UCIrvine | Internal Audit Services

Business Associate Agreements

Internal Audit Report No. I2020-204

June 30, 2020

Prepared By
Will Simonian, Senior Auditor
Darlene Nuñez, Senior Auditor
Reviewed By
Niran Joshi, Associate Director
Approved By
Mike Bathke, Director

UNIVERSITY OF CALIFORNIA, IRVINE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

INTERNAL AUDIT SERVICES
IRVINE, CALIFORNIA 92697-3625

June 30, 2020

SNEHAL BHATT
CHIEF PROCUREMENT OFFICER & DIRECTOR OF PROCUREMENT SERVICES
DIVISION OF FINANCE & ADMINISTRATION

SUSANNA RUSTAD
EXECUTIVE DIRECTOR, SUPPLY CHAIN MANAGEMENT & SUPPORT OPERATIONS
UCI HEALTH

RE: Business Associate Agreements Audit
Report No. I2020-204

Internal Audit Services has completed the review of the Business Associate Agreements and the final report is attached.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. If you have any questions or require additional assistance, please do not hesitate to contact me.

Mike Bathke
Director
Internal Audit Services

Attachment

C: Audit Committee

I. MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2019-2020 audit plan, Internal Audit Services (IAS) reviewed internal controls and practices when contracting for services that require a Business Associate Agreement - Appendix (BAA) to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) regulations. The review identified some internal control processes that could be improved to minimize compliance risks and ensure utilization of best business practices.

While IAS noted improvement opportunities, there was a significant transitional period that occurred in 2017 and that continues to improve significantly the negotiation, review, execution, monitoring, and maintenance processes of BAAs.

The following observations were noted:

Managing, Monitoring, and Maintaining BAAs – Twelve percent of vendor BAAs tested at the Medical Center (MC) were not maintained in a digital repository because those BAAs were still being negotiated or otherwise provided at a later time manually. Twenty-three percent of the vendors tested utilized an older, yet still applicable, University of California Office of the President (UCOP) version of the BAA. Fifty percent (40 percent - School of Medicine (SOM)/Campus, 10 percent - MC) of tested BAA-exempt vendors were not properly documented in the database as not having access to Protected Health Information (PHI) and thereby not requiring BAAs. These observation details are discussed in section V.1.

II. BACKGROUND

PHI may be disclosed by UC to a business associate (BA)[1] and may allow this individual/organization to create or receive such information on its behalf if UC obtains satisfactory assurances that the BA will appropriately safeguard the PHI.

HIPAA privacy regulations require satisfactory assurances to be provided in the form of a BAA that contains certain elements specifically enumerated in the regulations.

[1] The Department of Health and Human Services (HHS) guidance generally defines a business associate as a person or organization who performs certain services for covered entities (i.e., healthcare providers who electronically transmit any health information and usually having direct contact with patients) and other business associates that involve the use or disclosure of PHI.

The Office of General Counsel, Health Law Group, has developed a standard UC system-wide BAA that must be used. An annotated version of the BAA is available that provides guidance when using the BAA. Changes to the BAA, beyond those allowed in the annotated version, must be reviewed and approved by a local UC Health Privacy Officer and/or UC Health Privacy Lawyer.

MC Procurement/Contracting and Contracting is the gatekeeper of the BAAs, and as such, they will identify the contracts that require BAAs, as they are responsible for negotiating and executing vendor contract agreements. If Procurement experiences vendor pushback towards BAAs, they will contact SOM Privacy and Compliance who will advise them when necessary. Vendor pushback may occur for a multitude of reasons, such as the following:

- Vendor questioning as to why a BAA is required;
- Vendor requesting UCI to utilize their version of a BAA;
- Redlines were made to the UCOP BAA template;
- Vendors attempt to limit their liability by attempting to renegotiate more favorable indemnification terms into the BAA or Agreement; and
- Vendor requesting artificial limited liability caps to be added to the BAA to limit their exposure to liability, fines, and other disciplinary actions if a breach were to occur.

As mentioned above in section I, since 2017, significant transitions occurred at UCIMC due to management's shift in focus along with departmental/staffing changes, which greatly improved the BAA process in regards to negotiation, review, execution, monitoring, and maintenance of BAAs.

In July 2018, MC Procurement/Contracting collaborated with Privacy/Compliance to locate all known BAAs and to begin the process of converting these documents into a digital format. MC Procurement/Contracting also hired a fulltime Contracts Manager and a fulltime Business Analyst to assist with locating all BAAs throughout the MC.

Since the partnership of MC Procurement/Contracting and Privacy/Compliance, the following improvements either have been implemented or are underway.

1) These departments collectively review and identify BAA needs based upon legacy information.

2) In quarters two and three of calendar year 2018, Privacy/Compliance collected all known paper copy and digital copy BAAs. Privacy/Compliance digitized all known BAAs and created two shared temporary repository locations. The first location in an archive-type of all BAAs collected and digitized, and the second is an ancillary location, Privacy/Compliance dubbed "the Backlog List," where BAAs that Privacy/Compliance has initially identified as requiring review are stored and addressed. As such, Privacy/Compliance shares with MC Procurement/Contracting this temporary new digital database storing all digital BAAs on a Privacy/Compliance owned and controlled SharePoint and shared drive.

3) Paper copies of BAAs and associated contracts are not preferred and are no longer distributed to vendors.

4) MC Procurement/Contracting reviews all new and renegotiated/redlined BAAs, and seeks input from Privacy/Compliance, in addition to Information Technology (IT), UCI Legal, and Risk Management, when applicable, throughout all negotiations, prior to execution. The Contract Administrator collects the email confirmation from each department, as necessary, which are then stored with the digital contract documents for historical approval purposes.

5) MC Procurement/Contracting and Privacy/Compliance collectively, review current MC vendors, and through an analysis of risk-based priorities, determine which vendors to approach for renegotiations of the BAA (which sometimes leads to a renegotiation of the Master Agreement). Note: risk-based priorities are determined by analyzing the type of vendor/service category, level of spend of the vendor at the MC, and the anticipated size of a potential data breach. This analysis is time consuming and must be completed one vendor at a time.

6) Upon successful implementation of a contracts repository, which is nearly complete, all BAAs will be housed with their respective agreement(s) and maintained by MC Procurement/Contracting.

III. PURPOSE, SCOPE, AND OBJECTIVES

The purpose of the audit was to perform a review on the internal controls and practices when contracting for services that require a BAA to ensure compliance with HIPAA regulations. The audit scope included current vendors who provide services (note: vendors who provide goods to UCI generally do not require BAAs) for the MC and SOM/Campus. Note that SOM/Campus have very few vendors who require BAAs.

IAS conducted testing of randomly selected vendor service agreements predominantly from two listings to determine how BAAs were being managed, monitored, and maintained. MC Procurement/Contracting provided IAS a list of all current MC vendor service engagements that may have, at one time or another, required a BAA. The other listing was comprised of vendor engagements that Privacy/Compliance had utilized as an archive to store all digitized BAAs, which they had singled out as higher risk. As such, they were researching these agreements, along with MC Procurement/Contracting, to resolve various BAA related issues.

Lastly, since SOM/Campus had very few BAA vendors, only a few samples were selected from a third listing of current SOM/Campus vendor service agreements provided by the SOM/Campus Procurement.

IAS omitted a review of the UC Data Security and Privacy Appendix (DSA) from this audit because IT Security and MC Procurement/Contracting is responsible for negotiating this appendix with the vendors and because all PHI HIPAA restrictions are contained and governed by the BAA. Note that standard business practice at UCI normally follows that if a vendor has access to PHI data, then both a BAA and a DSA would be required, although exceptions occur based upon what is being purchased, at that time, from the vendor.

The audit included the following objectives:

1. Determine whether BAAs are properly managed, monitored, and maintained.

2. Conduct testing to identify whether the proper BAA template version was used and included the most current HIPAA regulations.

3. Test the BAA process to determine that a BAA is properly executed with the BA prior to allowing the BA access to UCI's PHI data.

4. Identify if there is a process in place to determine whether a BAA is required from a vendor.

5. Inquire if a material breach or violation by a BA has been identified, that reasonable steps were taken to cure the breach, or the violation was ended. Otherwise, if unsuccessful, then the contract with the BA is terminated or issues are reported to the Department of Health and Human Services Office for Civil Rights.

IV. CONCLUSION

Some internal controls related to BAAs could be improved upon. IAS noted concerns regarding managing, monitoring, and maintaining BAAs.

IAS discussed observation details with management who formulated action plans to address the issues. IAS presents these details below.

V. OBSERVATIONS AND MANAGEMENT ACTION PLANS

1. Managing, Monitoring, and Maintaining BAAs

A. BAA Digital Repository

Background

A digital repository is a central file storage location for managing and accessing digital content. It is useful in that it allows the following features and advantages over a traditional standard hardcopy filing system.

- Limitless storage capability without occupying large physical space.
- Accessibility of files are more readily available to multiple end users and can be accessed simultaneously by multiple users.
- Information retrieval is more readily available, user-friendly, and versatile by entering a multitude of possible search terms (e.g., word, phrase, title, name, subject, date, etc.) to search the entire database for specific needs/requests.

- Improved monitoring and management by setting up alerts and notifications in the application to identify when a document requires updating or other modifications.
- Preservation and conservation of materials that would otherwise deteriorate from repeated use. Backup of files also preserves the files in this regard.
- Security control capabilities by limiting accessibility to the files to certain individuals/departments.

As mentioned in section II above, MC Procurement/Contracting partnered with Privacy/Compliance to locate all known BAAs and Privacy/Compliance has converted them into digital format, while temporarily retaining custody and control of all BAAs. IAS tested BAAs in this audit to determine whether a centralized digital repository is being used consistently and as the primary storage database to monitor and maintain all BAAs and corresponding vendor agreements. It is important to note that the need for a BAA is driven, not by the vendor, but by what the vendor does for MC. Specifically, whether the vendor has access to PHI, even by accident. There are many instances where a vendor initially contracts with MC, and then the nature and scope of that engagement changes over time to require or eliminate the need for a BAA. As such, the need for a BAA is engagement driven and not vender centric.

Observation

Of 34 vendors tested for MC, four (12 percent) did not have a corresponding BAA maintained in the previously mentioned digital repository maintained by MC Procurement/Contracting and Privacy/Compliance. In addition, two of these four vendors were missing vendor agreements in the repository. IAS noted there were many other vendor agreements missing from the repository, however, IAS excluded these from the test results as long as the BAAs were included, since BAAs were the primary focus of this audit. IAS also noted that hardcopy files exist of these agreements and that BAAs were missing from the repository; however, for testing purposes, IAS specifically focused on whether these documents were in a digital repository.

As mentioned in section II above, a digital repository offers many advantages over standard physical storage of hard copy files in regards to managing, monitoring, and maintenance of BAAs. Although MC Procurement/Contracting has come a long way in digitizing BAAs and corresponding vendor agreements, improvement is ongoing in this area to

ensure all BAAs and vendor agreements are being stored in a digital repository.

In addition to the observations noted above, both the MC and Campus Procurement departments took some time to provide IAS with a requested current vendor listing, as both departments needed time to complete the listings to ensure they were sending up-to-date versions. As a best business practice, IAS recommends maintaining a current listing of vendors/BAA vendors. This listing should include other pertinent information such as the BAA version used; agreement expiration/renewal date (agreement renewal date can also be a good indicator/reminder to update/renegotiate the BAA version used, if necessary); vendor spend total; and why/how PHI is being used by the vendor. IAS notes that a robust and intuitive centralized digital repository should be able to generate a vendor listing at any time, feasibly and instantaneously.

Management Action Plan

Medical Center Procurement/Contracting

Explanations why the four vendor BAAs mentioned above were missing from the repositories are listed below.

- Two vendor BAAs were still being negotiated with the vendors while this audit was being conducted.

- One vendor had been purchased by another larger vendor during BAA negotiations, and the existing BAA from the larger vendor already met BAA requirements.

- One vendor already had a valid BAA in place which was later uploaded into the Privacy/Compliance shared drive.

Since 2017, significant transitions occurred at MC, which greatly improved the BAA process in regards to negotiation, review, execution, monitoring, and maintenance of BAAs.

In part, our MC Procurement/Contracting department partnered with the Privacy/Compliance department to locate all known BAAs and start the process of converting them to digital format. This continues to be a work in

progress priority for both departments to ensure all vendor BAAs and agreements are stored in a centralized digital repository. It should be noted that historically, Privacy/Compliance only wanted possession of the individual BAAs, not the contractual documents. Under the current and evolving partnership with Privacy/Compliance, they now receive the entire BAA related contract for full visibility, in case of a breach. The aforementioned Privacy/Compliance repositories were created by Privacy/Compliance for Privacy/Compliance and only contain BAAs. This partnership has been ever evolving, and has endured a large amount of employee attrition (from Privacy/Compliance) and unforeseen lengthy illness (from MC Procurement/Contracting). Nevertheless, both departments, through continued partnership, strive to protect PHI and have been successful, in that regard.

MC Procurement/Contracting is already in the process of implementing a concierge document service called LegalSifter, which sifts through vendor contracts, cleans/organizes document data, and stores important data in a cloud-based contract database called ContractSafe. These compatible applications also update old contracts by alerting end users of agreement end dates, renewals, and key contract activity. The applications also link master agreements with all other corresponding agreements, such as BAAs, and allows for unlimited usage of running filters on the database and generating useful reports. It is the intent of MC Procurement/Contracting to have a one-stop-shop for all vendor agreements, contracts, appendices, etc., to be digital in format, and to be visible and transparent to those individuals at MC whose job requires access to such information.

These aforementioned improvements that are currently underway should be implemented by December 1, 2020, as anticipated delays due to COVID-19 are accounted for in this estimated completion date.

It should also be reiterated that requiring a BAA is not vendor centric. Upon renegotiation of an engagement, whether a BAA is necessary can change based upon what is being purchased from that vendor at the time of contracting/ renewal/amendment.

Campus Procurement

Although Campus Procurement has a very small percentage of vendor agreements that require BAAs (approximately one to two percent of the total

population of vendors), they will maintain a listing of these BAA vendors with similar fields as mentioned in the Observation section above. This listing will be periodically updated and maintained. The implementation of this listing will be no later than October 31, 2020, as anticipated delays due to COVID-19 are also accounted for in this estimated completion date.

B. BAA Template

Background

There are several versions of BAA templates that have been used at UCI throughout the years. As HIPAA regulations have changed over the years, UCOP has periodically modified their template BAA, incorporating all of the applicable changes/updates. The Office of General Counsel, Health Law Group, has developed a standard system-wide BAA that is required to be used, but is also permitted to be redlined and modified. When a UCOP BAA is modified, it becomes a local BAA, only to be associated with that local vendor engagement.

One system-wide template BAA version that was currently being used, dated May 16, 2017, was superseded with a version dated August 1, 2019. Both of these versions include the most recent requirements of Health Information Technology for Economic and Clinical Health Act (HITECH)[2], which were incorporated into HIPAA in the Final Omnibus Rule, bringing HIPAA and HITECH together into the same legislation. The HIPAA Omnibus Final Rule was published in the first quarter of 2013 and had a compliance date of September 23, 2013.

Observation

Eight of 34 (24 percent) vendor BAAs tested at MC were prior UC BAA versions. The breakdown of these eight prior version BAAs consisted of the following:

- Five BAA versions were dated from 2013 to 2014;
- One BAA version was dated, 2009;

[2] The HITECH Act encouraged healthcare providers to adopt electronic health records (EHRs) and improved privacy and security protections for healthcare data. This was achieved through financial incentives for adopting EHRs and increased penalties for violations of the HIPAA Privacy and Security Rules.

- One BAA version was dated December 2015, with a corresponding Master Service Agreement (MSA) signed in December 2019; and
- One BAA did not contain a version date; however, the MSA Amendment was signed in November 2018.

Although MC Procurement/Contracting management (on advice from Privacy/Compliance) indicated during the audit that 2013 BAAs were acceptable because they included the most recent updated regulations (i.e., HITECH), there were still some regulatory/stipulation differences noted between the 2013 BAA version and the most recent 2017 and 2019 BAA versions.

MC Procurement/Contracting management also indicated that there is significant pushback from vendors in some cases when they are asked to update their BAA version to a more recent version. This is often due to vendor attorney costs and other related costs associated with reviewing updated/amended BAA documents. However, in a few of the observations noted above, the vendor MSAs were recently signed/renewed, which, evidently, may appear to have been an opportune time to also replace the older version BAAs with the most current versions and allow the vendors to review them at the same time as the MSAs.

As a best practice, the most current and updated BAA version should be used for all vendors to ensure regulatory uniformity and consistency throughout UCI and the UC system as a whole.

Management Action Plan

Medical Center Procurement/Contracting

As stated above in management action plan, implementation of the LegalSifter and ContractSafe applications will result in better monitoring and updating of BAAs, eventually ensuring that virtually all BAA templates used are identical. However, this will take time as MC Procurement/Contracting management's first priority is to ensure that all vendors who are required to have BAAs have valid BAAs already in place, that are at a minimum dated 2013, must contain the HITECH language, and/or approved by Privacy/Compliance.

It should be reiterated, since 2018, Privacy/Compliance and MC Procurement/Contracting have worked in concert, very diligently, to ensure

timely review of all current MC BAA relationships. This is a very large, detailed, and complicated effort. At that time, Privacy/Compliance management agreed with MC Procurement/Contracting management that Privacy/Compliance was best situated to temporarily maintain custody and control of all digital BAAs and to, review and reflect on the current MC vendor engagements. Privacy/Compliance would take the lead to contact vendors and address BAA concerns, looping in MC Procurement/Contracting as negotiations neared completion or failure. The update priority follows the level of potential risk involved with the services or data access of target vendors, starting with the highest risk first.

In addition, about 40 to 50 percent of the time when MC Procurement/Contracting management recommends to a vendor that a BAA version be updated, the vendor renegotiates by requesting an artificially limited liability cap be placed in the BAA language. This limits the vendor's liability exposure if a breach were to occur and/or the vendor attempts to alter the indemnification obligations to exclude BAA or HIPAA breaches. Consequently, sometimes updating a BAA version becomes more problematic because the vendor views it as an opportunity to leverage unrelated terms.

Both Privacy/Compliance and MC Procurement/Contracting are dedicated to ensuring that the University and its patients' PHI are properly protected. However, it should be understood, since 2018, during contract negotiations, all BAAs dated prior to the most recent version, at that time, are reviewed by Privacy/Compliance (and sometimes other departments), and Privacy/Compliance gives a final "green light-"type approval for continued usage or requires replacement language. As such, although the BAAs discussed above may be on older forms, Privacy/Compliance has approved their current use, and MC Procurement/Contracting must defer to Privacy/Compliance's judgment. It is MC Procurement/Contracting's responsibility to ensure Privacy/Compliance and/or Risk and/or Legal review and comment on relevant vendor redlines and suggested additions, and receive the "green light" to move forward toward execution of the BAA, or are provided reasons why the vendor relationship is not in the University's best interest. These approvals and rejections (via email) are verified and maintained by MC Procurement/ Contracting.

MC Procurement/Contracting will implement the LegalSifter and ContractSafe applications by December 1, 2020.

C. BAA Exemption Support Documentation

Background

When a vendor does not create, receive, maintain, or transmit PHI for/from a Covered Entity, then the vendor is not a Business Associate and does not require a BAA. In these situations, as a best business practice, support documentation should be provided in the digital repository validating and explaining why the vendors do not require BAAs.

Observation

Five of ten (50 percent) vendors (i.e., four vendors –SOM/Campus, one vendor – MC) who do not require BAAs were not documented as such in the respective database repository.

As a best practice, maintaining email from the vendor itself and/or correspondence from UC management (after the vendor is properly vetted and it is determined they do not use PHI data in any way, shape, or form), documents why the vendor does not require a BAA (e.g., vendor provides food services at the MC thereby not having any access to PHI data from UCI). Support documentation for BAA-exempt vendors is useful for not only audit purposes but also assists the departments' directly overseeing and monitoring vendor agreements and BAAs by having a documented record of vendors not requiring BAAs that can be referred to at any time.

This support documentation also serves as a quick reference when monitoring and comparing which vendors do not require BAAs in relation to those vendors who may have been inadvertently overlooked regarding their BAA status and thus who require further examination. If no support documentation exists indicating which vendors are legitimately BAA-exempt, then this distinction cannot easily be made and a vetting process must be conducted for each vendor not having a BAA to determine which vendors are BAA-exempt and which vendors were inadvertently overlooked. This process can result in workload inefficiencies and duplication of efforts of contract management job responsibilities.

Management Action Plan

Medical Center Procurement/Contracting

Going forward, MC Procurement/Contracting Department has implemented a process to provide support documentation for BAA relevant vendors who do not require BAAs. It needs to be understood that the majority of vendor engagements at MC do not require BAAs. Often times the type of purchase is very open, obvious, and historic whereby a BAA vetting process is a waste of University resources. For example, a one-time purchase of 100,000 N95 masks from a vendor will never result in the transmission of patient PHI, therefore, vetting that vendor/engagement and receiving green-light approvals is an obvious waste of time and precious resources. A blanket rule of "best practice" to vet all vendors resulting in written confirmation for those not needing/requiring BAAs, for this example above, would undoubtedly cause undue delay, potentially negatively affecting patient care as well as employees' own health protection. This is why it is important to remember HIPAA and BAA review is not vendor centric. This review is limited to engagements that could result, even by accident, in the unapproved transmission of PHI.

Support documentation will be in the form of vendor emails and/or UC management correspondence validating why the vendors are exempt from BAA requirements and do not have access to PHI data. As of fiscal year 2019, MC has already implemented this best practice. It should be noted, for the vendor identified in the Observation section, directly above, MC Procurement/Contracting had an email from the vendor, dated August 2019, confirming no PHI transfer or receipt is contemplated. In February 2020, MC Procurement /Contracting was finally able to obtain a confirmatory email from MC IT/IS. Within days of this support and confirmation email, all support documentation was, in fact, uploaded into Privacy/Compliance's shared drive. This was accomplished during the audit-testing phase herein, and should be reflected as completed, through no fault or delay attributable to the MC Procurement/Contracting.

Proper HIPAA BAA maintenance is not singular to MC Procurement/Contracting nor jointly to Privacy/Compliance, but is a University and MC-wide effort that must be instilled and re-addressed at every opportunity. Privacy/Compliance and MC Procurement/Contracting may have an intertwined responsibility to ensure BAA compliance; however, this responsibility falls directly on every employee of the University, especially at

MC and SOM to not violate HIPAA, to report HIPAA violations promptly, and to guide MC Procurement/Contracting through the contractually purchased engagement.

Campus Procurement

Since Campus Procurement only has about one to two percent of contracts requiring BAAs, this process recommended by IAS is a a very significant adminstrative burden on our very lean team to gather and log this information for 98 percent of our agreements that do not require BAAs. Although Campus Procurement understands the rationale for this recommendation as a best practice, it is not feasible for the disproportionate amount of agreements that actually do not require a BAA. Unless we are also given the funding to implement LegalSifter and ContractSafe, this manual tracking of vendor emails is not manageable with the existing staff. Campus Procurement has, in fact, put one of the vacant Contracts Analyst position on hold due to hiring restrictions resulting from COVID-19.