Statement of Work

Prepared for: YouBreakWeFix

September 16, 2023

Bit Dancing Studios
123 Some St.
Yourtown, IL 60547
https://bitsdanceforme.blog/

Point of Contact
Amy Devine
adevine@depaul.edu

Disclaimer: Statement of work is valid when signed before 2023-OCT-30.
This SOW is modeled off of Mandiant and ERS SOWs. See References.

1. Background **2**
2. Scope **2**
2.1. In Scope 2
2.1.1. Physical Testing 4
2.1.2. Network Breach Testing 4
2.1.3. Wireless Testing 5
2.1.4. People Testing 5
2.2. Out of Scope 5
2.2.1. Insider Threat 5
3. Deliverables **6**
4. Schedule and Staffing **6**
5. Service Fees **7**
6. Technology/Equipment Fees **7**
7. Expenses **7**
8. Invoices and Payment **7**
9. Assumptions **8**
10. Requirements **8**
11. Contact Information **8**
12. Handling of Findings **9**
13. Change Requests **9**
14. Signatures **10**
15. References **11**

This Statement of Work ("SOW") is made and entered into as of the later of the signature dates below ("SOW Effective Date"), by and between Bit Dancing Studios ("BDS" aka Amy Devine) and YouBreakWeFix ("Customer"). This SOW is governed by the Master Services Agreement (the "Agreement") dated May 14, 2021, between Customer and Bit Dancing Studios.

1. Background

Health Insurance Portability and Accountability Act (HIPAA) is a federal law for the protection of Electronic Protected Health Information (EPHI) or simply "medical records". There are 4 main rules for HIPAA[1]: Privacy, Security, Breach Notification, and HIPAA Omnibus Rule. (The latter 2 rules deal with notification of data breaches and violations of HIPAA rules, respectively. They will not be covered under the scope of this agreement.) The Privacy Rule and the Security Rule provide physical, administrative and technical controls around the protection of EPHI ensuring confidentiality, integrity and availability of medical records. Violation of HIPAA rules may result in a fine of up to $50,000 per violation.

2. Scope

2.1. In Scope

The Customer seeks the services of Bit Dancing Studios to conduct an internal assessment of the Customer's ability to protect ePHI as set forth by HIPAA. BDS will assess the Customer's network security to:

- Prevent retrieval of confidential ePHI without authorization
- Prevent modification of ePHI without authorization

BDS will also assess the Customer's physical security to:

- Prevent unauthorized access to PHI

BDS will assess the Customer's administrative security to:

- Prevent breaches of ePHI
- Detect breaches of ePHI
- Contain breaches of ePHI
- Correct breaches of ePHI

In order to achieve the objectives of this professional services agreement, BDS will conduct in-person interviews with the Customer's staff (technical, administrative, end users) as well as active network testing (aka pentesting) of the production network

[1] https://www.datalinknetworks.net/dln_blog/what-are-the-most-important-hipaa-compliance-requirements

environment, limiting to resources required for HIPAA compliance and within the local network. (See Out of Scope)

BDS will test and probe for security vulnerabilities and exploit vulnerabilities on all discoverable devices and hosts within the internal network of the Customer. The Customer has asked for network resources and system administrative controls be limited to those needed for HIPAA compliance and specified a preference for work to be done after hours.

An initial network survey will be performed during working hours and after hours on the least busy day. This will allow BDS to look for any differences in network resources or configurations that could affect the validity of the overall security assessment. If there are differences, BDS will review these initial findings with the Customer to determine the right course of action.

All relevant discovered devices and hosts within the Customers network and system administrative control will be subject to testing after hours until complete.

BDS will conduct the assessment based on the objectives above and provide a written report detailing any findings. The report will also contain recommendations the Customer can take to improve any findings from the assessment. BDS will also provide an in-person read out of the assessment to the Customer's stakeholders.

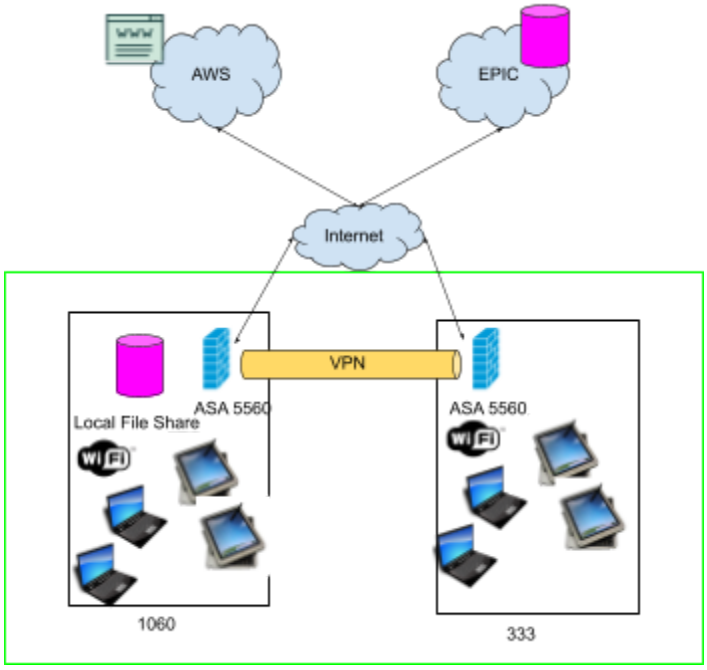

Figure 1: Network Architecture for the Customer

Figure 1 shows the network architecture for the client. The resources in green indicate what is in scope for this professional services agreement. Anything outside the green box is considered out of scope.

2.1.1. Physical Testing

As shown in Figure 1, the Customer has 2 physical locations:

- 1060 W Addison (1060)
- 333 W 35th street (333)

BDS will attempt to access each of the locations with the intent of gaining unauthorized access to the Customer's network, and subsequently ePHI. Specifically, BDS will attempt to gain persistent access to your network and retrieve documents without authorization.

2.1.2. Network Breach Testing

Each location has an ASA 5560 firewall. Location 1060 also hosts the local store for the ePHI. There is a site-to-site VPN used to connect the two locations.

For this assessment, the initial entry point for testing will be the Internet. If external breach is not achieved, it will be assumed and BDS will proceed to internal attacks.

2.1.3. Wireless Testing

The Customer is operating their own wireless network at each location. Meraki Access Points are used. Nurse tablets are connected to the wireless network. BDS will perform wireless pentesting to gain access to the internal network at each location.

2.1.4. People Testing

BDS will utilize social engineering techniques (such as phishing and phone calls) to attempt to gain access to PHI of patients at both locations. In addition, BDS will leave behind devices designed to gain access to network resources.

2.2. Out of Scope

Externally hosted resources and third party vendors are out of scope for the purpose of this engagement. Specifically, the Customer is utilizing external vendors for hosting their website (through AWS) and for health record storage (EPIQ). HIPAA does not yet currently provide compliance requirements for Cloud Service Providers (CSP).

> "AWS aligns our HIPAA risk management program with FedRAMP and NIST 800-53, which are higher security standards that map to the HIPAA Security Rule. NIST supports this alignment and has issued SP 800-66 An Introductory Resource Guide for Implementing the HIPAA Security Rule, which documents how NIST 800-53 aligns to the HIPAA Security Rule."[2]

Services relating to the ability to make appointments and pay medical bills is outside the scope of this engagement.

2.2.1. Insider Threat

This professional services agreement does not include evaluation or remediation for Insider Threat scenarios. An Insider Threat is where a person with valid credentials performs an activity within their authorized role but for malicious purposes. For example, an employee with credentials to the ASA 5506 firewall logs in and changes the configuration to allow all traffic from the Internet. Our

[2] https://aws.amazon.com/compliance/hipaa-compliance/

pentest would identify a misconfiguration with the firewall but would not identify any malicious intent of an individual.

3. Deliverables

In addition to the following billable milestones, BDS will provide a monthly status report to the Customer.

Milestone	Date	Invoice
Kickoff	1 month After Receipt of Order (ARO)	$36,000
Initial Network Survey	1.5 months ARO	$9,000
Physical Testing	3 months ARO	$36,000
Network Breach Testing	4 months ARO	$36,000
Wireless Testing	5 months ARO	$36,000
People Testing	6 months ARO	$36,000
Written report provided	7 months ARO	$18,000
Read-out meeting	7.5 month ARO	$18,000
Assessment Closeout	8 months ARO	$50,000
Total Cost		$275,000

4. Schedule and Staffing

If the professional services agreement is signed by 2023-OCT-30, work will begin on 2023-NOV-1 and conclude by 2023-NOV-30.

The Customer's work hours are weekdays from 8am – 6pm CT. Network and Wireless testing will be conducted after hours starting at 6:30pm CT and completing at 7:30am CT. People testing will be conducted during business hours. Physical testing may be conducted anytime during the testing agreement (24/7).

During the Internal Assessment phase, the Customer will support BDS testing. Specifically, Customer resources (people, services) will be provided to help assess the detection,

containment and correction of breaches to ePHI. The scope of this effort will include in-person interviews about the controls in place to detect, contain and correct breaches, followed by security assessment testing (“pentest”).

5. Service Fees

Bit Dancing Studios has an labor rate of $225/hour.

6. Technology/Equipment Fees

BDS does not anticipate needing specialized equipment to support this assessment. Wherever possible BDS will

- Use commercially available software, freeware, shareware, and custom scripts to conduct network reconnaissance, vulnerability analysis, and limited exploits of areas deemed most vulnerable.

7. Expenses

The Customer will reimburse Bit Dancing Studios for reasonable travel and lodging during the engagement.

8. Invoices and Payment

BDS will submit invoices and electronic monthly status reports to the Customer. The Customer will review invoices submitted by BDS and approve the invoice for payment within 10 business days.

9. Assumptions

9.1. AWS infrastructure meets the NIST requirements for HIPAA.

9.2. There is no difference between network resources and configuration between working hours and “after hours”.

9.3. Customer will provide physical access to the 2 locations:

9.3.1. 1060 W Addison

9.3.2. 333 W 35th street

9.4. If needed, the Customer will provide credentials, physical badges and keys to BDS.

9.5. BDS will furnish all equipment, hardware and software, for the completion of this SOW unless otherwise stated in Technology/Equipment Fees.

9.6. The Customer’s third party vendors are responsible for their own HIPAA compliance. BDS will not attempt to assess any 3rd party vendor.

9.7. Customer operates two different subnets: 10.10.10.0/24 and 10.10.20.0/24

9.8. The Customer owns 198.51.100.0/29 for external IP addresses.

9.9. The Customer runs bitlocker on the network resources.

9.10. The Customer runs Windows Defender on the network resources.

9.11. The Customer is operating their own wireless network, leveraging Meraki Access Points.

10. Requirements

10.1. The Customer will not use any special access restrictions against BDS that do not apply to the Customer’s general network as a matter of business.

10.2. In the event that the Customer identifies and blocks access to any BDS resource scanning the network, the Customer will add the IP address for the BDS resource to the approved access control list (aka whitelist).

11. Contact Information

In the event the Customer’s services are affected by any of the assessments, BDS will contact the Customer’s emergency contact immediately.

11.1. Emergency Contact: Ryan Haley - rhaley@depaulseclabs.com

12. Handling of Findings

In the event that PHI is obtained during testing, BDS will stop testing and notify the Customer immediately that ePHI was obtained, how it was obtained and how much was obtained. BDS will not retain any ePHI and is not responsible for removing ePHI from the Customer's resources during the test. Any ePHI obtained through unauthorized means will be considered a finding.

At the end of the engagement, BDS will secure wipe any and all ePHI collected.

13. Change Requests

BDS will keep the Customer informed of actions on a monthly basis through reports as well as through daily updates during the Initial Assessment period. During this engagement, if there is a desire from either party to increase the scope of the initial professional services agreement, a conversation will be had with the potential for the contract scope and cost to change. This will be handled on a case-by-case basis.

14. Signatures

YouBreakWeFix	Bit Dancing Studios
_____	_____
Signature	Signature
_____	_____
Name	Name
_____	_____
Title	Title
_____	_____
Date	Date

15. References

1. HIPAA Compliance - https://www.atlantic.net/hipaa-compliant-hosting/hipaa-compliance-guide-what-is-hipaa/
2. SOW Template - https://www.alaskapublic.org/wp-content/uploads/2021/06/Statement-of-work-%E2%80%94-Mandiant.pdf
3. Mandiant SOW Template - https://www.alaskapublic.org/wp-content/uploads/2021/06/Statement-of-work-%E2%80%94-Mandiant.pdf
4. Coalfire SOW Template - https://www.iowacourts.gov/static/media/cms/Service_Order__Redacted_581A59C144331.pdf
5. HIPAA Compliance and the Rules - https://www.datalinknetworks.net/dln_blog/what-are-the-most-important-hipaa-compliance-requirements
6. https://aspe.hhs.gov/standards-privacy-individually-identifiable-health-information#:~:text=The%20Privacy%20Rule%20establishes%20a%20federal%20requirement%20that%20most%20doctors,health%20care%20operations%20(TPO).
7. Information on the Security Rule - https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf
8. AWS HIPPA Compliance - https://aws.amazon.com/compliance/hipaa-compliance/
9. Running Epic on AWS - https://aws.amazon.com/health/solutions/epic/