omada

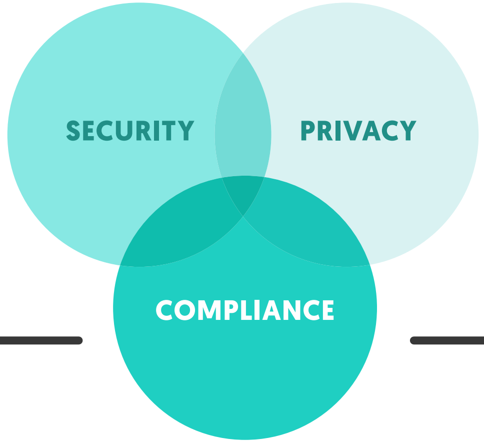
INCLUDES NO DIRT

A Practical Approach to Threat Modeling for Digital Healthcare and Beyond

AUTHORS

William Dougherty, MSIT, CISSP, CISM, CCSP
VP IT & Security

Patrick Curry, PhD, CIPP/US
Director of Compliance



Introduction

Risk analysis and threat modeling are critical procedures for all organizations, but these procedures are especially important to healthcare companies. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires all covered entities and business associates to assess their risks and vulnerabilities, and take steps to reduce their risks. NIST special publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations recommends a risk management life cycle that includes assessment of security controls. Risk assessments are also a requirement of the HITRUST CSF, category 3.0.

The problem for practitioners in digital healthcare, like for most other healthcare organizations, is the limited resources describing how to consistently and scalably evaluate risks. - Concepts may be clear, but real world methodologies are lacking - a dangerous proposition for an increasingly large percentage of the healthcare sector.. The objective of this paper is to provide an actionable guide for security, privacy and compliance practitioners in digital healthcare. However, we believe the processes described in this guide can extend to nearly any organization that takes security and privacy seriously. The framework we have developed is built on the foundation of decades of work done by other recognized bodies. Our threat model builds chiefly on two major frameworks that have effectively guided practices even as industries have rapidly evolved

Stride - A computer security framework developed by Loren Kohnfelder and Praerit Garg while at Microsoft.

Linddun - A privacy framework developed by the DistriNet Research Group.

45 CFR § 164.308 (a) (1) (ii) A covered entity or business associate must, in accordance with § 164.306: (A) Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity. (B) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). (C) Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. (D) Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

We supplemented these two resources with others. When brainstorming potential risks, the MITRE Common Attack Pattern and Classification (CAPEC) catalog is an excellent, although sometimes overwhelming resource. Additionally, for privacy related risks, Solove's taxonomy of privacy is invaluable in evaluating the risk of harm:. The Solove Taxonomy identified four categories that may infringe on privacy: activities, collection, dissemination, and invasion. Each of these activities also directly relate to security risks.

NIST has produced several special publications on risk assessment and risk management. NIST's SP 800-30 Guide for Conducting Risk Assessments provides a good theoretical overview of risk management, including threat analysis.

Lastly, The United States Department of Health and Human Services (HHS) has published several guides for health care organization to assess their risks:

Related to HIPAA: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

OCR 2016 Desk Audit protocol, element S2, Risk Analysis: https://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

Healthcare in general - Compliance Program Guidance documents, HHS Office of Inspector General: https://oig.hhs.gov/compliance/compliance-guidance/index.asp

Our model borrows from, and builds upon all of these sources, as well as others.

So why is yet another threat model required? The short answer is we needed a consolidated approach that we could apply universally, and which is easy for our staff to understand and remember. STRIDE is a model for secure software. LINDDUN is a model for privacy design. But neither model brings is holistic enough for companies operating in the evolving world of digital healthcare.

Within healthcare, firms need to incorporate techniques from both, while layering in additional compliance and regulatory concerns. To the untrained eye, privacy and security are often viewed in conflict, but in a well-run program, these conflicts are resolved through collaboration and judgement. Healthcare requires a single model that addresses security, privacy, and compliance in a way forces teams to identify and resolve apparent conflicts across all three categories. While both STRIDE and LINDDUN were developed primarily in the realm of software development, digital healthcare requires an approach that can be applied to software development, vendor selection and analysis, and business processes. Although Omada Health is currently focused more on digital content than many healthcare companies this content is applicable across the broader industry.

> **Concepts may be clear, but real world methodologies are lacking - a dangerous proposition for an increasingly large percentage of the healthcare sector.**

There are several different methods for performing a threat model. Typically, these methods start with a team of smart people and a white board, discussing all possible negative outcomes, then using a model like STRIDE to guide the development of processes. Threat models may be asset-centric, attacker-centric or software-centric, depending on how the team conceptualizes risks. In an asset-centric model, the team considers an asset, such as a building, and then discusses all the ways it could be harmed. In a software-centric model, the team considers an application or a feature and analyzes the data flows and trust boundaries to identify how they could be abused or misused.

For the INCLUDES NO DIRT model ("NO DIRT"), we needed two layers of abstraction in order to scale the threat modeling process. First, we abstracted the model to be system-centric. A system can be a software feature, a vendor, a business process, an asset, or anything else that required analysis. Second, we abstracted the analysis to be primarily controls focused rather than brainstorming focused. This approach may seem counterintuitive at first, but it allows for rapid modeling and triage, enabling our team to focus deeper analysis on the biggest risks. As an example, Omada Health already has a pattern for strong authentication in our systems to prevent spoofing and enhance non-repudiation. Rather than brainstorming all the ways authentication could break, we simply asked if the system uses our standard authentication pattern. If it does, we can feel comfortable in its security controls, and move on to other issues. If it does not, it we raise the calculated risk score which informs the team that this is an area for further attention. After analysis, the team may create an action item to change the authentication method and then reassess.

Obviously, this approach does not eliminate the need for brainstorming, data flow diagrams, or other analysis. The very first requirement in the NO DIRT threat model process is for the modeler to provide a system description, including appropriate diagrams. The complexity of the diagrams will depend on the system being modeled and the analytic needs of the team. For a new feature being developed, descriptions and diagrams can become quite complex. For a new vendor of a non-critical system, they may be as simple as a short paragraph and a link to the vendor's website. The amount of effort invested in system diagramming and brainstorming is at the discretion of the threat modeling team. Our paper includes a sample brainstorming worksheet below that can be used for complex analysis.

The NO DIRT Model has eight governing principles:.

1. The model has to be easy for a non-security, non-privacy, or non-compliance person to understand and interpret. That means explaining terms, and reasoning, in plain language. In most digital health organizations, security, privacy and compliance teams are dwarfed in size by the teams responsible for writing new software and acquiring new vendors. NO DIRT is designed as a model that empowers any employee to self-assess a potential risk, thus acting as a force multiplier.
2. The model must be easy to perform, especially for non-critical systems. Our company works with hundreds of vendors and dozens of internal applications. Many of them are not mission critical. But threat assessments should be performed on all of them. To make that feasible, the model should be able to be completed on a non-critical system in less than 15 minutes, by a single person.
3. For critical systems, the model had to be powerful enough and flexible enough to capture all reasonable concerns.
4. The model must be repeatable. We turned NO DIRT into a standard set of questions in our governance, risk and compliance (GRC) system. Using a consistent set of questions speeds the process, and storing those questions in our GRC system provides documented evidence of a team's thought process at the time a decision is made. When facts or assumptions change, we can repeat the process to produce a new model.
5. When operationalizing the model in our GRC system, it had to have a weighted scoring system that would automatically classify the risk of the system based on the answers. This allows security, privacy and compliance teams to review self-assessments and quickly triage which systems, projects or vendors need extra attention.
6. The model has to be useful in the architecture and design stage to guide decisions, and as an analytical tool for existing systems.
7. The model had to tie directly to our vendor assessment process. We tweaked and simplified our vendor questionnaires to only ask questions critical to the model.
8. The model had to be memorable, hence the catchy acronym. This may seem trivial, but the name sets the stage for organizational desire to be "dirt free."

> “
> **INCLUDES NO DIRT model needed two layers of abstraction in order to scale the threat modeling process...This approach may seem counterintuitive at first, but it allows for rapid modeling and triage, enabling our team to focus deeper analysis on the biggest risks.**
> ”

Taxonomy

Lastly, before we dive into the model, it is helpful to review a taxonomy. In the world of threat modeling and risk analysis, the words threat and risk are often used interchangeably (our own team is not immune).

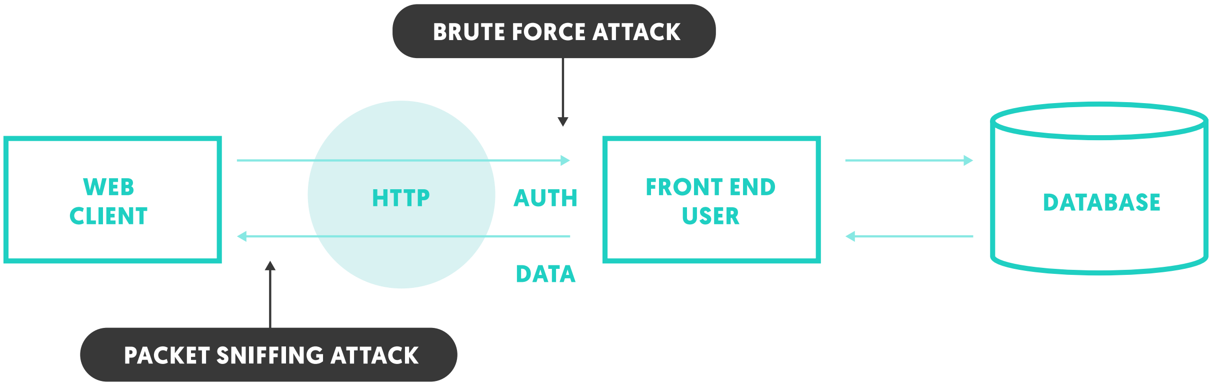
Arguing over the distinctions is largely a semantic discussion. For the purposes of this model, we will utilize the following definitions:

System	The thing being modeled. This can be an application, business process, network, a vendor service, etc. The defining characteristic of a "system" is that the organization desires its protection from threats.
Trust Boundary	The places in a system where principles interact. Some models also refer to attack surfaces, which are a type of trust boundary where a threat actor can interact, but trust boundaries can exist in a system beyond the attack surface.
Vulnerability	A weakness in a system. Vulnerabilities are things that can be exploited.
Threat	An actor or principle. A threat can be an employee, a malicious third party, a business process, a natural occurrence, or a piece of code.
Attack Vector	The method by which a threat exploits a vulnerability.
Risk	A resulting bad outcome when a threat exploits a vulnerability in a system.
Probability	The likelihood of a risk occurring.
Impact	The cost of a risk occurring.
Control	A feature or mitigation in a system that reduces the probability or impact of a risk.
Threat Modeling	An analysis of a system's vulnerabilities, controls, and threats against a defined list of risks.
Action Items	Tasks to be performed by the system owner or risk assessor as a result of the threat model.

An example will help to illustrate. Let's consider a hypothetical patient record application with a web interface. The application communicates over http and has a weak password management system. We are worried about a malicious third party (such as a hacker) stealing credentials and gaining access to PHI.

Traditional Threat Model

PATIENT RECORD APPLICATION (EXAMPLE)



SYSTEM	Patient Record Application
TRUST BOUNDARY	Login Prompt
THREAT	Hacker
VULNERABILITIES	Weak Password Management, Unencrypted http
ATTACK VECTORS	Brute Force, Packet Sniffing
RISKS	Account Take-over, PHI Breach

PROBABILITY	High
IMPACT	High
CONTROLS	Password Policy, Encryption, Logging, Monitoring
ACTION ITEMS	Enforce TLS encryption, Implement two-factor authentication

In a traditional threat model process, teams would brainstorm and produce multiple threat scenarios such as the above, for the application being modeled. This approach can be powerful, but also time consuming. By focusing first on the features and controls of the system, and using a consistent process, we are able to condense the process for lower risk, lower priority systems and focus efforts where they are needed most.

Includes No Dirt - Summary Model

The acronym INCLUDES NO DIRT is intended to help risk assessors identify the areas of potential weaknesses in the systems they are evaluating. In each case, the risk has a corresponding property or goal that represents the desired intent of the system being evaluated. As an example, most websites have Availability as a goal. The risk to Availability is Denial of Service. Some of the goals, such as Anonymity vs. Non-Repudiation, are mutually exclusive. This is by design. When evaluating systems in healthcare (and other industries), there are cases where privacy and security are in conflict. The dominant property depends on the thing being assessed.

	RISK	PROPERTY/GOAL	REALM
I	IDENTIFIABILITY	Anonymity	Privacy
N	NON-REPUDIATION	Plausible Deniability	Privacy
C	CLINICAL ERROR	Correct Application of Clinical Standards	Compliance
L	LINKABILITY	Unlinkability	Privacy
U	UNLICENSED ACTIVITY	Proper Credentials or Licensure	Compliance
D	DENIAL OF SERVICE	Availability	Security
E	ELEVATION OF PRIVILEGE	Authorization	Security
S	SPOOFING	Authentication	Security
N	NON-COMPLIANT TO POLICY OR OBLIGATIONS	Policy or Contractual Adherence	Compliance
O	OVERUSE	Minimum Necessary	Compliance
D	DATA ERROR	Integrity	Security
I	INFORMATION DISCLOSURE	Confidentiality	Security
R	REPUDIATION	Non-Repudiation	Security
T	TAMPERING	Integrity	Security

IDENTIFIABILITY

Identifiability is the property of a system that lets activities be traced to a specific user. Some systems, such as an application for reporting fraud or abuse, may require an option to act anonymously. If anonymity is required, then the risk assessor must identify what controls are in place to ensure it.

NON-REPUDIATION

Non-Repudiation is the process by which it can be proven that a user performed an action. Like anonymity, some systems require may require plausible deniability. The difference between anonymity and plausible deniability is subtle but important. An application that allows for anonymity may still record IP addresses, machine IDs or other metadata that can be traced back to the user. For some systems, such as a Whistleblower application, it may be required to ensure plausible deniability. In those cases, it's important to analyze not only the user features but also the metadata being recorded.

CLINICAL ERROR

In healthcare, and especially within digital health, accuracy in management and transformation of data is critical. This is especially true for data that concerns the health status, condition, or participation of an individual. Clinically relevant errors can occur if the system does not enforce agreed-upon clinical standards, or does not preserve information fidelity.

LINKABILITY

Linkability is the ability to relate two or more pieces of information. Linkability can be a risk to both anonymity and plausible deniability. In healthcare, linkability most often comes up in the context of de-identification of protected health information (PHI). HHS has identified 18 potential identifiers that must be removed from a dataset to de-identify it according to the "Safe Harbor" method 45 CFR § 164.514 (b) (2):

1. Name
2. Address (including geographic subdivisions smaller than state)
3. Dates related to an individual (birthdate, treatment date, age)
4. Telephone number
5. Fax number
6. Email Address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate or License number (including drivers license number)
12. Vehicle identifiers including license plate numbers
13. Device serial number
14. Web URL
15. IP address
16. Biometric identifiers including finger or voice print
17. Photographic image
18. Any other characteristic that could identify the individual

UNLICENSED ACTIVITY

Many activities in healthcare require specific licensure or certification to be legally performed, either at the entity or the person level. Failing to track licenses can create a significant legal risk for a company when those rules apply. In digital health, where care is often provided nationwide, a company may need to track compliance with multi-faceted licensing requirements across different jurisdictions. For example, there may be a need to track licenses of professionals, or credentials required by customers.

DENIAL OF SERVICE

Denial of Service is any activity that impacts the Availability of a system. Availability means that the system is able to perform its tasks when required by the business.

ELEVATION OF PRIVILEGE

Elevation of Privilege occurs when a user is able to perform a function that exceeds his or her authorization. A system may apply authorizations directly to a user or to a group (role) of which the user is a member. In healthcare, a weak authorization scheme can threaten the security of the system, its compliance with the minimum necessary standard, and potentially incorrect or inappropriate provision of services. For example, a billing clerk for a lab who is supposed to only see payments due may inappropriately have access to lab test results.

SPOOFING

Spoofing is the ability for a user to pretend to be someone else. It is a risk for systems that have weak or non-existent authentication mechanisms. The required strength of an authentication mechanism depends on the system being protected and the types of data it houses. A system that stores or processes protected health information (PHI) may have different requirements than a company Intranet.

45 CFR § 164.312 of the HIPAA Security Rule establishes technical safeguards including authentication that must be implemented to protect PHI. The NIST 800-63b Digital Identity Guidelines is a good reference to authentication methods and levels.

NON-COMPLIANT TO POLICY OR OBLIGATIONS

All organizations have a wide variety of rules, regulations, internal policies, and contractual obligations to which they must adhere. As a threat assessor, it is important to identify the specific policies and obligations that apply to the system being modeled, and then review how those obligations are enforced, monitored, and audited. HIPAA requires Covered Entities and their business associates to have written policies and procedures for handling PHI, and the absence of such written policies is a threat in its own right, on top of the threats posed by lack of consistent process.

OVERUSE

Overuse is a risk prominent in healthcare, although other industries may have similar obligations. 45 CFR § 164.502 of the HIPAA Privacy Rule restricts covered entities and business associates from the use or disclosure of protected health information (PHI) to the minimum necessary to accomplish its intended purpose except for use or sharing in the case of treatment by a physician or other healthcare professional. If a system stores, processes or accesses PHI and does not have mechanisms in place to limit the use of the data to the minimum necessary when that limit is required, there may be a risk of overuse. Additionally, in cases where people provide specific consent for the use of their information regardless of regulation, it is important to understand if the risk of use outside of consent exists.

DATA ERROR

Data error is any risk to the integrity of data in the system, due to weak controls, user error, software bugs or faulty logic. Data error is generally unintentional or accidental, as opposed to intentional tampering. Systems must be evaluated on their controls to verify data integrity and correct any error identified. Consideration in testing should be paid to data transformation and the movement of data between systems.

INFORMATION DISCLOSURE

Information disclosure is any unauthorized, non-permitted, or unintended publication, leak, or loss of data that threatens the confidentiality of data held by the organization. In addition to authentication and authorization controls, systems must have strong encryption, data locality, and physical security to protect confidentiality. 45 CFR § 164.312 of the HIPAA Security Rule establishes technical safeguards including data encryption at rest and in transit that may be used to protect the confidentiality of PHI.

REPUDIATION

Most systems require non-repudiation, or the ability to prove a specific user performed a specific action. Note that this is the mirror risk to a system that requires anonymity. Authentication, authorization, system logging, accurate timestamps and digital signatures can all be used to assure non-repudiation. When assessing non-repudiation controls, the assessor should also look at how long logs or other evidence are retained to make sure they match policy and obligations.

TAMPERING

Tampering is the intentional modification of the system or its data with an intent to do harm. In healthcare, tampering can impact confidentiality, integrity, availability, and clinical accuracy. Anti-tampering controls may include network security, physical security, chain of custody, change management, code review, and vulnerability assessments. The HHS Office of Civil Rights (OCR) has stated that tampering which renders PHI unavailable, such as by ransomware, is a reportable Breach. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf, Q/A 6.

MISCELLANEOUS

Not all risks fit neatly into a generic threat model. Some risks are specific to system or process being modeled. It is the responsibility of the risk assessor to consider all possible risks and threats and then determine if there are any material and relevant threats to the system that must be evaluated and mitigated. Miscellaneous threats may include:

1. Physical Risks
2. Environmental Risks
3. Criminal Risks
4. Disaster Risks
5. Regulatory Risks
6. Vendor Risks
7. Competitive Risks
8. Other

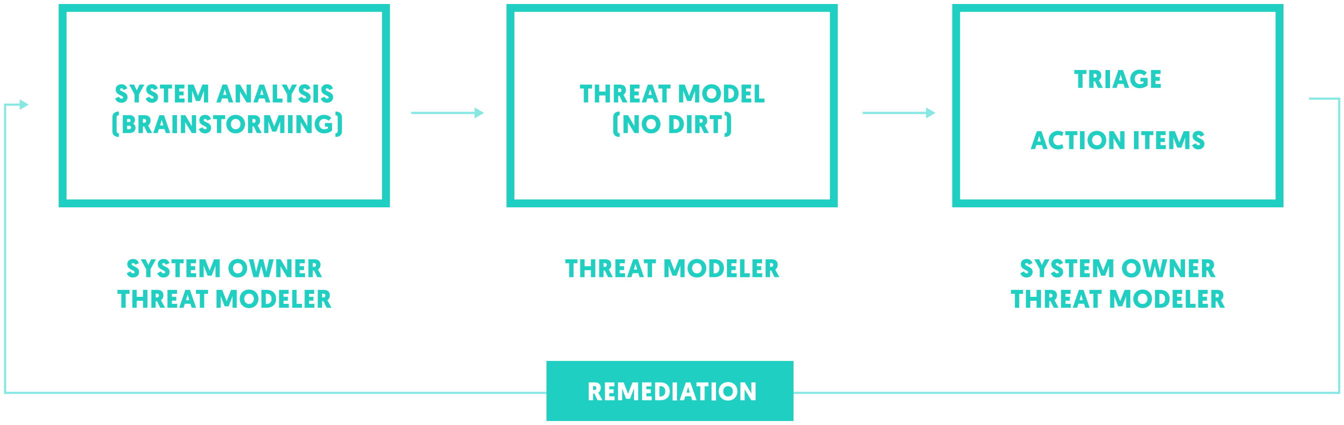
Putting NO DIRT Into Action

Regardless of the threat model used by an organization, it is only valuable when actually in use. Key considerations for any organization include WHEN to do threat models, WHO performs them, and HOW they are performed. Threat models can (and should) be triggered by significant changes to the organization, such as new projects or vendors. They should also be a part of annual risk assessments. Finally, they are a useful tool to evaluate existing processes and systems on-demand. While anyone can perform threat models, they are primarily the responsibility of the System Owner(s) and the Threat Modeler(s). The System Owner may be the project manager of a large project, the product manager or engineer of a new product, the business owner requesting a new vendor, or whomever else is responsible for the thing being modeled. Threat Modelers are usually members of the security and compliance teams but can include members of other Risk Assessing Organizations as makes sense for the company, and the problem at hand.

At the organizational level, the executive team is responsible for ensuring that enterprise threats to company are addressed appropriately. The NO DIRT model has the added benefit of creating a system executives can use to evaluate the totality of threats across an organization's business. Examples of WHEN, WHO, and HOW to perform threat models are outlined in the table below:

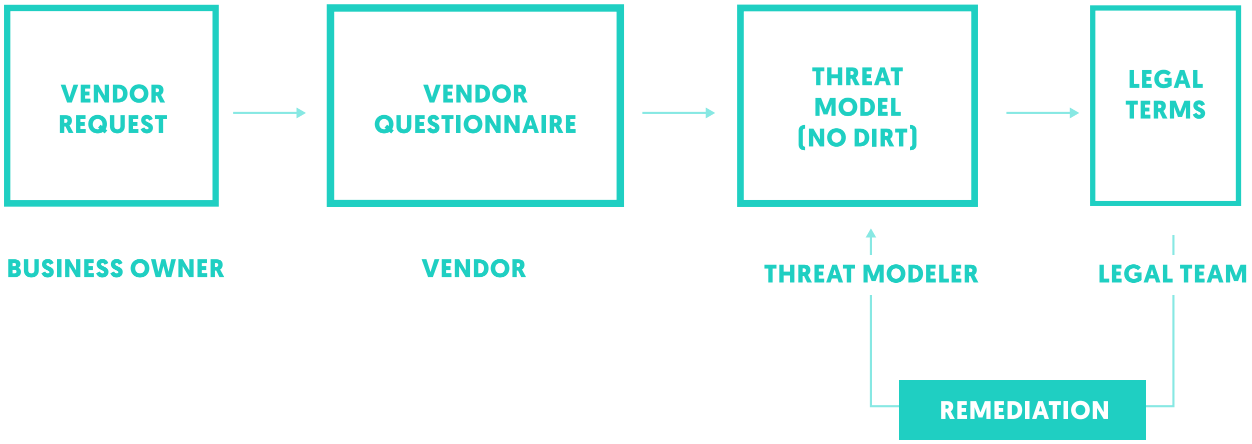
WHEN	WHO	HOW
Initiation of a significant project	System Owner Threat Modeler	Brainstorm System Diagrams Data Flow Diagrams Data Classification NO DIRT Questionnaire
Vendor Acquisition	System Owner Threat Modeler	Vendor Questionnaire NO DIRT Questionnaire Contractual Review
Annual Risk Assessment	Risk Assessment Team Threat Modeler	Review of Previous Assessment Brainstorm NO DIRT Questionnaires
Annual Vendor Assessment	System Owner Threat Modeler	Vendor Questionnaire NO DIRT Questionnaire Contractual Review
On-Demand	Requestor Threat Modeler	Depends on request NO DIRT Questionnaire

What goes into the threat model depends on the system being modeled, as well as the needs of the team. The foundation of the NO DIRT model is a repeatable questionnaire that focuses the team on top risks, and allows for rapid assessment and triage. Complex systems may generate multiple threat models, with many action items and remediation steps. Threat modeling should be thought of as an iterative process, rather than an event. OCR requires that covered entities assess their risk annually , and this model enables that annual review, with the added benefit of enabling risk assessment over time through iteration.



VENDOR QUESTIONNAIRES

Vendors represent a specific type of system that may add significant risk and complexity to an organization. When an organization acquires or initiates work with a new vendor with access to critical systems or data, the trust boundaries of the system become more important. Part of the vendor acquisition process is an assessment of the vendor's controls, including the services or products being offered. This is typically accomplished with a vendor security questionnaire. Many organizations fail to go beyond the questionnaire to a threat model that takes into account the true risks to the company, based on the service being acquired. The NO DIRT model streamlines the vendor questionnaire/assessment process. Our goal is to only ask questions critically relevant to threat modeling, instead of generic forms ranging from hundreds to thousands of questions. Once we identify critical components, we can map those to specific risks we want to assess.



The general process within NO DIRT is simple: a business owner submits a request for a new vendor relationship. The security team sends the vendor a questionnaire that maps to key portions of the threat model. When the questionnaire is completed, the security team completes a threat model and either approves or rejects the vendor. Vendor approval may be conditioned on remediation or contract terms. For reference, we have included our vendor questionnaire in the appendix.

Scoring Risks

A key feature of the NO DIRT threat model is the ability to objectively score risks based upon the threat assessment. This is accomplished by establishing a weighted scoring for specific questions that represent a higher risk. In the sample questionnaire, we apply scores to each answer, then total the scores for the model. It is important to note that not all questions have scores associated. The model generally asks a yes/no question, and then a descriptive question. An illustrative example: "Does the tool/process/service/system have mechanisms to authenticate users or processes? yes/no" and "Describe the authentication mechanisms." The yes/no question is scored, and the descriptive question captures relevant detail for further review.

The maximum score possible in our sample is 70. We establish a range for the scores to let us triage where to spend our time. A score of less than 21 gets ranked a LOW risk. A score of 21 - 40 gets ranked a MEDIUM risk. A score greater than 40 gets ranked a HIGH risk. It is easy for a user of this model to modify the scoring to meet their specific needs and risk tolerance, by adjusting the scores on each question, the definitions for low, medium and high, or both.

Conclusion

Our goal in creating the NO DIRT model was to take a process of evaluation that can be subjective, inconsistent, and/or under-documented and apply standards of practice to better ensure consistency, accuracy, and documentation that can be referenced later for a number of use cases. As we've used the model, we've noticed that the rigor of process can uncover unstated assumptions that various teams performing the evaluation have, but which conflict when gathered together. This forcing function alone has provided additional risk detection and the opportunity for mitigation. We hope the users of the NO DIRT Model will find it provides clarity, even in traditionally "muddy" situations.

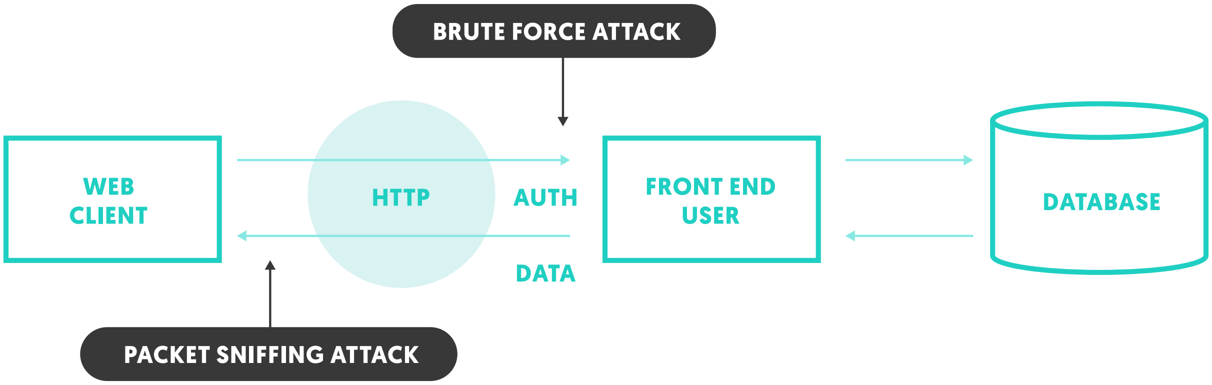
Appendix A

EXAMPLE NO DIRT THREAT MODEL IN ACTION

In the paper, we provided an example of a traditional threat model. For comparison, we've modeled the same application using the NO DIRT model. Additionally, in Appendix B, we provide blank worksheets for modification and use.

Appendix A1

TRADITIONAL THREAT MODEL [FOR COMPARISON]



SYSTEM	Patient Record Application
TRUST BOUNDARY	Login Prompt
THREAT	Hacker
VULNERABILITIES	Weak Password Management, Unencrypted http
ATTACK VECTORS	Brute Force, Packet Sniffing
RISKS	Account Take-over, PHI Breach

PROBABILITY	High
IMPACT	High
CONTROLS	Password Policy, Encryption, Logging, Monitoring
ACTION ITEMS	Enforce TLS encryption, Implement two-factor authentication

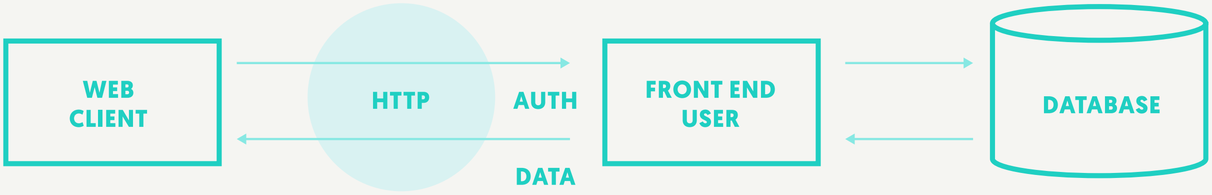
Appendix A2

INCLUDES NO DIRT - SAMPLE ASSESSMENT QUESTIONNAIRE

System Description - Describe the tool/process/service/system being analyzed in this questionnaire. If it involves a third party vendor, provide vendor information, URLs, and other information pertinent to your analysis. Attach any pertinent documentation or diagrams, including the results of any brainstorming sessions:

The Patient Record Application is a web-based tool to allow patients to access their health records. It consists of a web front-end application and a back-end datastore of their data.

PATIENT RECORD APPLICATION (EXAMPLE)



1.0 **Identifiability** - Does the tool/process/service/system require anonymity for compliance?
[ ] Required (1 point)
[x] Not Required (go to question 2.0)

1.1 Does the tool/process/service/system have strong controls to ensure anonymity?
[ ] Yes
[ ] No (2 points)

1.2 **Anonymity Controls** - Describe how anonymity is enforced:

2.0 **Non-Repudiation** - Does the tool/process/service/system require plausible deniability for compliance?
[ ] Yes (1 point)
[x] No (go to question 3.0)

2.1 Does the tool/process/service/system have controls to ensure plausible deniability?
[ ] Yes
[ ] No (2 points)

2.2 Describe how plausible deniability is enforced:

3.0 **Clinical Error** - Does the tool/process/service/system involve or impact clinical activities?
[x] Yes(1 point)
[ ] No (go to question 4.0)

3.1 Does the tool/process/service/system correctly enforce clinical standards and prevent the introduction of clinical error?
[ ] Yes
[x] No (2 points)

3.2 Explain how clinical errors are prevented:

Clinical advice is a part of the patient record. Clinical standards and error prevention are provided in other related systems.

3.3 Clinical Monitoring - Describe any monitoring of clinical activity contained in the tool/process/service/system that would identify clinical errors:

4.0 **Linkability** - Does the tool/process/service/system require unlinkability or de-identification?
[ ] Yes(1 point)
[x] No (go to question 5.0)

4.1 Does the tool/process/service/system enforce unlinkability or de-identification?
[ ] Yes
[ ] No (2 points)

4.2 Explain how unlinkability is enforced:

5.0 **Unlicensed Activity** - Does the tool/process/service/system require a specific license (Federal, State, other) to be used/performed? Consider in your response both the person providing or performing the service, and/or the entity (company) doing the same.
[ ] Yes(1 point)
[x] No (go to question 6.0)

5.1 Does the tool/process/service/system check the license of the user, and deny the user if unlicensed?
[ ] Yes
[ ] No (2 points)

5.2 Explain the licenses required and how license checks are enforced:

6.0 **Denial of Service** - Is the tool/process/service/system considered mission critical?
[x] Yes (2 points)
[ ] No

6.1 Does the tool/process/service/system have a defined availability target?
[x] Yes
[ ] No (1 point)

6.2 Describe the availability targets, contingency plans, and how availability is monitored.

99.9% availability. Availability is monitored via synthetic web monitoring program.

7.0 **Elevation of Privilege** - Does the tool/process/service/system have controls to enforce authorization?
[x] Yes
[ ] No (2 points)

7.1 Does the tool/process/service/system involve customer data, patient data, employee data, or other sensitive or confidential data?
[x] Yes (2 points)
[ ] No (go to quesiton 7.5)

7.2 Data Classifications - check all that apply
[X] Protected Health Information (PHI) (go to question 7.3) (2 points)
[ ] Customer Data (1 point)
[X] Patient Data (1 point)
[ ] Employee Data (1 point)
[ ] Company Sensitive Data (1 point)
[ ] Company Confidential Data (1 point)

7.3 **PHI Identifiers** - Which PHI identifiers are included in the data?
[X] Name
[X] Address (including all geographic subdivisions smaller than state)
[X] Dates related to an individual (birthdate, treatment date, etc.)
[X] Telephone number
[ ] Fax number
[X] Social Security number (2 points)
[X] Medical record number
[X] Health plan beneficiary number
[X] Account number
[ ] Certificate or License number (including drivers license number)
[ ] Vehicle or device serial number
[ ] Web url
[X] email address
[X] IP Address
[ ] Biometric identifiers including voice or fingerprint
[ ] Photographic image
[ ] Any other characteristic that could uniquely identify an individual

7.4 Describe the types of data and the authorization mechanisms

Full patient records including records of care, contact information, and billing information

7.5 **Role-Based Authorization** - Does the tool/process/service/system control authorization by defining specific user roles, and assigning users to those roles?
[x] Yes
[ ] No (1 point)

7.6 Does the tool/process/service/system define authorization using the principles of LEAST PRIVILEGE and MINIMUM NECESSARY?
[x] Yes
[ ] No (1 point)

8.0 **Spoofing** - Does the tool/process/service/system have mechanisms to authenticate users or processes?
[x] Yes
[ ] No (2 points)

8.1 Describe the authentication mechanisms:

Each patient is assigned a unique username and password. Email addresses are used as user name. Multi-factor is provided at the patient's option via SMS.

8.2 Does the tool/process/service/system conform to NIST 800-63b standards for user names, passwords, and other factors?
[X] Yes (go to question 8.3)
[ ] No (1 point)

8.3 What AAL level is required by tool/process/service/system?
[x] AAL1 (single factor)
[ ] AAL2 (multi-factor)
[ ] AAL3 (multi-factor with hardware)

8.4 Describe the reasons why authentication is not required:

9.0 **Non-Compliant to Policy or Obligations** - What policies or obligations govern the use or function of the tool/process/service/system?
[x] HIPAA (2 points)
[x] Privacy Policy (1 point)
[x] Terms of Use
[x] Security Policy
[x] Healthcare Compliance Policy (2 points)
[ ] Customer Contracts (1 point)
[ ] Employee Handbook
[ ] Vendor Contract
[ ] Omada as a Business Associate (1 point)
[ ] Vendor or Partner as a Business Associate (2 points)
[ ] Other policy or obligation
[ ] Not Applicable (go to question 10.0)

9.1 Describe how the tool/process/service/system adheres to the identified policies and obligations above:

System has been designed to conform to all policies, and is audited annually by a third party for compliance.

9.2 Does the tool/process/service/system have the ability to monitor or audit for compliance with the identified policies?
[X] Yes
[ ] No (go to question 9.4) (1 point)

9.3 Describe how policy compliance is monitored or audited:

System includes audit logs that identify misuse.

9.4 Is the tool/process/service/system in scope for any third party/independent audit or assessment?
[X] Yes
[ ] No (go to question 10.0)

9.5 Identify the third party audits that apply to the tool/process/service/system:
[x] SOC 2
[x] HITRUST
[ ] ISO 27001
[x] PCI
[ ] Financial Audit
[ ] Vendor SOC 2, HITRUST, ISO, or PCI
[ ] Customer audit or review
[ ] Other

(*** if the answer to question 7.1 was no, skip section 10**)

10.0 **Overuse** - Does the tool/process/service/system have mechanisms to enforce the use of the "minimum necessary" amount of data and to prevent overuse?
[x] Yes
[ ] No (go to question 11.0) (1 point)
[ ] Not Applicable (go to question 11.0)

10.1 Describe the mechanisms that restrict use and access to the minimum necessary amount:

System includes role-based authorization. Patients are limited to their own data. Administrator accounts are limited to key employees only, and access is audited quarterly.

11.0 **Data Error** - Does the tool/process/service/system have mechanisms to ensure data integrity?
[ ] Yes
[x] No (go to question 12.0) (2 point)
[ ] Not Applicable (go to question 12.0)

11.1 Describe the data integrity mechanisms:

System includes role-based authorization. Patients are limited to their own data. Administrator

(* **if the answer to question 7.1 was no, skip section 12**)

12.0 **Information Disclosure** - Does the tool/process/service/system have mechanisms to ensure Confidentiality?

[x] Yes
[ ] No (go to question 13.0) (2 points)

12.1 Describe the mechanisms used to ensure confidentiality:

Data is encrypted at rest via whole disk encryption

12.2 Confidentiality Mechanisms - select all that apply:

[x] Data is encrypted at rest (answer question 12.3)
[ ] Data is encrypted during transmission (answer question 12.4)
[x] Passwords are hashed with a one-way function
[x] Data is stored, processed and transmitted on a protected network
[x] Data is stored, processed and transmitted in a protected facility (answer question 12.5)

12.3 What method of encryption is used to protect data at rest?

AES 256

12.4 What method of encryption is used to protect data during transmission?

12.5 **Secure Facility** - Where is the data located?

AWS US-WEST-1

12.6 **Data Locality** - Is the data processed, stored or accessed outside the United States?

[ ] Yes (2 points)
[x] No

(* **if the answer to question 2.0 was yes, skip section 13**)

13.0 **Repudiation** - Does the tool/process/service/system require non-repudiation for security?

[x] Yes (1 point)
[ ] No (go to question 14.0)

13.1 Does the system have strong mechanisms to ensure non-repudiation?

[x] Yes
[ ] No (2 points)

13.2 Describe the controls used by the system to ensure non-repudiation:

logging

13.3 Non-repudiation Mechanisms - select all that apply:

[x] User activities are logged
[x] Log files capture IP addresses
[ ] Log files capture machine ID or profile
[x] System ensures accurate timestamps
[ ] System utilizes digital signatures
[ ] User activities are recorded and can be replayed
[ ] System requires out-of-band confirmation (email confirmation)
[ ] System requires multiple people to perform sensitive functions (separation of duties)
[ ] System retains/archives previous versions of data (version control)

13.4 How long are log files retained?
[ ] <3 months (1 points)
[ ] 3 - 6 months
[x] >6 months

14.0 **Tampering** - Does the tool/process/service/system have mechanisms to prevent tampering?
[x] Yes
[ ] No (go to question 15) (2 points)

14.1 Describe the mechanisms that exist to prevent tampering:

14.2 Anti-Tampering Mechanisms - select all that apply:
[x] Physical Security
[x] Network Security
[ ] Endpoint Security
[ ] Chain of Custody
[x] Change Management Process
[x] Third Party Vulnerability Assessments
[x] Code Review
[ ] Other

15.0 **Miscellaneous Risks** - Is the tool/process/service/system susceptible to any additional threats? Select all that apply:
[x] Physical Risks (1 points)
[ ] Environmental Risks (1 points)
[ ] Criminal Risks (1 points)
[ ] Disaster Risks (1 points)
[ ] Regulatory Risks (1 points)
[ ] Vendor Risks (1 points)
[ ] Competitive Risks (1 points)
[ ] Other

15.1 Describe additional risks that should be considered for the system being assessed. If there are any additional risks or details not previously elaborated, detail them here:

Application currently exists in 1 availability zone only.

15.2 **Miscellaneous Risk Ranking** - In the view of the threat modeler, are any of the miscellaneous threats significant? Rank the miscellaneous threats:
[x] Low
[ ] Medium (2 points)
[ ] High (5 points)

15.3 **Action Items** - List any follow-up/action items identified during the threat model:

THREAT MODEL TOTAL SCORE: **21**

□ LOW <21
☒ MEDIUM 21-40
□ HIGH >40

Appendix A3

INCLUDES NO DIRT - SAMPLE BRAINSTORMING WORKSHEET

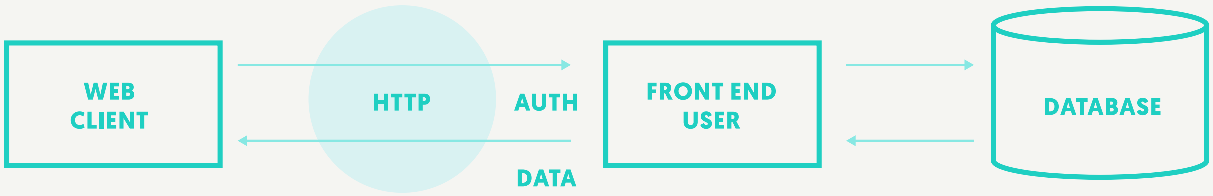
For complex threat models that require traditional brainstorming sessions, this worksheet can help focus the team on risks.

SYSTEM OR PROCESS DESCRIPTION:

The Patient Record Application is a web-based tool to allow patients to access their health records. It consists of a web front-end application and a back-end datastore of their data.

Data Flow Diagram with trust boundaries:
Hand drawn diagrams or whiteboard photos are sufficient for brainstorming

PATIENT RECORD APPLICATION (EXAMPLE)



THREATS

Circle all that apply:

Actors

- [✓ Malicious 3rd Party]
- [✓ Employee]
- Vendor
- [✓ Participant]
- Customer
- Regulator
- Partner
- Researcher

Processes

- Marketing
- Application
- Eligibility
- Enrollment
- Kickoff
- [✓ Claims]
- [✓ Billing]
- Milestones
- Reporting
- [✓ Record Request]
- Customer Onboarding
- Customer Termination
- Support Call
- Vendor Onboarding
- Vendor
- Termination
- Software Development
- Change Management
- Employee Hiring
- Employee Termination
- [✓ Clinical process]

Other

- [✓ Natural Disasters]
- Geo Political Unrest

VULNERABILITIES AND ATTACK VECTORS

List known or suspected vulnerabilities and attack vectors in the system. Refer to OWASP (https://www.owasp.org) and CAPEC (https://capec.mitre.org) for common attack vectors:. Duplicate this page as necessary to document all vulnerabilities in the system.

#	VULNERABILITY	ATTACK VECTOR
1	User credentials could be guessed	Brute force attack on login prompt
2	Web app transmits over HTTP unencrypted	Packet sniffer
3	Natural Disaster risk	Earthquake
4		
5		

INCLUDES NO DIRT CHECKLIST

Check the risks that apply to each vulnerability and attack vector from the list above.

	RISK (What we want to avoid)	GOAL (What is threatened by the vulnerability)	VULNERABILITY				
			1	2	3	4	5
I	IDENTIFIABILITY	Anonymity					
N	NON-REPUDIATION	Plausible Deniability					
C	CLINICAL ERROR	Correct Application of Clinical Standards					
L	LINKABILITY	Unlinkability					
U	UNLICENSED ACTIVITY	Proper Credentials or Licensure					
D	DENIAL OF SERVICE	Availability			✕		
E	ELEVATION OF PRIVILEGE	Authorization					
S	SPOOFING	Authentication	✕	✕			
N	NON-COMPLIANT TO POLICY OR OBLIGATIONS	Policy or Contractual Adherence					
O	OVERUSE	Minimum Necessary					
D	DATA ERROR	Integrity		✕			
I	INFORMATION DISCLOSURE	Confidentiality		✕			
R	REPUDIATION	Non-Repudiation		✕			
T	TAMPERING	Integrity		✕			

ACTION ITEMS

List action items to address above risks.

		VULNERABILITY #
1	Verify that application locks accounts after a large number of unsuccessful attempts. Reference NIST 800-63b for limits.	1
2	Implement TLS encryption	2
3	Explore option to create a disaster recovery instance in another AWS region.	3
4		
5		
6		
7		
8		
9		
10		

Appendix B - Sample Documents

INCLUDES NO DIRT - SAMPLE ASSESSMENT QUESTIONNAIRE

System Description - Describe the tool/process/service/system being analyzed in this questionnaire. If it involves a third party vendor, provide vendor information, URLs, and other information pertinent to your analysis. Attach any pertinent documentation or diagrams, including the results of any brainstorming sessions:

1.0 **Identifiability** - Does the tool/process/service/system require anonymity for compliance?
[ ] Required (1 point)
[ ] Not Required (go to question 2.0)

1.1 Does the tool/process/service/system have strong controls to ensure anonymity?
[ ] Yes
[ ] No (2 points)

1.2 **Anonymity Controls** - Describe how anonymity is enforced:

2.0 **Non-Repudiation** - Does the tool/process/service/system require plausible deniability for compliance?
[ ] Yes (1 point)
[ ] No (go to question 3.0)

2.1 Does the tool/process/service/system have controls to ensure plausible deniability?
[ ] Yes
[ ] No (2 points)

2.2 Describe how plausible deniability is enforced:

3.0 **Clinical Error** - Does the tool/process/service/system involve or impact clinical activities?
[ ] Yes(1 point)
[ ] No (go to question 4.0)

3.1 Does the tool/process/service/system correctly enforce clinical standards and prevent the introduction of clinical error?
[ ] Yes
[ ] No (2 points)

3.2 Explain how clinical errors are prevented:

3.3 Clinical Monitoring - Describe any monitoring of clinical activity contained in the tool/process/service/system that would identify clinical errors:

4.0 **Linkability** - Does the tool/process/service/system require unlinkability or de-identification?
[ ] Yes(1 point)
[ ] No (go to question 5.0)

4.1 Does the tool/process/service/system enforce unlinkability or de-identification?
[ ] Yes
[ ] No (2 points)

4.2 Explain how unlinkability is enforced:

5.0 **Unlicensed Activity** - Does the tool/process/service/system require a specific license (Federal, State, other) to be used/performed? Consider in your response both the person providing or performing the service, and/or the entity (company) doing the same.
[ ] Yes(1 point)
[ ] No (go to question 6.0)

5.1 Does the tool/process/service/system check the license of the user, and deny the user if unlicensed?
[ ] Yes
[ ] No (2 points)

5.2 Explain the licenses required and how license checks are enforced:

6.0 **Denial of Service** - Is the tool/process/service/system considered mission critical?

[ ] Yes (2 points)

[ ] No

6.1 Does the tool/process/service/system have a defined availability target?

[ ] Yes

[ ] No (1 point)

6.2 Describe the availability targets, contingency plans, and how availability is monitored.

7.0 **Elevation of Privilege** - Does the tool/process/service/system have controls to enforce authorization?

[ ] Yes

[ ] No (2 points)

7.1 Does the tool/process/service/system involve customer data, patient data, employee data, or other sensitive or confidential data?

[ ] Yes (2 points)

[ ] No (go to quesiton 7.5)

7.2 Data Classifications - check all that apply

[ ] Protected Health Information (PHI) (go to question 7.3) (2 points)

[ ] Customer Data (1 point)

[ ] Patient Data (1 point)

[ ] Employee Data (1 point)

[ ] Company Sensitive Data (1 point)

[ ] Company Confidential Data (1 point)

7.3 **PHI Identifiers** - Which PHI identifiers are included in the data?

[ ] Name

[ ] Address (including all geographic subdivisions smaller than state)

[ ] Dates related to an individual (birthdate, treatment date, etc.)

[ ] Telephone number

[ ] Fax number

[ ] Social Security number (2 points)

[ ] Medical record number

[ ] Health plan beneficiary number

[ ] Account number

[ ] Certificate or License number (including drivers license number)

[ ] Vehicle or device serial number

[ ] Web url

[ ] Email address

[ ] IP Address

[ ] Biometric identifiers including voice or fingerprint

[ ] Photographic image

[ ] Any other characteristic that could uniquely identify an individual

7.4 Describe the types of data and the authorization mechanisms

7.5 **Role-Based Authorization** - Does the tool/process/service/system control authorization by defining specific user roles, and assigning users to those roles?
[ ] Yes
[ ] No (1 point)

7.6 Does the tool/process/service/system define authorization using the principles of LEAST PRIVILEGE and MINIMUM NECESSARY?
[ ] Yes
[ ] No (1 point)

8.0 **Spoofing** - Does the tool/process/service/system have mechanisms to authenticate users or processes?
[ ] Yes
[ ] No (2 points)

8.1 Describe the authentication mechanisms:

8.2 Does the tool/process/service/system conform to NIST 800-63b standards for user names, passwords, and other factors?
[X] Yes (go to question 8.3)
[ ] No (1 point)

8.3 What AAL level is required by tool/process/service/system?
[x] AAL1 (single factor)
[ ] AAL2 (multi-factor)
[ ] AAL3 (multi-factor with hardware)

8.4 Describe the reasons why authentication is not required:

9.0 **Non-Compliant to Policy or Obligations** - What policies or obligations govern the use or function of the tool/process/service/system?
[ ] HIPAA (2 points)
[ ] Privacy Policy (1 point)
[ ] Terms of Use
[ ] Security Policy
[ ] Healthcare Compliance Policy (2 points)
[ ] Customer Contracts (1 point)
[ ] Employee Handbook
[ ] Vendor Contract
[ ] Omada as a Business Associate (1 point)
[ ] Vendor or Partner as a Business Associate (2 points)
[ ] Other policy or obligation
[ ] Not Applicable (go to question 10.0)

9.1 Describe how the tool/process/service/system adheres to the identified policies and obligations above:

9.2 Does the tool/process/service/system have the ability to monitor or audit for compliance with the identified policies?
[ ] Yes
[ ] No (go to question 9.4)(1 point)

9.3 Describe how policy compliance is monitored or audited:

9.4 Is the tool/process/service/system in scope for any third party/independent audit or assessment?
[ ] Yes
[ ] No (go to question 10.0)

9.5 Identify the third party audits that apply to the tool/process/service/system:
[ ] SOC 2
[ ] HITRUST
[ ] ISO 27001
[ ] PCI
[ ] Financial Audit
[ ] Vendor SOC 2, HITRUST, ISO, or PCI
[ ] Customer audit or review
[ ] Other

(*** if the answer to question 7.1 was no, skip section 10**)

10.0 **Overuse** - Does the tool/process/service/system have mechanisms to enforce the use of the "minimum necessary" amount of data and to prevent overuse?
[ ] Yes
[ ] No (go to question 11.0) (1 point)
[ ] Not Applicable (go to question 11.0)

10.1 Describe the mechanisms that restrict use and access to the minimum necessary amount:

11.0 **Data Error** - Does the tool/process/service/system have mechanisms to ensure data integrity?
[ ] Yes
[ ] No (go to question 12.0) (2 point)
[ ] Not Applicable (go to question 12.0)

11.1 Describe the data integrity mechanisms:

(* **if the answer to question 7.1 was no, skip section 12**)

12.0 **Information Disclosure** - Does the tool/process/service/system have mechanisms to ensure Confidentiality?

[ ] Yes

[ ] No (go to question 13.0) (2 points)

12.1 Describe the mechanisms used to ensure confidentiality:

12.2 Confidentiality Mechanisms - select all that apply:

[ ] Data is encrypted at rest (answer question 12.3)

[ ] Data is encrypted during transmission (answer question 12.4)

[ ] Passwords are hashed with a one-way function

[ ] Data is stored, processed and transmitted on a protected network

[ ] Data is stored, processed and transmitted in a protected facility (answer question 12.5)

12.3 What method of encryption is used to protect data at rest?

12.4 What method of encryption is used to protect data during transmission?

12.5 **Secure Facility** - Where is the data located?

12.6 **Data Locality** - Is the data processed, stored or accessed outside the United States?

[ ] Yes (2 points)

[ ] No

(* **if the answer to question 2.0 was yes, skip section 13**)

13.0 **Repudiation** - Does the tool/process/service/system require non-repudiation for security?

[ ] Yes (1 point)

[ ] No (go to question 14.0)

13.1 Does the system have strong mechanisms to ensure non-repudiation?

[ ] Yes

[ ] No (2 points)

13.2 Describe the controls used by the system to ensure non-repudiation:

13.3 Non-repudiation Mechanisms - select all that apply:
[ ] User activities are logged
[ ] Log files capture IP addresses
[ ] Log files capture machine ID or profile
[ ] System ensures accurate timestamps
[ ] System utilizes digital signatures
[ ] User activities are recorded and can be replayed
[ ] System requires out-of-band confirmation (email confirmation)
[ ] System requires multiple people to perform sensitive functions (separation of duties)
[ ] System retains/archives previous versions of data (version control)

13.4 How long are log files retained?
[ ] <3 months (1 points)
[ ] 3 - 6 months
[ ] >6 months

14.0 **Tampering** - Does the tool/process/service/system have mechanisms to prevent tampering?
[ ] Yes
[ ] No (go to question 15) (2 points)

14.1 Describe the mechanisms that exist to prevent tampering:

14.2 Anti-Tampering Mechanisms - select all that apply:
[ ] Physical Security
[ ] Network Security
[ ] Endpoint Security
[ ] Chain of Custody
[ ] Change Management Process
[ ] Third Party Vulnerability Assessments
[ ] Code Review
[ ] Other

15.0 **Miscellaneous Risks** - Is the tool/process/service/system susceptible to any additional threats? Select all that apply:
[ ] Physical Risks (1 points)
[ ] Environmental Risks (1 points)
[ ] Criminal Risks (1 points)
[ ] Disaster Risks (1 points)
[ ] Regulatory Risks (1 points)
[ ] Vendor Risks (1 points)
[ ] Competitive Risks (1 points)
[ ] Other

15.1 Describe additional risks that should be considered for the system being assessed. If there are any additional risks or details not previously elaborated, detail them here:

15.2 **Miscellaneous Risk Ranking** - In the view of the threat modeler, are any of the miscellaneous threats significant? Rank the miscellaneous threats:
[ ] Low
[ ] Medium (2 points)
[ ] High (5 points)

15.3 **Action Items** - List any follow-up/action items identified during the threat model:

THREAT MODEL TOTAL SCORE: □

□ **LOW <21**

□ **MEDIUM 21-40**

□ **HIGH >40**

INCLUDES NO DIRT - SAMPLE VENDOR QUESTIONNAIRE

1.0 **General** - Please describe the services you are providing:

1.1 **General** - Provide your current W-9 and payable information:

1.2 **General** - Omada Health, Inc., is considered a covered entity under HIPAA. If required, will your company execute a Business Associates Agreement (BAA)?
[ ] Yes
[ ] No (2 points)

2.0 **Contracts** - Attach MS Word versions of all contracts and service level agreements for our legal review.

2.1 **Contracts** - What are your standard insurance policies and limits?

2.2 **Contracts** - Attach your most recent Certificates of Insurance.

2.3 **Availability** - Does your service include an availability guarantee (SLA)?
[ ] Yes
[ ] No (1 point) (go to question 2.6)

2.4 **Availability** - Describe your availability targets, contingency plans, and how availability is monitored and guaranteed.

2.5 **Availability** - What is your availability guarantee?
[ ] <99% (1 point)
[ ] 99% (1 point)
[ ] 99.9%
[ ] 99.99%
[ ] >99.99%

2.6 **Availability** - Do you have a formal Business Continuity and Disaster Recovery Plan?
[ ] Yes
[ ] No (1 point) (go to question 3.0)

2.7 **Availability** - Please provide your Business Continuity Plans and Disaster Recovery Plans, and the results of / your most recent test.

3.0 **Policies** - Do you have documented security and privacy policies?
[ ] Yes
[ ] No (2 point) (go to question 3.2)

3.1 **Policies** - Attach your security and privacy policies. Include all of the following, if available:
Security Policy, Privacy Policy, Encryption Policy, Network Policy, Wireless Policy, Acceptable Use Policy, SDLC Policy, Change Management Policy, Patch Management Policy, Monitoring Policy, Log Management Policy, Backup and Recovery Policy, Incident Response Policy, Security Incident Response Policy, and Password Policy:

3.2 **Third Party Assessment** - Does your company have a third party assessment or certification, such as SOC 2 Type 2, HITRUST, or ISO 27001?
[ ] Yes
[ ] No (2 points) (go to question 4.0)

3.3 **Third Party Assessment** - Attach the results, including any third party penetration test results:

4.0 **Authentication** - Do you support integration to Okta for single sign on via SAML?
[ ] Yes
[ ] No (1 point) (go to question 4.2)

4.1 **Authentication** - If Okta is enabled, is SAML enforced?
[ ] Yes (go to question 5.0)
[ ] No (1 point) (go to question 5.0)

4.2 **Authentication** - If you do not support SAML, does your authentication policy comply with NIST 800-63b?
[ ] Yes
[ ] No (1 point)

5.0 **Authorization** - Does your service enforce role-based access?
[ ] Yes
[ ] No (1 point)

5.1 **Authorization** - Describe the available roles available within your service.

5.2 **Authorization** - Does your service involve the accessing, processing or storage of sensitive information? If so, which types?
[ ] PHI (2 points)
[ ] PII (2 points)
[ ] Omada Confidential (1 point)
[ ] Public
[ ] Other (go to question 5.3)

5.3 **Authorization** - Please specify other types of information:

6.0 **Confidentiality** - Is your data encrypted at rest?
[ ] Yes
[ ] No (2 points)

6.1 **Confidentiality** - Is your data encrypted in transit?
[ ] Yes
[ ] No (2 points)

6.2 **Confidentiality** - What are the encryption algorithms you support?

7.0 **Non-repudiation** - Are user activities logged or recorded?
[ ] Yes
[ ] No (2 points)

7.1 **Non-repudiation** - How long are log files retained?
[ ] <3 months (1 point)
[ ] 3 - 6 months
[ ] >6 months

8.0 **Hosting** - Where is your service hosted (cloud, colocation, own facility, other)?

8.1 **Hosting** - Describe the security and availability controls of the facilities that host your service.

8.2 **Hosting** - Provide any third party assessments of your facilities or hosting providers if applicable.

8.3 **Hosting** - Is any part of your service delivered outside the United States?
[ ] Yes (2 points)
[ ] No

8.4 **Hosting** - If required, can you agree to a data locality requirement that all Omada data be kept inside the United States?
[ ] Yes
[ ] No (1 point)

9.0 **Personnel** - Do you background check all employees delivering the service to include felony criminal history and employment history?
[ ] Yes
[ ] No (1 point)

INCLUDES NO DIRT - SAMPLE BRAINSTORMING WORKSHEET

For complex threat models that require traditional brainstorming sessions, this worksheet can help focus the team on risks.

SYSTEM OR PROCESS DESCRIPTION:

Data Flow Diagram with trust boundaries:
Hand drawn diagrams or whiteboard photos are sufficient for brainstorming

THREATS

Circle all that apply:

Actors

Malicious 3rd Party

Employee

Vendor

Participant

Customer

Regulator

Partner

Researcher

Processes

Marketing

Application

Eligibility

Enrollment

Kickoff

Claims

Billing

Milestones

Reporting

Record Request

Customer Onboarding

Customer Termination

Support Call

Vendor Onboarding

Vendor

Termination

Software Development

Change Management

Employee Hiring

Employee Termination

Clinical process

Other

Natural Disasters

Geo Political Unrest

VULNERABILITIES AND ATTACK VECTORS

List known or suspected vulnerabilities and attack vectors in the system. Refer to OWASP (https://www.owasp.org) and CAPEC (https://capec.mitre.org) for common attack vectors:. Duplicate this page as necessary to document all vulnerabilities in the system.

#	VULNERABILITY	ATTACK VECTOR
1		
2		
3		
4		
5		

INCLUDES NO DIRT CHECKLIST

Check the risks that apply to each vulnerability and attack vector from the list above.

	RISK (What we want to avoid)	GOAL (What is threatened by the vulnerability)	VULNERABILITY				
			1	2	3	4	5
I	IDENTIFIABILITY	Anonymity					
N	NON-REPUDIATION	Plausible Deniability					
C	CLINICAL ERROR	Correct Application of Clinical Standards					
L	LINKABILITY	Unlinkability					
U	UNLICENSED ACTIVITY	Proper Credentials or Licensure					
D	DENIAL OF SERVICE	Availability					
E	ELEVATION OF PRIVILEGE	Authorization					
S	SPOOFING	Authentication					
N	NON-COMPLIANT TO POLICY OR OBLIGATIONS	Policy or Contractual Adherence					
O	OVERUSE	Minimum Necessary					
D	DATA ERROR	Integrity					
I	INFORMATION DISCLOSURE	Confidentiality					
R	REPUDIATION	Non-Repudiation					
T	TAMPERING	Integrity					

ACTION ITEMS

List action items to address above risks.

		VULNERABILITY #
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		