketts, Shari Watkins, Emma Chacon, Aaron Eliason, Melanie Henderson

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The Utah Department of Health (DOH) Division of Medicaid and Health Financing (DMHF) Privacy/Security office is responsible for maintaining records of all Business Associate Agreements (BAA) issued by Medicaid. Any Medicaid program manager has the ability to issue contracts representing Medicaid with proper final approval. Health Insurance Portability and Accountability Act (HIPAA) standards require that all covered entities have written agreements with a business associate that performs functions on behalf of the covered entity that involve protected health information (PHI). The Privacy/Security office tracks compliance of contractors to the BAA. Under the HIPAA rule, Subtitle F Section 1171 (5) (E), DOH/Medicaid is a covered entity.

The department has developed a SharePoint program that guides the contractee through a process and requires answers to determine if a contract will also require a BAA from the contracted. The BAA contract used by DMHF, complies with suggested elements from Health and Human Services (HHS).

**Audit Objectives:**

- Determine if the Utah DMHF has BAAs with necessary entities.
- Determine if the business associates of Utah DMHF are in compliance with BAA's.

**Audit Scope:**

The scope of the audit will cover the current list of BAA's on file with DMHF Privacy/ Security office.

**Audit Findings:**

**Finding 1: The BAA list should contain all BAAs issued by DMHF.**

The list of BAA's should be only those issued by the DMHF. The list provided included others issued by Department of Technology Services (DTS). All required BAA's are not included on the list. The list should include all local Health Departments as part of the main list. Stated in Code of Federal Regulations (CFR) 160.103 (i) "On behalf of such covered entity", or those issued by the covered entity. DTS has a BAA with DOH. This finding was also part of a prior audit performed by the Office of Internal audit (OIA).

**Finding 2**: **Recertification letters are not current.**

The determination of annual compliance with BAA's and contractors are not current. The issuing of annual recertification letters to contracted entities on an unscheduled basis is not current. A plan to send all letters in the same month with annual due dates of the same month is being developed by the Privacy/Security office, but not issued as of the audit.

**Observation: Privacy/Security office lacks copy of final prior audit report by OIA.**

The Privacy office does not have a copy of final prior audit report performed by the OIA.

# INTRODUCTION

## BACKGROUND

The Utah Department of Health as the designated single state agency for the state of Utah with responsibility of the administration of the State Medicaid program is a covered entity for HIPAA regulations. Regulations allow a covered entity to contract with providers of required services that use PHI, with a BAA. The written BAA used by the DMHF meet requirements set forth by HHS.

Medicaid program managers can draft a contract as needed with service suppliers. Top management signs approved contracts. DMHF has developed procedures with the use of SharePoint that help in determining if the contractor also requires a BAA issued to cover all HIPAA requirements involving PHI.

The DMHF office of Privacy/Security has the responsibility for maintaining and tracking eligibility of contractors with DMHF that also require a BAA. CFR 164.308 requires that a covered entity implement policies and procedures to detect security violations. The first step in detecting is knowing what contractors sign a BAA. In this process, a list of contractors with signed BAAs, issued by the covered entity is necessary.

The DMHF office of Security as part of the requirement in CFR 164.308 to detect and contain security violations has developed a non-standardized form "Certification of Compliance" to allow BAA contractors to attest to HIPAA requirements applicable to PHI. The form reminds the contractor of the requirements agreed to in the BAA contract. The Security office will on an unscheduled basis request the certification from BAA contracted suppliers.

## OBJECTIVES AND SCOPE

### Audit Objectives:

- Determine if the Utah DMHF has BAA with necessary entities.
- Determine if the business associates of Utah DMHF are in compliance with BAA's.

### Audit Scope:

The scope of the audit will cover the current list of BAA's on file with the DMHF Privacy/Security office.

## METHODOLOGY

To determine if Utah DMHF has BAAs with necessary entities and if the contracted entities comply with the requirements, the Utah Office of Inspector General (Utah OIG) did the following:

- Researched the definition of a Business Associate Agreement. (BAA) by CMS.
- Researched what group or person CMS considers a BAA.
- Researched the need and requirements of HIPAA regulations relating to BAAs.
- Researched the requirements of a BAA contract as stated by HHS.
- Researched the definition of a covered entity.
- Determined what office within the DOH is responsible for BAA issuing and tracking.
- Requested and receive a copy of the BAA template.
- Requested information about procedures that determine need for a BAA.
- Requested information about ongoing compliance of contracted to BAA regulations.
- Requested information on control over approval and issuing a BAA.
- Requested and receive a list of Medicaid suppliers with BAA contracts.
- Requested and receive copies of current BAA contracts.
- Requested and receive copies of "Certification of Compliance" letters.
- Requested and received DMHF contracting and BAA needed, flow chart.
- Compared copies of BAAs to List of BAAs.
- Compared copies of "Certification of Compliance" letters to list of BAAs.
- Requested copy of prior audits performed on BAA compliance.
- Received from Privacy/Security Office a draft copy of the prior audit performed.
- Received from Prior Audit Manager copy of Final prior audit performed.
- Evaluated prior audit findings and recommendations for adoption.

## CONCLUSIONS

The list of BAAs provided is a combination of BAA contracts issued by DMHF and DTS. A separate list includes all County Health Departments. The list does not include all BAAs issued by DMHF. A copy of a BAA contract provided did not appear on the list. A BAA contract and a Certification of Compliance letter did not have signatures. An unsigned document is not a final enforceable document.

The Recertification or "Certification of Compliance" letters are not standardized making issuing of letters more difficult. Compliance recertification is inconsistent. Based on the prior audit performed by the OIA, management's response states that the business associate would be required on an annual basis to provide statements of certification. Compliance to CRM 164.308 requires a covered entity to detect and contain security violations.

The Security office presented proposals of changes to the process, but are not in place at beginning of audit.

| FINDING 1 | The BAA list should contain all BAAs issued by DOH |
|---|---|

CFR 164.502 (e) (1). A covered entity must obtain satisfactory assurances that the business associate will appropriately safeguard PHI. BAAs issued are for the covered entity to manage in its protection and controlled release of PHI. The first step in the management of BAAs issued should be a list of the issued documents. A requirement for a list of BAAs issued by DMHF was a finding on a prior audit performed by the OIA. A list should be all inclusive of documents issued and under the management of the responsible office. OIG found the following deficiencies in the list provided:

- The list contained contracts issued by DTS
- The list contained a contract that is not a BAA.
- A copy of a BAA provided was not on the list.
- A list of local Health departments was separate and should be included in the list of all BAAs.

CFR 164.308 security management process includes policies and procedures to prevent, detect, contain and correct security violations. An unsigned document is not a final enforceable document.

- A copy of a BAA provided did not have signatures and was not part of a larger contract. The UOIG reviewed a number of BAAs that were unsigned but part of a larger contract which govern the BAA therefore not requiring signatures. It is suggested that if a BAA is attached as part of a contract that the unneeded signature page be removed or noted that no signature is required.

CFR 164.316 specifications stated must be reasonable and appropriate safeguards for the protecting of health information.

- The security office should have on file all signed final copies of BAAs.

**Recommendations**

1.1 The list should only contain DMHF issued, finalized and signed BAAs.

1.2 The list should contain all BAAs issued by DMHF and updated with newly issued BAAs.

| FINDING 2 | Recertification letters are not current. |
|---|---|

The determination of BAAs annual compliance with contracted are not current. The issuing of annual recertification letters to contracted entities on an unscheduled basis is not current and inconsistent with prior agreements. A prior audit performed by the OIA, management's response states that the business associate would be required on an annual basis to provide statements of certification.

A plan to send all letters in the same month with annual due dates of the same month is being purposed and developed by the security office, but not issued as of the audit date.

**Recommendations**

2.1 Complete the process of standardizing the recertification letter

2.2 Complete the process of issuing and tracking the return of the recertification letter. Issuing the recertification letter for all BAA contracts in the same month.

| OBSERVATION | Privacy/Security Office lacks a copy of prior final audit report. |
|---|---|

The Privacy/security office should have a copy of the final prior audit report performed by the OIA to enable implementation of recommendations and corrections from findings and audit follow-up.

**Recommendation**

3.1 The Privacy/Security office should keep on file copies of all final prior audit reports involving the office.

3.2 The Privacy/Security office should make sure that all recommendations agreed to by management are implemented going forward.

# GLOSSARY OF TERMS

The first use of each term is described in the report. The glossary is included to help ensure easier reading.

| Term | Description |
|---|---|
| BAA | Business Associate Agreement |
| CFR | Code of Federal Regulations |
| CMS | Centers for Medicare & Medicaid Services |
| DMHF | Division of Medicaid & Health Financing |
| DOH | Utah Department of Health |
| HHS | Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act |
| OIA | DOH Office of Internal Audit |
| OIG | Utah office of Inspector General over Medicaid |
| PHI | Protected Health Information |

# MANAGEMENT RESPONSE

State of Utah

GARY R. HERBERT
*Governor*

SPENCER J. COX
*Lieutenant Governor*

**Utah Department of Health**

JOSEPH K. MINER, MD, MSPH, FACPM
*Executive Director*

**Division of Medicaid and Health Financing**

NATE CHECKETTS
*Deputy Director, Utah Department of Health*
*Director, Division of Medicaid and Health Financing*

July 27, 2017

Gene Cottrell
Inspector General
Office of the Inspector General of Medicaid Services
P.O. Box 14103
Salt Lake City, Utah 84114

Dear Mr. Cottrell:

Thank you for the opportunity to respond to the audit entitled *Audit of HIPAA Compliance for BAA of Utah DOH* (Report Number 2016-02). We appreciate the effort and professionalism of you and your staff in this review. Likewise, our staff spent time collecting information for your review, answering questions, and planning changes to improve the program. We believe that the results of our combined efforts will make a better, more efficient program.

We concur in part with the recommendations in this report. Our response describes the actions the Department plans to take to implement the recommendations. The Department of Health is committed to the efficient and effective use of taxpayer funds and values the insight this report provides on areas that need improvement.

Sincerely,

Nate Checketts

Nate Checketts
Deputy Director, Department of Health
Division Director, Medicaid and Health Financing

UTAH DEPARTMENT OF HEALTH

288 North 1460 West · Salt Lake City, UT
Mailing Address: P.O. Box 143101 · Salt Lake City, UT 84114-3101
Telephone (801) 538-6689 · Facsimile (801) 538-6478 · www.health.utah.gov

[Insert

*Response to Recommendations*

Recommendation 1.1

*The list should only contain DMHF issued, finalized and signed BAAs.*

Department Response:

DMHF concurs. DMHF provides the following clarifying information. DMHF can generate a separate list of active BAAs from the list maintained by DMHF for all BAAs entered into by the Division. The list can be filtered and notated to differentiate between current BAAs in effect and those that have expired due to a change in circumstance or situation. Business associates may have continuing obligations under the BAA to protect PHI until return or destruction of PHI becomes feasible, which may occur after the contract is terminated.

Due to DMHF's statutory relationship with the Department of Technology Services (DTS), a Medicaid business associate, DMHF works closely with DTS on contracts DTS has with subcontractors who create, receive, transmit, or maintain DMHF ePHI on behalf of DTS. DMHF tracks these BAAs for its own purposes, including exercising due diligence in performing oversight functions. DMHF will continue to maintain a list of BAAs its business associates have entered into with subcontractors regarding ePHI when deemed necessary.

*Contact: Blake Anderson, Privacy Officer, DMHF 801-538-9925*
*Implementation Date: September 1, 2017*

Recommendation 1.2

*The list should contain all BAAs issued by DMHF and updated with newly issued BAAs.*

Department Response:

DMHF concurs. As part of the SharePoint contracting process, DMHF will add new BAAs to its existing list. During the course of the audit, DMHF provided a copy of a BAA not on the initial list furnished to the auditors and the list was updated at that time. In addition, each annual local health department contract will be listed separately.

*Contact: Blake Anderson, Privacy Officer, DMHF 801-538-9925*
*Implementation Date: Implemented*

Recommendation 2.1

*Complete the process of standardizing the recertification letter.*

Department Response:

DMHF concurs in part. We provide the following clarifying information. Because of timing issues in the development and approval of contracts, the use of a standard recertification letter has not been feasible in all situations. DMHF monitors business associates through different methods based on the level of risk a business associate presents to DMHF. One method DMHF currently uses is through statements where a business associate can certify and attest to data security. The recertification letter has been standardized to the extent practicable.

*Contact: Blake Anderson, Privacy Officer, DMHF 801-538-9925*
*Implementation Date: Implemented*

Recommendation 2.2

> *Complete the process of issuing and tracking the return of the recertification letter. Issuing the recertification letter for all BAA contracts in the same month.*

Department Response:

DMHF concurs in part. We provide the following clarifying information. Not all business associates need to attest to data security on an annual basis. For example, local health department contracts may be renewed on an annual basis and if so, a new contract and BAA attachment are signed each year. Any business associate attestation of data security measures are tracked by DMHF.

*Contact: Blake Anderson, Privacy Officer, DMHF 801-538-9925*
*Implementation Date: Implemented*

Observation 3.1

> *The Privacy/Security office should keep on file copies of all final prior audit reports involving the office.*

Department Response:

DMHF appreciates this observation and will maintain a copy of the only previous audit and this audit.

*Contact: Blake Anderson, Privacy Officer, DMHF 801-538-9925*
*Implementation Date: Implemented.*

Observation 3.2

*The Privacy/Security office should make sure that all recommendations agreed to by management are implemented going forward.*

Department Response:

DMHF concurs with this observation and will implement recommendations agreed to by management.

*Contact: Blake Anderson, Privacy Officer, DMHF 801-538-9925*
*Implementation Date: Implemented*

# EVALUATION OF MANAGEMENT RESPONSE

Medicaid management concurs in part with the findings and recommendations of this report.

The following are UOIG evaluations of management's response to each recommendation.

**Response to Recommendation 1.1**, Management concurs with clarifying information:

UOIG based its findings on information requested and received from DMHF for the audit stated. The ability to filter the list into needed arrangements is commendable going forward, however a demonstration did not occur to UOIG of that ability for the audit. DMHF is not clear in its statement if this is a new feature of the listing of BAAs. UOIG recognized the possible need for a separate list of DTS issued BAA contracts as well as other possible needs and stated so during both Pre Draft and Exit conference meetings. Based on the prior audit by OIA, DMHF concurred with the need of a list of BAA contracts managed by DMHF. Co-mingling of BAAs from other sources with those managed by DMHF on the master list would not comply with the recommendation. UOIG recommends DMHF comply with the recommendation in full for a master list of only BAA's issued by DMHF.

**Response to Recommendation 1.2**, Management concurs:

DMHF should understand that the audit scope covers a point in time. Documents provided by DMHF are included in the examination and evaluation based on the request made.

**Response to Recommendation 2.1**, Management concurs in part:

UOIG determined that the response is acceptable with continued efforts to comply with the recommendation going forward.

**Response to Recommendation 2.2**, Management concurs in part:

The statement "Any business associate attestation of data security measures are tracked by DMHF", going forward UOIG anticipates compliance to the recommendation. Evidence received during the audit shows the need for improvement in timely issuing and tracking of recertification letters. Based on the management response to Recommendation 2 from the OIA audit, DMHF concurred that an annual recertification would take place. If that recertification is with a new BAA contract, it is acceptable to UOIG.

**Response to Observation 3.1 and 3.2**, Management concurs:

UOIG issues recommendations in an effort to improve functions and ensure compliance to laws, rules and guidelines set forth for the management of HIPAA, BAA contracts. DMHF should keep copies of "all" future audits as well as this audit and the OIA audit and implement all recommendations when feasible.

# UTAH OIG CONTACTS AND STAFF ACKNOWLEDGEMENT

**UTAH OIG CONTACT**

Dennis Hooper CIGA
Auditor

Neil Erickson
Audit Manager

**UTAH OIG MISSION STATEMENT**

The Utah Office of Inspector General will enhance the integrity of the Utah State Medicaid program by preventing fraudulent, abusive, and wasteful practices within the Medicaid program and recovering improperly expended Medicaid funds while promoting a high quality of patient care.

**ADDRESS**

Utah Office of Inspector General
Martha Hughes Cannon Health Building
288 N 1460 W
Salt Lake City, Utah 84116

**OTHER**

Website: http://www.oig.utah.gov/
Hotline: 855.403.7283