

CAFDA, JUNE 2020

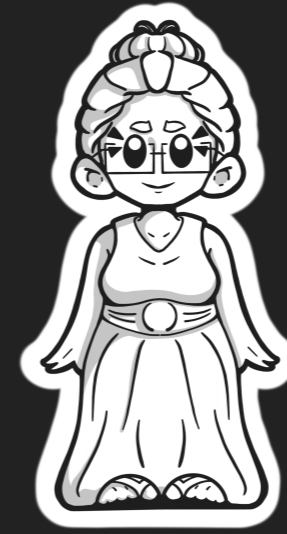
HEATHER McCUE

---

# HIPAA COMPLIANCE

## HEATHER McCUE

- ▶ Lead Developer, Harmonic
  - ▶ FileMaker Certified: versions 7 - 18
  - ▶ First use: 1988, FileMaker II
- ▶ Developer of CDMPro
  - ▶ HIPAA-compliant App for SC Department of Mental Health
- ▶ Authored white paper, "FileMaker – A Tool of Compliance"
- ▶ Compliance Consultant to other FileMaker Developers
- ▶ 'Oma' to seven brilliant grandchildren



### DISCLAIMER...

This is not intended to be a substitute for legal consultation

I am Heather McCue, Lead Developer at Dallas-based Claris Partner, Harmonic Software Production Studios.

I won't bore you by reading aloud the minutia of detail shown here, the gist of which is that I've been around a good long while, and much of my FileMaker career has been spent working with compliance for regulated environments.

Before we get started, I should clarify that I am not an attorney << [CLICK to show DISCLAIMER](#) >>.

However, what I share with you today **IS** based on three decades of FileMaker experience, nearly two of which have revolved heavily around compliance.

Okay then, let's dive in.

# WHY HIPAA? WHY NOW?

If you develop FileMaker-based custom apps intended for use within the medical industry, you need to be familiar with HIPAA. If you were familiar with HIPAA back in the day, it's time for a refresher.

Even if you don't expect to take on any HIPAA-regulated clients, you may just find the topic more relevant than you expected in light of recent pandemic-related changes to workplace environments and workforce distributions.

## WHAT WE'LL COVER TODAY

- ▶ HIPAA Basics
- ▶ Developer Responsibilities
- ▶ HIPAA Specifics
- ▶ Developing for Compliance
- ▶ Deployment

Our outline for today includes:

- The basics
- Your responsibilities
- The specifics
- Development, and
- Deployment

# HIPAA BASICS

## HISTORY — Health Insurance Portability and Accountability Act

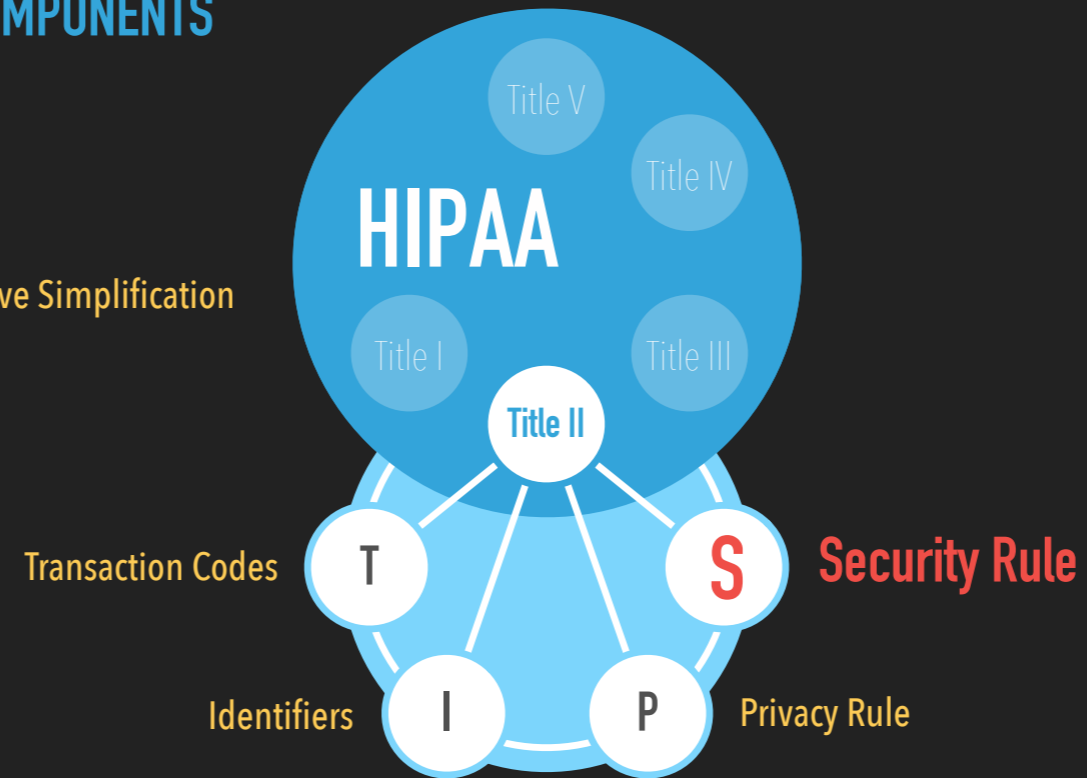
- ▶ 1996 –HIPAA enacted by Congress
  - ▶ Administered by the U.S. Department of Health and Human Services
- ▶ 2009 – HITECH Act
- ▶ 2013 – HIPAA Omnibus Final Rule



- >> Enacted by Congress in 1996, HIPAA — which stands for the **Health Insurance Portability and Accountability Act**, so two ‘A’s not two ‘P’s — went into effect nearly two decades ago.
- >> HIPAA is administered by the Dept. of Health & Human Services
- >> The **Health Information Technology for Economic and Clinical Health Act** — HITECH —
  - is also administered by HHS. The HITECH Act was created in 2009 to motivate the implementation of Electronic Health Records and supporting technology
- >>Then in 2013, HHS introduced the HIPAA Omnibus Final Rule — a single rule to finalize their implementation of both HIPAA and the HITECH Act

## HIPAA COMPONENTS

**Title II:**  
Administrative Simplification



45 CFR Parts 160, 162 & 164 (Titles I, II, III, IV, & V)

>> Our focus is on Title II: Administrative Simplification, which covers four areas: (represented here as T.I.P.S.)

- >> Transaction Codes
- >> Identifiers
- >> the Privacy Rule, and
- >> the Security Rule

The **Security Rule** is a developer's primary focus since it pertains specifically to the **protection of electronic information**.

When a Covered Entity refers to HIPAA compliance, they **could** be referring to any of the four provisions within Title II {Administrative Simplification}. When speaking of HIPAA compliance in the context of systems or development, we are referring specifically to the **Security Rule**.



## PRIMARY OBJECTIVES OF THE SECURITY RULE

1. Ensure data confidentiality, integrity, and availability
2. Protect against unauthorized access

The Security Rule boils down to two primary objectives:

1. “Ensuring confidentiality, integrity, and availability”
  - Well, the meaning of confidentiality is fairly obvious, but what about integrity?
  - And why is availability a concern? We’ll get into these when we discuss HIPAA Specifics
2. Keep in mind that the need to protect against unauthorized access applies to both internal & external threats, from known and potentially unknown sources

## WHAT IS COVERED?

- ▶ The Security Rule regulates all instances of electronic Protected Health Information (PHI) within the medical industry
- ▶ What is PHI?

**Any unique identifying number, characteristic, or code, unless no individual could be identified from it in any manner, and it is not derived from or related to information about the individual.**

So what data, specifically, is covered by HIPAA?

>> Electronically stored PHI within the medical industry — which by the way is not limited to a doctor's office or hospital.

>> And what exactly is this PHI that we need to protect?

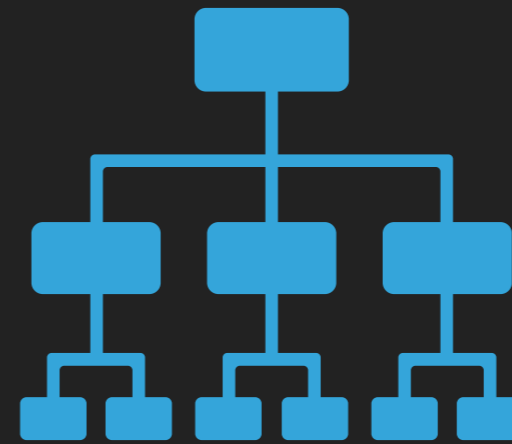
>> It essentially boils down to this: If the data can be used to uniquely identify a specific individual, then it is PHI and is subject to the provisions of HIPAA and HITECH.

{ Examples of PHI would include, but are not limited to:

- ▶ Names (of patient or family members)
- ▶ Geographic subdivisions smaller than a state
- ▶ Dates directly related to an individual, such as a birthday
- ▶ Phone, Fax, Email
- ▶ Identifying Numbers (Social Security, Medical record, Health plan beneficiary, accounts, and certificate/license numbers)
- ▶ Vehicle identifiers and serial numbers, including license plate numbers
- ▶ Device identifiers and serial numbers
- ▶ URLs & IP numbers
- ▶ Biometric identifiers, including finger and voice prints
- ▶ Full face photo images and comparable images }

## WHO IS COVERED?

- ▶ Covered Entity
- ▶ Business Associates
- ▶ Sub-Contractors



So who needs to comply with HIPAA?

>> The Covered Entity, your client, may be a provider, medical practice or facility, a research lab, or even a medical equipment manufacturer.

If your client is in the healthcare industry and they maintain or transmit electronic PHI, they are probably a covered entity.

>> You — the consultant and developer with necessary access to the PHI — are a Business Associate

Hosting services such as AWS are also Business Associates

>> Your sub-contractors are also subject to the same compliance requirements

## HITECH — Health Information Technology for Economic and Clinical Health

- ▶ Electronic Health Records (EHR)
  - ▶ Monetary incentives
  - ▶ Penalties
- ▶ Business Associate Liability
- ▶ Subject to Audit
- ▶ Increased enforcement
- ▶ Established “harm” criteria and Breach Notification requirements



- Between 2011 & 2015, healthcare providers were given monetary incentives for being able to demonstrate meaningful use of Electronic Health Records (EHR)  
<< **CLICK** to drop money >>  
That was the carrot.
- After 2015, penalties were levied for **failing** to demonstrate such use.  
And so begins the stick.
- HITECH also made Business Associates directly liable for compliance with portions of the HIPAA Privacy and Security Rules;  
Extended the definition of a Business Associate, and
- Subjected Business Associates to the possibility of audit;
- While also increasing enforcement scrutiny for violations of HIPAA & HITECH
- HITECH also introduced breach requirements and established concrete criteria to determine whether “harm” occurred as the result of a PHI breach  
— One could say **“the HITECH carrot was followed by a substantial stick”**

# DEVELOPER RESPONSIBILITIES

**The integrity, confidentiality,  
and availability of the data  
within your control is  
sacrosanct.**

Your choices need to be made with an understanding and appreciation for the fact that ...  
“The integrity, confidentiality, and availability of the data within your control is sacrosanct.”

**THE FORCES OF EVIL  
ARE FULLY FUNDED.**

**Steven Blackwell**



You must also be mindful that, in the words of Steven Blackwell:  
“The forces of evil are fully funded.”

## RESPONSIBILITIES

- ▶ Data Protection

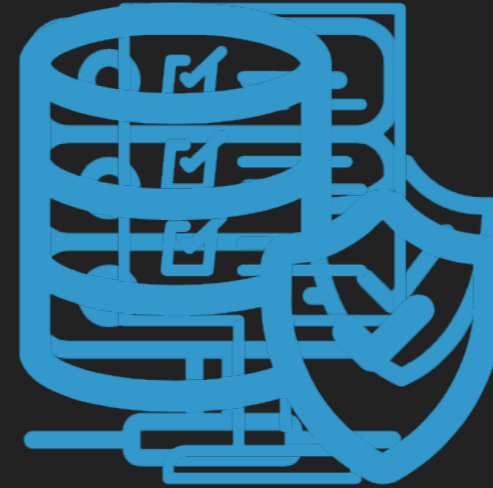
**YES**

- ▶ System Protection

**PERHAPS**

- ▶ Business Rules

**NO**



As a Business Associate it will be important for you to define with your client the scope of your responsibilities.

>> As the developer, you will likely be responsible for data protection.

>> You may or may not also be responsible for systems and network protection, and

>> Unless your stable of talent happens to include an experienced writer with compliance expertise, you are unlikely to develop the Business Rules, and you certainly won't be responsible for enforcing them



## BUSINESS ASSOCIATE AGREEMENTS



- ▶ Use PHI solely for meeting its obligations, and return or destroy all PHI on termination
- ▶ Implement safeguards to protect electronic PHI
- ▶ Notify Covered Entity of a breach of unsecured PHI
  - ▶ Cooperate with breach analysis
  - ▶ Including risk assessment
- ▶ Report any Security Incident, and mitigate any known harmful effect
- ▶ Take reasonable steps to ensure employees don't cause a breach of terms
  - ▶ Have and apply appropriate sanctions
- ▶ Possible auditing
- ▶ Additional Business Associate Agreements
  - ▶ Subcontractors
  - ▶ Hosting Providers

A Covered Entity is required to have a Business Associate Agreement with you prior to disclosing or sharing any electronic PHI with you.

In addition to your agreement to comply with all applicable Security Rule requirements, this document protects the Covered Entity by formalizing your agreement to:

- Use PHI solely for meeting your obligations to the Covered Entity, and as may otherwise be required by law or regulation, and that on termination of the agreement you will return or destroy all PHI in your possession
- Implement reasonable & appropriate safeguards to protect electronic PHI  
You will implement appropriate safeguards to prevent the unauthorized use or disclosure of PHI.  
More specifically, you will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that you create, receive, maintain, or transmit on behalf of the Covered Entity.
- You will notify the Covered Entity of any known breach of unsecured PHI, and
  - cooperate with their breach analysis procedures,
  - Including risk assessment, if requested
- You will report to the Covered Entity any "Security Incident", and you will to the extent practicable, mitigate any known harmful effect of a use or disclosure of PHI by yourself, employees or agents, in violation of the Agreement
- You will take reasonable steps to ensure that employee actions or omissions don't cause you to breach the terms, and
  - You will have and apply appropriate sanctions against any employee, subcontractor, or agent who uses or discloses the Covered Entity's PHI in violation of the Agreement or applicable law
- You are also acknowledging that to ensure the Covered Entity's compliance, the Secretary of HHS has the right to audit your records and practices related to the use and disclosure of PHI
- A similar, but separate Business Associate's Subcontractor Agreement is also required if you engage the services of a non-employee

- The same applies to Hosting Providers

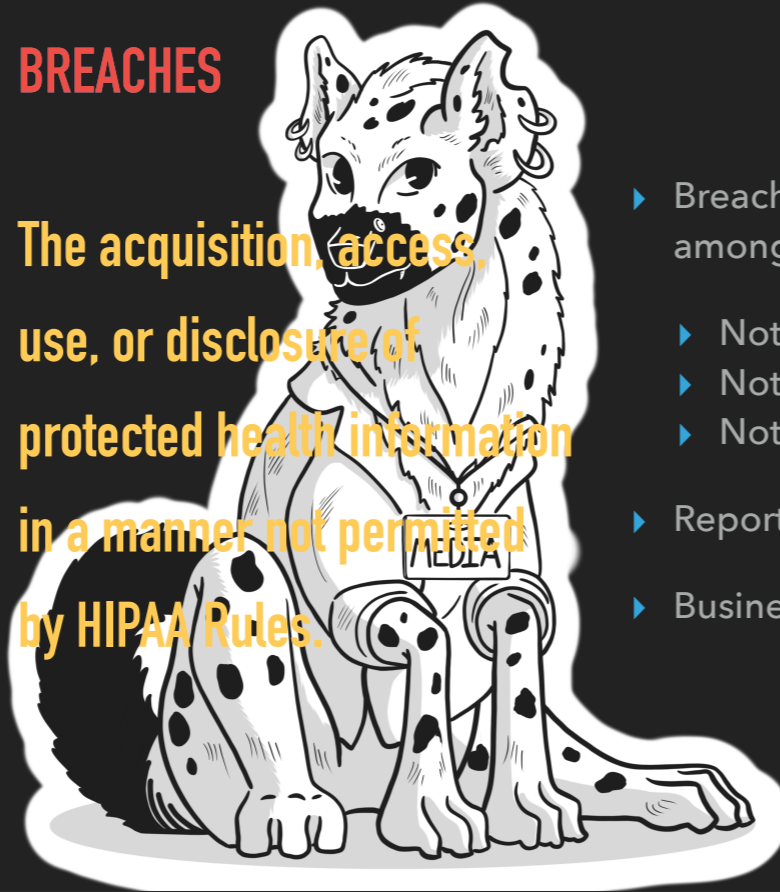
##### STOP HERE #####

*One of the biggest changes that affects HIPAA compliant software and SaaS (software as a service) companies is that hosting providers are now considered business associates under HIPAA. That means colocation and cloud hosting services that house PHI (protected health information) now fall under the purview of HIPAA and are subject to civil & criminal penalties of up to \$1.5M. These penalties and fines apply whether or not the hosting provider knowingly has PHI on their servers or in their data center.*

*The final ruling also makes it clear that healthcare & HIPAA compliant service and software companies must sign a BAA (business associate agreement) with their hosting providers and that the HIPAA compliant service & software companies have ultimate accountability for their hosting provider meeting or not meeting HIPAA requirements.*

## BREACHES

The acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA Rules.



- ▶ Breach Notification regulations are among the HITECH provisions
- ▶ Notify affected individuals
- ▶ Notify HHS
- ▶ Notify the Media
- ▶ Report to the Covered Entity
- ▶ Business Associates must comply

A breach is essentially “The acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA Rules.”

- << CLICK >>

HITECH requires prompt notifications of a breach event, and

- The failure to comply with these requirements can result in a significant financial penalty.

- << CLICK to show three sub-bullets >>

Notifications must be sent to the impacted individuals, HHS, and to the media if more than 500 were impacted.

- The timing requirements for these notifications vary somewhat based on how many individuals were impacted by the breach, and your own State laws may be more strict in this regard

It is typically the Covered Entity who will issue the notifications, including to the media if warranted, but

- Business Associates are required to promptly report the discovery of a breach.
- You must also cooperate in their breach analysis procedures, which may include performing a risk assessment, if requested.

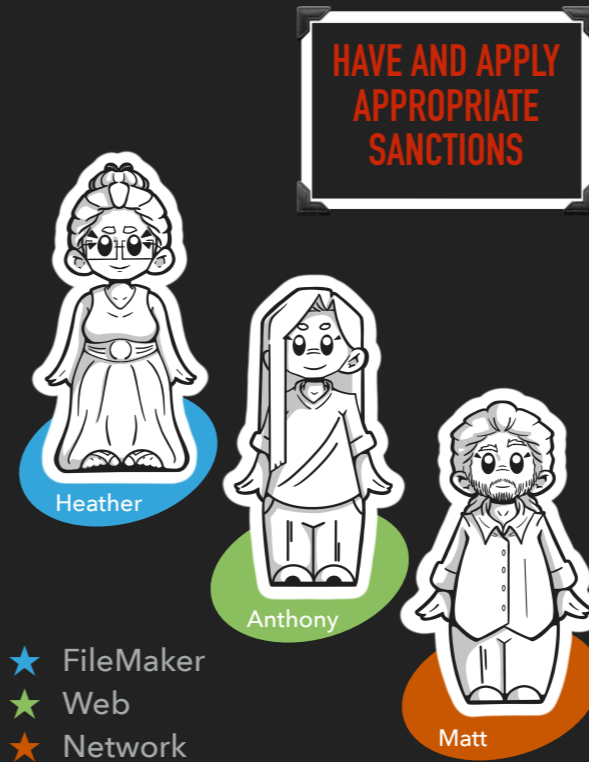
Now, if you're not 100% convinced about the importance of following the terms of your Business Associate Agreement ...

- << CLICK to show the media hyena >>

Consider the potential damage to your reputation that could be wrought by our friend the Media Hyena.

## YOUR TEAM

- ▶ Take reasonable steps to ensure employees don't cause a breach of terms
- ▶ Sub-contractors
- ▶ Hosting Providers



- If you're working with a team, you obviously don't want them causing a breach.

- Think about who's going to be on your internal team

<< **CLICK to show team** >>

- FileMaker developers
- Non-FileMaker developers, Web, mySQL, etc., and
- Network Admins
- When choosing your team, you want trustworthy individuals, preferably with a history of following best practices, not only with security but in their code. Remember that data integrity and availability are among the Security Rule's primary objectives, so an intern honing their skills may not be the way to go.
- You also need to set expectations with your team
- In addition to communicating clearly their roles and responsibilities, you are required by HITECH

<< **CLICK** >>

- To have and apply appropriate sanctions.
- Regardless of who was actually responsible, remember that if there is a breach, your own policies may be subject to audit.

You should also take similar precautions with any non-employee team members,

<< **CLICK** >>

and if a sub-contractor or

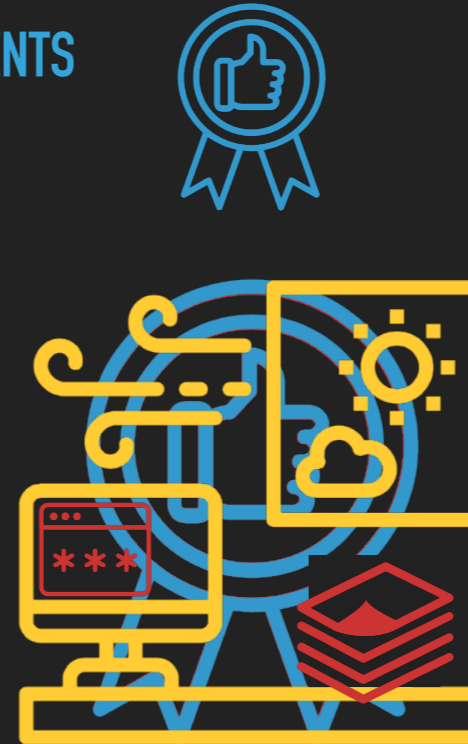
hosting provider doesn't have a Business Associate Agreement directly with the Covered Entity,

make sure that a Sub-Contractor Business Associate Agreement is in place prior to granting any access to systems containing PHI.

<< **CLICK** >>

## YOUR BEST PRACTICES & ENVIRONMENTS

- ▶ Passwords
- ▶ Proxy files
- ▶ **Never Externally Auth a [Full Access] Account**
- ▶ Physical Environment
  - ▶ Paper
  - ▶ Leaving your desk



You'll need to define your own best practices, but here are a few examples:

- >> Do you save [Full Access] passwords to client systems? What about Admin Passwords to a client's Server Admin Console?  
As a general rule, I never save these details in my local keychain.
- >> Consider using a separate file — with reduced privileges — for reporting and other low-level access tasks
- >> **DON'T EVER SET A [FULL ACCESS] ACCOUNT TO EXTERNAL AUTH**
- >> Implement and follow Business Rules that are appropriate for your environment
  - >> If you work in an office with cleaning crews, don't leave paper laying around if it contains PHI; lock it up when you leave, shred it when you're done.  
I follow the same rule when I work from home.
  - >> Do you log out when you step away from your desk? An open App that contains PHI should never be left unattended.  
When I'm at the office, I'm in the habit of logging out of my desktop when I walk away from my desk — Always.  
When I'm at home, my rule is that I log out when I clock out, even if I'm just breaking for lunch and don't plan to leave the house.

# HIPAA SPECIFICS

## RULE TYPES

- ▶ Standards and Implementation Specifications
- ▶ Standards
  - ▶ Required
- ▶ Implementation Specifications
  - ▶ Required
  - ▶ Addressable

The Security Rule includes two types of rules:

- ▶ >> Those are **Standards** and **Implementation Specifications**
  - ▶ >> All of the **Standards** are Required, but
  - ▶ >> **Implementation Specifications:**
    - include both Required and Addressable rules

## REQUIRED VS. ADDRESSABLE

	STANDARDS	SPECIFICATIONS	
		Required	Addressable
Administrative	9	10	11
Physical	4	2	6
Technical	5	2	5
	<b>32</b>		<b>22</b>
		<b>54</b>	

The Security Rule includes 54 separate rules { which are often overlapping in their intent }.

18 Standards and 36 Implementation Specifications

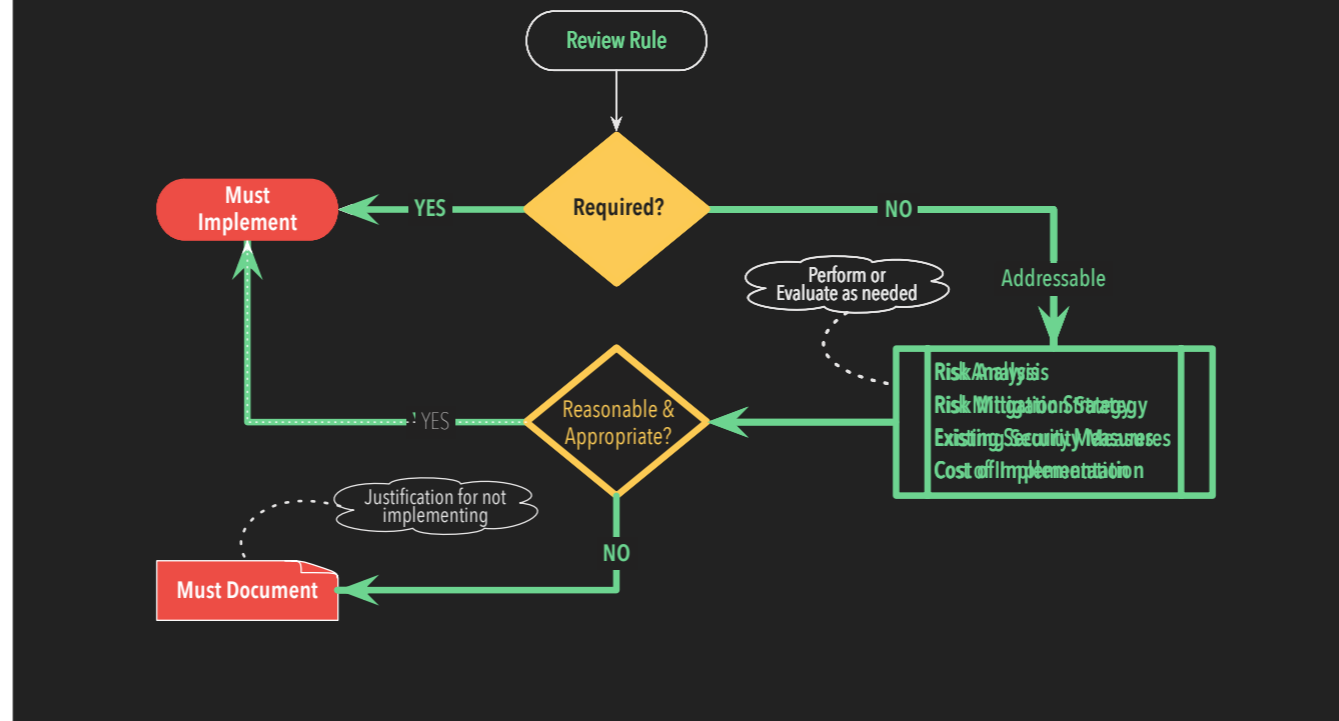
Each is classified as either Administrative, Physical, or Technical.

Our primary focus as developers is on the Technical.

- ▶ So you're probably wondering what the difference is between Required and Addressable, and why we care.
  - ▶ >> "Required" means required, and
  - ▶ >> An Addressable Rule is also required,
    - ▶ but only if implementation is deemed Reasonable & Appropriate
- ▶ So how is this determination made? << CLICK to next slide >>



## REASONABLE &amp; APPROPRIATE



1. First review the rule and determine if it is defined as Required
2. If it is, then it must be implemented (if applicable)
3. If it is not, then it is Addressable; you and/or your client will need to perform a risk analysis, and evaluate a risk mitigation strategy, the existing security measures, and costs associated with implementation
4. Based on these findings the Covered Entity (usually following your guidance in combination with their budget) must decide if implementation of the measures necessary to comply are both Reasonable & Appropriate
5. If they are, then the Rule must be implemented, and
6. If they are not, then the justification for not implementing the Rule must be documented
  - This documentation is ultimately the Covered Entity's responsibility, but you may be asked to provide supporting details

## TRANSLATING REGULATIONS

- ▶ 2019 DevCon Session:  
*Compliance is a Process: FileMaker is Your Toolbox*

<https://community.claris.com/en/s/article/DevCon-2019-sessions-by-track>

- ▶ *FileMaker and HIPAA – A Tool of Compliance*  
(pg 7)

[https://support.claris.com/s/article/FileMaker-Pro-and-HIPAA-1503692934786?language=en\\_US](https://support.claris.com/s/article/FileMaker-Pro-and-HIPAA-1503692934786?language=en_US)

- ▶ [har.fm/hipaa](https://har.fm/hipaa)

For advice on how to translate the HIPAA regulations into actionable development tasks, I would refer you to my 2019 DevCon session, “*Compliance is a Process: FileMaker is Your Toolbox*”, And to page 7 of my white paper, “*FileMaker and HIPAA – A Tool of Compliance*”.

The white paper is available from Claris Support, and the DevCon Session is available in the Claris Community. You can also find both at “[har.fm/hipaa](https://har.fm/hipaa)”.

## THE ESSENTIAL DOZEN

1. Access Control
2. Access Reporting
3. User Authentication
4. Password Management
5. Auto Log-Off
6. Incident Tracking
7. Encryption
8. Data Integrity
9. Audit Log
10. Data Authentication
11. Contingency Planning
12. User Documentation

If you intend to develop a compliant system, a thorough review of the applicable regulations is in order, but there's no need (or time) to review all 54 rules today. The following short list summarizes for brevity the technical requirements that will impact your development choices: Not all of these will be applicable to every project, but those that appear in green are related to Requirements.

>> 1...12

User Documentation is not a Technical Requirement, but more on this later.

# DEVELOPING FOR COMPLIANCE

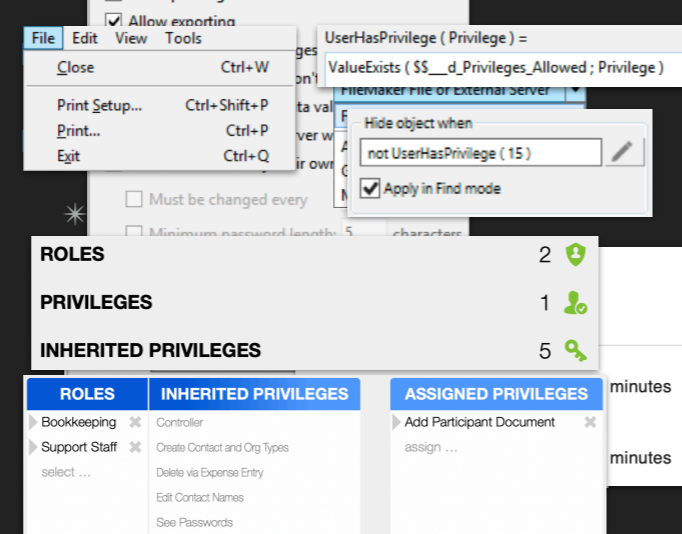
HIPAA does not specify methodology because the regulations are expected to endure while technology is expected to continue evolving.

HIPAA does not specify methodology because the regulations are expected to endure while technology is expected to continue evolving.

## SECURITY

▶ FileMaker-Native Security Toolset

▶ Other Privileges Options



\* Accounts & Privileges

\* Authentication Options

\* Extended Privileges

\* Access & Design

\* Script Triggers

\* Hide Conditions

\* Button Bars

\* Cards

\* Validated Scripts

\* Conditional Scripts

\* Script Triggers

\* Hide Conditions

\* Button Bars

\* Cards

\* Validated Scripts

\* Conditional Scripts

- \* There are plenty of security-specific resources that have been developed by the community, so I'm not going to get into the nitty gritty of how to secure your App, but I would be remiss if I didn't take a few moments to remind you of some of the most applicable options.
- \* These are important because we are building custom Apps, which means you won't find an on-off switch to "make-it-HIPAA-compliant". Instead, you will layer options that are the most appropriate for your App when deployed in its intended environment.

<< CLICK >>

The FileMaker-Native Security Toolset

Accounts, Authentication Options, Privileges, Extended Privileges, Access & Design — Record-Level Access (RLA), Field-level Validations, File Access, Encryption At Rest

<< CLICK >>

Your Data- & Design-Driven Options can be invaluable

Roles & Privileges, UI (Custom Menus, Custom Functions, Script Triggers, Hide Conditions, Button Bars, Cards)

<< CLICK >>

When it comes to Scripting

You want to Control the Experience and Exposure, Use OnFirstWindowOpen, Conditionally Forked Scripts, and Validated Scripts

<< CLICK >>

For your Hosting & Network requirements

Encrypt Traffic, employ Idle Time Out, and follow good Backup Hygiene

Let's return now for a closer look at the essential dozen and explore some of your development options for compliance ...

## 1. ACCESS CONTROL

- ▶ Deny access to unauthorized users
- ▶ Require user-specific log-ins
- ▶ Incorporate Access Controls & User Authentication
- ▶ Apply Encryption At Rest to all files
- ▶ Use SSL
- ▶ Restrict referential access to files, and
- ▶ Implement appropriate external security measures



To meet the requirement for **Access Control**, you will need to ...

1. Deny access to unauthorized users
2. Require user-specific log-ins
3. Incorporate Access Controls & User Authentication
4. Apply Encryption At Rest to all files
5. Use SSL
6. Restrict referential access to files, and
7. Implement appropriate external security measures

>> And remember that although you and your team may be brilliant, in the absence of comprehensive access controls, your Apps will be susceptible to the wily and devious nature of the nefarious.



## 2. ACCESS REPORTING

- ▶ Server Logs
- ▶ Session Logs
- ▶ Activity Logs

6/12/2020 5:50:06 PM	HDA_JMatic	192.168.1.236 -2 6.3
6/12/2020 7:00:30 PM	[Full Access]	ProAdvanced 17.0.6
6/12/2020 5:48:05 PM	harmonicadmin on TS	192.168.1.236 -2 6.3
	[Full Access]	ProAdvanced 17.0.6
6/12/2020 4:17:54 PM	HV	192.168.1.236 -2 6.3
	[Full Access]	ProAdvanced 18.0.3

Session Log

__creation	_serverScriptName	Result	Comment
8/1/2017 12:30:12 AM	[SSS] Build BillingItems from BillingSheets	Start ...	8/1/2017 12:30:12 AM
8/1/2017 12:30:13 AM	[SSS] Build BillingItems from BillingSheets	Billing Sheets Evaluated: 157	0:00:01
8/1/2017 2:48:14 AM	[SSS] Trigger_Billing_Push	Start ...	8/1/2017 2:48:14 AM
8/1/2017 3:22:18 AM	Set Billing Triggers	Pushed: TimeItems, 0; BillingItems, 0; Adjustments, 0; LineItems, 2928	0:34:04
8/1/2017 3:29:09 AM	UpdateBillingLines	Billing Lines Updated: 6157	0:06:51
8/1/2017 11:32:06 AM	Prep for OT	[1] Build Staff Weeks; Additional Staff Weeks Built (for OT testing): 15766	1:25:41

Activity Log

To meet the requirement for **Access Reporting**, you can

1. Use the Server Logs, which will include both successful and unsuccessful access attempts
2. Add Session Logs to record and maintain a full history of successful system entry, and
3. Integrate Activity Logs to record processes like sever-side schedules that have the potential to bypass Start scripts
  - This example shows the running of several server-side scripts; and several of these entries include the results and total run time
  - An Activity Log like this can also be used to track the performance of specific processes over larger swaths of time than can be accessed from a single Server Log.

### 3. USER AUTHENTICATION

- ▶ FileMaker Accounts
- ▶ External Authentication/SSO
- ▶ Role- and function-based privileges

Choose the most appropriate authentication method, and  
Short of a single-user app, role-based options are required.

{Claris ID, an SSO, supports multi-factor authentication}

**EMPLOYEES**

- Daisy Graves
- Heather McCue**
- Steve Sykora
- Matt Monroe
- Paul Mitchell
- Robert Sandefur
- Eric Clark
- Anthony Nguyen
- Jefferson Matic
- MJ Cook
- Bob Trammel

## Heather McCue

**i** Summary   **DevCons**   **Roles & Privileges**

**DEVCONS**   2000 Palm Desert ... 2019 Orlando (18) ✓

**ROLES**   0

**PRIVILEGES**   0

**INHERITED PRIVILEGES**   0

**HARMONIC**

Let's take a look at assigning Roles and Privileges

— Let's add a Role

Notice that the Privilege "See Password" was inherited

— Let's add another Role

You can see that more Privileges were inherited

— We can also assign a Privilege directly

— And we can disable Roles or Privileges at any time

— Turning them back on and returning to our Summary

We can see that I've been assigned two Roles, inherited five Privileges, and I've been explicitly assigned one Privilege

After Roles and Privileges have been assigned, the Start script that runs when the App is opened creates a new session record and collects the user's active privileges, which can be recorded in a global field or variable for quick reference by hide conditions, scripts, and other objects.

<<CLICK>> Shown now are three variations of simple Custom Function calcs that will return a boolean true/false result.

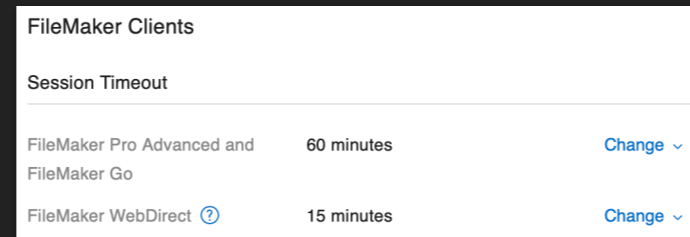
#### 4. PASSWORD MANAGEMENT

**If you are not using external authentication, you will need to provide password management tools**

The Covered Entity must have the ability to add and remove authorized users, But it is often [or could become] true that the individuals tasked with this responsibility won't or shouldn't have [Full Access] privileges. Fortunately, for an App that uses only FileMaker Accounts, the necessary functionality can be scripted.

## 5. AUTO LOG-OFF

**Utilize idle limits via FileMaker Server  
or establish auto log-off controls**



FileMaker Clients		
Session Timeout		
FileMaker Pro Advanced and FileMaker Go	60 minutes	<a href="#">Change</a> ▾
FileMaker WebDirect <a href="#">?</a>	15 minutes	<a href="#">Change</a> ▾

Auto Log-Off is required, and easy to implement, but

Remember that Idle Time Out requires both the Session Timeout setting in the FileMaker Server Admin and a Privilege Set that allows the server to disconnect.

If you are going to deploy an un-hosted, stand-alone file that contains PHI, you will need to employ an alternate approach to ensure compliance.

## 6. INCIDENT TRACKING

A “Security Incident” is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system

Before we can determine how best to track incidents, we need to understand what qualifies as an incident.

A “Security Incident” is the **attempted or successful** unauthorized access, use, disclosure, modification, or destruction of information **or interference with system operations** in an information system.

- Whether or not you will be responsible to provide Incident Tracking will depend on your agreed scope of work
- Your methods for tracking incidents will likely vary depending on the types of incidents being tracked and the level of incursion
- A multi-layer approach might include a combination of access, audit, and activity logs, in addition to external system monitoring

## 7. ENCRYPTION

- ▶ Implement Encryption At Rest
  - ▶ All Files
  - ▶ ALWAYS
- ▶ Encrypt Network Traffic
- ▶ Encrypt External Data Sources

Encryption of PHI protects confidentiality by preventing unauthorized disclosure — including when physical access to a file has been compromised — so it has always been an essential and required component of compliance.

>> Thanks to Encryption At Rest, the days of complex data structures are behind us, along with the multiple versions of each protected field that were necessary in order to manage their encryption & decryption.

There is, in my opinion, simply no excuse for not implementing Encryption At Rest.

I would further argue that all files should always be encrypted — regardless of whether or not they are expected to contain PHI.

Client requirements are ever-evolving and it's simply too easy to introduce functionality and data to a file that wasn't originally expected to require encryption.

>> You must also encrypt your network traffic using SSL

>> And if your eco-system includes external data sources like MySQL that also contain PHI, these should be encrypted as well

## 8. DATA INTEGRITY

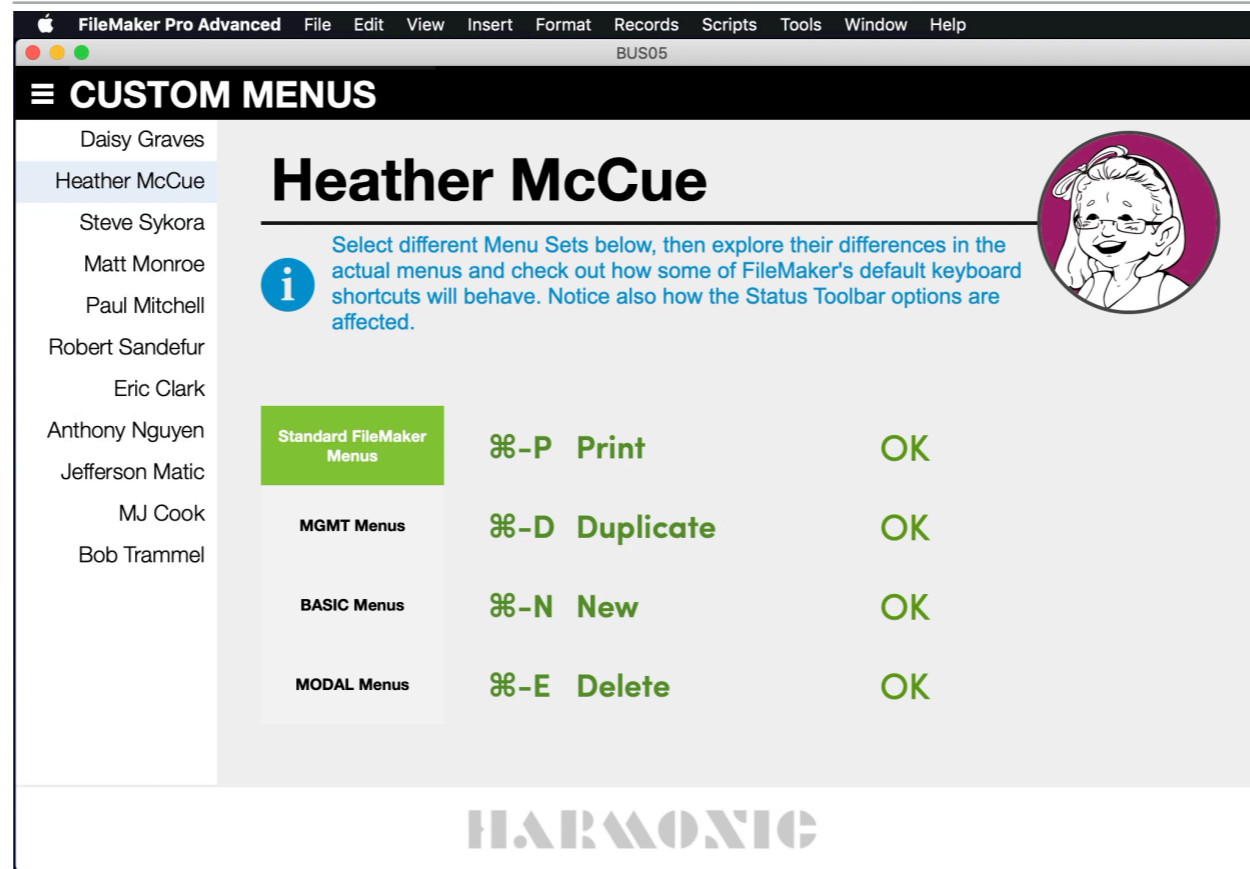
- ▶ Create a controlled environment where create, edit, and delete functionality is limited to authorized users under “proper” circumstances
- ▶ Employ data authentication methods for electronically transmitted data



To comply with Data Integrity requirements you need to...

1. Create an environment where create, edit, and delete functionality is not only controlled (which you can do via Accounts & Privileges), but where this functionality is limited to authorized users **under “proper” circumstances**
  - The tricky part here is in the definition of “proper”, which is determined not by statute, but by the Covered Entity who will establish which Roles are appropriate for whom and when. Fortunately, you can support the sometimes complex and changing definitions of “authorized” and “proper” by incorporating data-driven Role- and function-based access controls.
    1. Consider the plight of Owl’s Ophthalmology, where our receptionist, Sally Squirrel is the only user in the office with access to edit the scheduling calendar, but
    2. She gets sick and has to leave, so someone else whose primary role doesn’t normally include the need to access this functionality ...
    3. Dr. Owl for example, may need to temporarily assume Sally’s role.
2. Another component of data integrity may apply if data is transmitted electronically; in which case you may also need to employ data authentication methods to ensure transmission accuracy.





Let's take a quick look at Custom Menus, another tool you can employ to ensure data integrity.

>> We can see that our Standard FileMaker Menus include shortcuts for **N**ew, **D**uplicate, and **D**elete

- Switching to MGMT menus we no longer have access to the **D**uplicate shortcut, and if we select New or Delete — from either the menu or via keyboard shortcuts — the process is controlled by a script
- Our Basic menus contain none of these options, so if we want to provide this functionality, we'll have to provide a button or other access
- And finally, our Modal menus include little to nothing

## DEVELOPING FOR COMPLIANCE — DEMO: Trigger-Controlled Object Access

The screenshot displays a software interface with a list of employees and a script editor. The employee list includes names like Daisy Graves, Heather McCue, and Steve Sykora, and a table with columns for year and location. The script editor shows code for an OnModify+Exit trigger with parameter options for editing control.

```
OnModify+Exit [0=NoEdit; 1=EditAllowed; Null=ExitField]
1 # This script is called by Script Triggers to allow or disallow entry and/or modification
2 # May also be used to prevent exiting from a layout object when used with OnObjectExit
3
4 # PARAMETER OPTIONS:
5 # 0 = NO Editing
6 # Used in combination with an OnModify trigger,
7 # this will revert a disallowed edit, such as when a checkbox
8 # or radio button field is selected
9 # 1 = ALLOW Editing
10 # Exits script, action is allowed to continue
11 # NULL = EXIT
12 # Not the same as 0 because, this doesn't revert an edit
13 # Employed with an OnObjectModify on field with a value list, this allows
14 # the edit, but will subsequently exit the field.
15 # With a radio button-formatted field, for example, the editing actually
16 # occurs on selection, and because this does not undo, the edit is retained.
17 # When employed with an OnObjectEnter, entry is prevented
18
19 Set Variable [ $p ; Value: Get ( ScriptParameter ) ]
20 If [ $p = 0 ]
21 # 0 = NO Editing
22 Undo/Redo [ Undo ]
23 Exit Script [ Text Result: False ]
24 Else If [ $p = 1 ]
25 # 1 = ALLOW Editing
26 Exit Script [ Text Result: ]
27 Else
28 # no parameter = Exit field, e.g., pop-ups or to preventing field entry
29 Commit Records/Requests [ With dialog: On ]
30 Exit Script [ Text Result: 0 ]
31 End If
```

This demo will illustrate the use of Script Triggers to control object access.

It will also show how the same script, running with the same parameter, can behave differently based on field formatting.

<<CLICK to start video>>

- With my Edit Trigger Status parameter set to Null
  - I can edit the checkbox-formatted field, but
  - Not the Edit Box-formatted field
- After changing my parameter to Zero [0]
  - I am unable to edit either
- After switching my parameter to One [1]
  - I am able to edit either

Now let's take a look at how this works ... <<CLICK to show checkbox field>>

- To my checkbox-formatted field I've attached an OnObjectModify script trigger
- <<CLICK>> And to my edit field I've attached both OnObjectModify and OnObjectEnter triggers
- All three triggers call the same script and use the same parameter
- So why do I have an OnEntry trigger on the edit field, but not on the checkbox field?
  - Fields formatted as Checkbox or Radio Button behave differently:
  - The act of selecting or de-selecting a value triggers the field to know that it's been entered, but by that point the value has already been edited, so
  - attaching an OnObjectEnter trigger is redundant and won't always perform as expected[

Let's take a look at the script ... << CLICK to show script >>

- The script supports three options:

- NO Editing, ALLOW Editing, and EXIT Field
- using the parameters of 0, 1, and null
- The script is simple and can be applied to other objects as well
  - It can be used, for example, to prevent an end user from closing a popover or switching panels
- And the reason it works to prevent editing a checkbox field is because the NO Editing option includes an Undo step

## 9. AUDIT LOG

- ▶ Track data modification & record deletion
- ▶ Track system access
- ▶ Provide mechanisms for review

{ No Clicks Required }

Audit Logs come in many flavors and can be used to track multiple details.

You will need to track data modification — where appropriate and relevant — and system access, and provide your client with mechanisms for review

**COMMENT ALSO ON SELF-AUDITING TRANSACTIONAL TABLES, e.g., Validations & Errors**

# AUDIT LOGS

```

{
  "Edit" :
  {
    "2020-05-22 14:37:01 (5/22 2:37 PM)" :
    {
      "Account" : "web",
      "Layout" : "_php_EntryExpenses",
      "Level" : "0",
      "Status" : "New",
      "User" : "web",
      "Window" : "ISS_Docs_Exp"
    },
    "2020-05-22 14:37:13 (5/22 2:37 PM)" :
    {
      "Account" : "mmeyer",
      "Layout" : "List",
      "Level" : "2",
      "Script" : "Populate Expense Entry from JSON",
      "Status" : "Data Entry",
      "User" : "mmeyer",
      "Window" : "List"
    },
    "2020-06-03 08:14:51 (6/3 8:14 AM)" :
    {
      "Account" : "ladmin",
      "Layout" : "Detail Vendor Invoice",
      "Level" : "3",
      "Script" : "Payable Batch [Controls]",
      "Status" : "Validating",
      "User" : "ladmin",
      "Window" : "Detail"
    },
    "2020-06-03 08:14:53 (6/3 8:14 AM)" :
    {
      "Account" : "ladmin",
      "Layout" : "List",
      "Level" : "3",
      "Script" : "Validation Prep",
      "Status" : "Validating",
      "User" : "ladmin",
      "Window" : "List"
    },
    "2020-06-03 08:14:55 (6/3 8:14 AM)" :
    {
      "Account" : "ladmin",
      "Layout" : "Validations",
      "Level" : "-1",
      "Script" : "Validation Prep",
      "Status" : "Error",
      "User" : "ladmin",
      "Window" : "List"
    }
  }
}

```

5/23/2020 4:34:56 AM | ServerReportAgent | Complete | 3353

5/22/2020 3:23:57 PM | web | Complete

5/22/2020 3:23:57 PM | web | Bill I

5/22/2020 3:23:57 PM | web | Bill I

5/22/2020 2:16:49 PM | web | Bill I

5/22/2020 1:53:24 PM | kconroy | Bill I

5/22/2020 1:51:36 PM | kconroy | Queue

5/22/2020 4:32:53 AM | ServerReportAgent | Complete

Evaluate ( "List ( Get ( CurrentHostTimestamp ) & ' | ' & Get ( AccountName ) & ' | ' & GetFieldName( ClaimAction ) & ' | ' & GetFieldName( ClaimComment ) & ' | ' & \_CommentHistory ); [ClaimAction, ClaimComment ] )

Quote ( Get ( ScriptParameter ) );

\$json )

};

// RETURN \$json WHEN ...

Evaluate ( "\$json"; [ EntryExpenses::\_entryStatusLevel; EntryExpenses::\_c ] )

)

"User" : "ladmin",

"Window" : "List"

## 10. DATA AUTHENTICATION

- ▶ Prove that Data Integrity Controls worked
- ▶ Audit Logs don't prevent unauthorized activity
- ▶ Measures must be employed to ensure the failure of unauthorized attempts to alter or destroy PHI
- ▶ Test Plans

The Data Integrity requirement protects against unauthorized alteration or destruction. This is not that.

This refers instead to a system being able to substantiate that PHI has not been altered or destroyed in an unauthorized manner.

>> So this is essentially a requirement to prove that the Data Integrity controls are successful

- But how do you prove that something didn't happen?

>> An audit trail can document alterations and deletions, but the mere auditing of activity does not inherently prevent unauthorized activity

>> A comprehensive set of controls should be employed to ensure the failure of unauthorized attempts, and

- >> Formal test plans can be written, and QA testing performed to prove and document "successful failures"

## 11. CONTINGENCY PLANNING

Follow reliable backup procedures and develop a contingency plan appropriate to address the most likely emergencies



- ▶ Frequent
- ▶ Encrypted
- ▶ Tested
- ▶ Stored Offsite

The Covered Entity must be able to retrieve their data during or immediately following an emergency which renders either the data or usual security controls unavailable.  
<< CLICK >>

To accomplish this, you'll need to establish a reliable backup schedule and coordinate with your client to ensure that an **appropriate** contingency plan is in place.

Also, Backups must be:

<< CLICK >>

- Frequent,
- Encrypted,
- Tested, and
- Stored Offsite

If your client is located in a hurricane-prone region, their offsite backups should not be.

## 12. USER DOCUMENTATION

- ▶ Assist your client and end users with their training requirements
  - ▶ Tooltips & Legends
- ▶ Interactive QA tool
- ▶ Internal documentation may be reusable



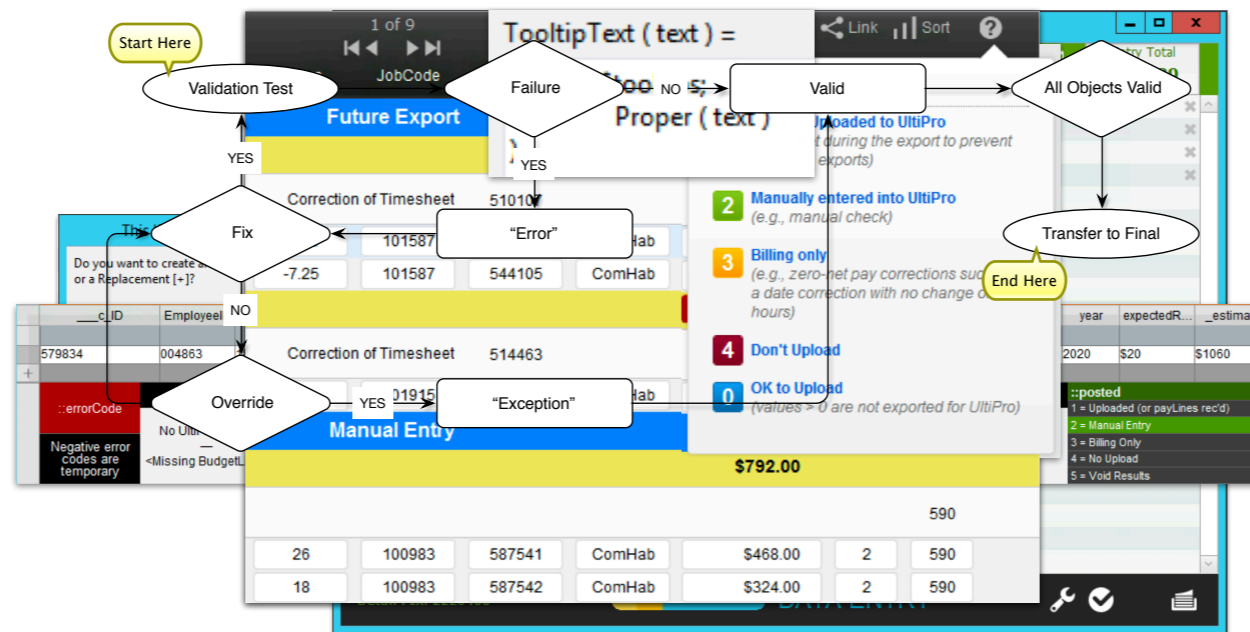
Though not a technical requirement, good documentation can serve multiple purposes and support appropriate use.

<< ONE CLICK ONLY >>

And while I'm on the topic of documentation, don't forget to self-document your code



## DOCUMENTATION EXAMPLES



- Simple tooltips & a legend (in the footer) for error & posting codes
- Interactive report with
  - Legend in a popover for entry codes with explanations
- A more traditional documentation of workflow
- An internal workflow example that could be used by the covered entity in their compliance documentation

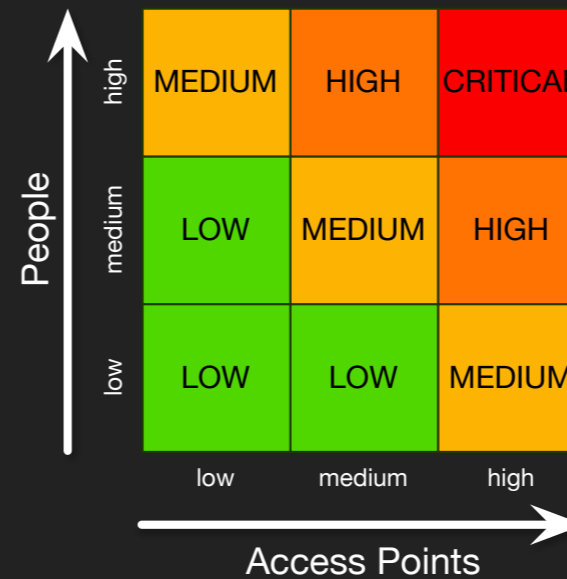
**DEPLOYMENT**

**The first and most important consideration when supporting compliance across multiple environments — within and beyond the FileMaker Platform — is an **evaluation of risk.****

“The first and most important consideration when supporting compliance across multiple environments — within and beyond the FileMaker Platform — is an **evaluation of risk.**”

## RISK CONSIDERATIONS

- ▶ What's Your Risk Profile?
  - ▶ Users Increase Risk
  - ▶ Access Points Increase Risk
- ▶ FileMaker First
- ▶ Don't Be Foolish or Shy
- ▶ Communicate Solutions



Your App's level of risk will not only guide the choices you make for addressing requirements, but it also serves to inform you (and your client) when it comes to defining responsibilities.

Most of OUR Apps are ever-evolving, which means initial risk assessments will need to be re-visited; though often within the more limited scope of a particular feature or perhaps the introduction of a new access point.

[1] So, What does your RISK PROFILE look like?

[1.1] How many users do you anticipate?

- On which platforms? Pro, Go, CWP, or perhaps Data API; What's your mix?
- Remember — More Users = Greater Risk

[1.2] Access points exist to support communications, in and/or out; so naturally, each introduces a potential point of vulnerability, which obviously increases risk

[2] 'FileMaker First' — Consider your requirements from the context of FileMaker first, then overlay those requirements — and your approach to addressing them — onto each additional access point

- Is the requirement even applicable?

If the requirement is to encrypt all PHI, for example, and a SQL transactions table used for reporting contains no PHI, do you need to encrypt the SQL table?

- If a requirement is applicable, will your approach in FileMaker extend elsewhere?
  - If not, how will you (or a trusted source) address it?

[3] I believe it was Bruce Lee who said, "A wise man can learn more from a foolish question than a fool can learn from a wise answer."

- It's essential that you honestly determine what you can do vs. where it may be preferable to retain others
- Should you, for example, consider outsourcing document retention?

[4] And finally, no one looks forward to giving (or receiving) potentially bad news; but if you are able to share your concerns — which you have a responsibility to do — while offering viable solutions to address them, you can be the hero.

- An honest Risk Assessment can open the door to expanded opportunities, and as I said just a few moments ago ...
- It will also help you define limits and establish responsibilities

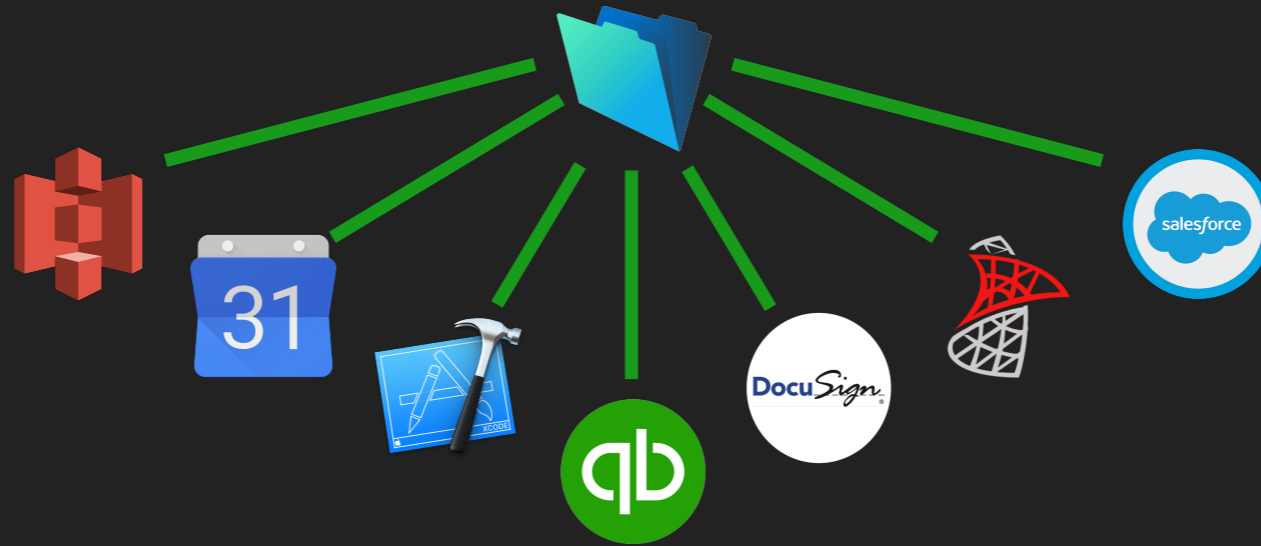
## WHAT'S IN YOUR ECO-SYSTEM?



- ▶ FileMaker Pro Advanced
- ▶ FileMaker Go
- ▶ FileMaker Server
- ▶ FileMaker Cloud
- ▶ FileMaker WebDirect
- ▶ Custom Web Publishing
- ▶ FileMaker Data API

- Within the FileMaker Platform, Pro Advanced is just the first of multiple access points, we also have ...
- Go,
- Server,
- Cloud,
- WebDirect, and
- Custom Web Publishing,
- And more recently, the FileMaker Data API

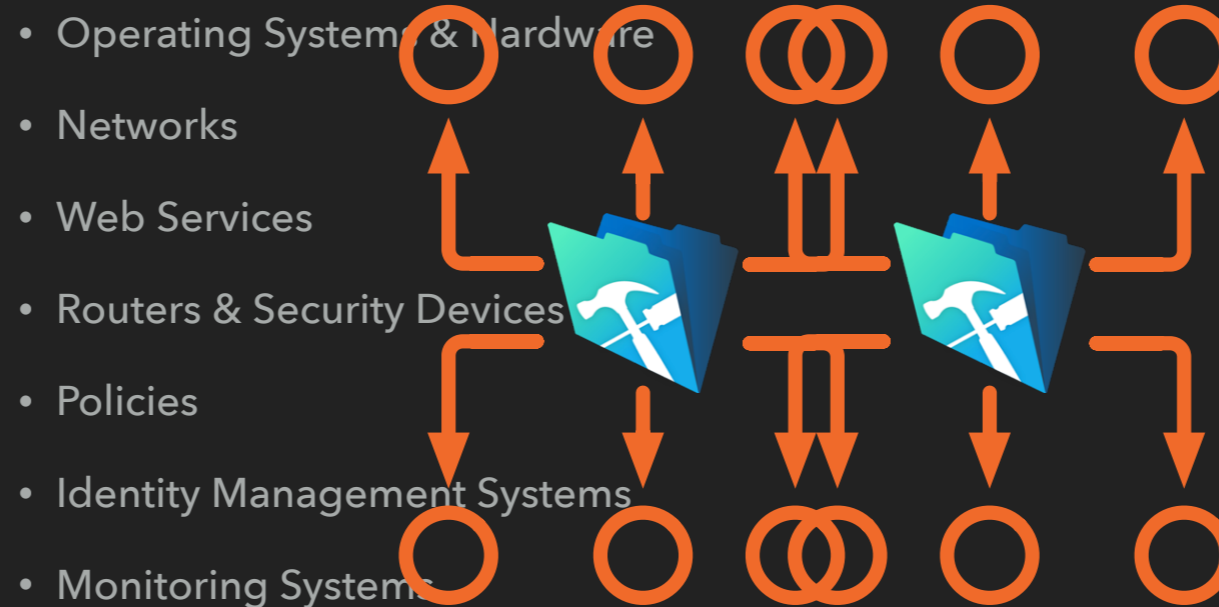
## WHAT ELSE IS IN YOUR ECO-SYSTEM?



But, you also need to consider what else is within the sphere of your eco-system?  
Here are just a few examples from the unlimited possibilities beyond the FileMaker Platform...

- Amazon S3 (Simple Storage System)
- Calendars
- iOS SDK (X-Code)
- QuickBooks
- DocuSign
- SQL
- Salesforce

## NON-FILEMAKER CONSIDERATIONS



There are a number of factors external to FileMaker itself that we also need to consider because they unequivocally affect our ability to deliver.

It's also important for you and your client to be on the same page about which of these you will and won't be responsible for; and IF not you, who?

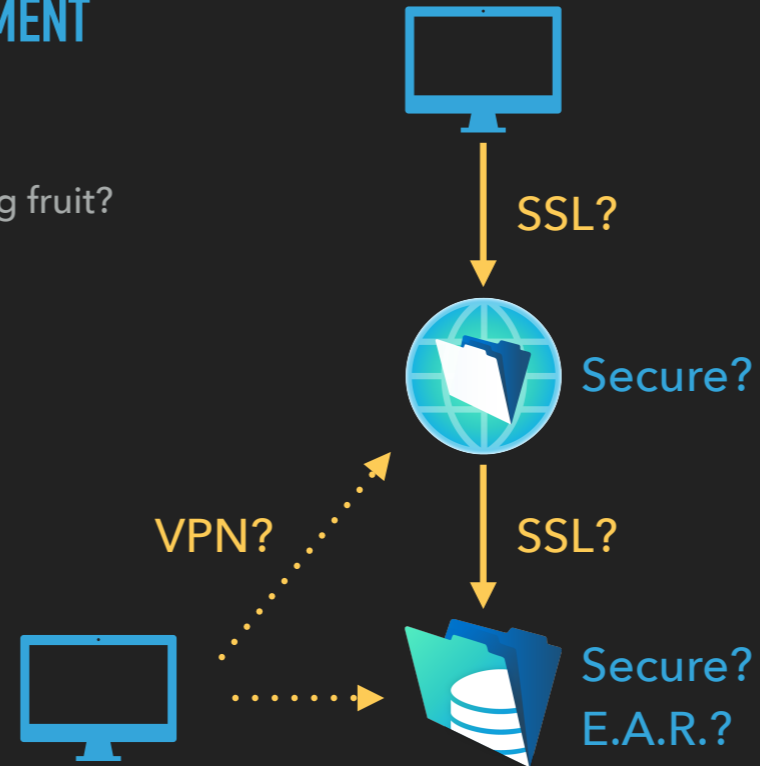
It has been my experience that the more regulated the environment, the greater the likelihood that you'll find yourself working with a client's internal or outsourced IT departments; and this is perfectly fine — sometimes even preferable — but when you rely and depend on fellow professionals, just remember the mantra: TRUST BUT VERIFY

- [1] So, who is responsible for systems and hardware?
- [2] What does the network look like? LAN, WAN, RemoteApp, Terminal Server, VPN
- [3] What about Web Services?
- [4] Who's responsible for routers and other security devices? And will they follow your recommendations?
- [5] Are there any external policies that you need to take into account (such as AWS policies, for example)?
- [6] Are Identity Management, and
- [7] Monitoring Systems part of the mix?



## NETWORK RISK ASSESSMENT

- ▶ What's the lowest hanging fruit?
  - ▶ Data Transfer
- ▶ How Many Hops?



- When assessing your App's level of risk for external threats, begin by identifying the lowest hanging fruit.
- The **Transfer of Data** is the easiest point to hit or probe, so ensuring "Security in Transit" is essential.
- To do this, you need to first ask yourself, "how many hops are there between my desk and the data storage?"

<< CLICK to start image build >>

<<CLICK >> SSL?

<<CLICK>> Secure?

<<CLICK>> LAN/WAN Client

## WEB SERVER

- ▶ Ancillary Services?
- ▶ Cached Data?
- ▶ Does the machine self-update?
- ▶ What else is this machine doing?
  - ▶ Email? **STOP NOW**
- ▶ DNS Server?
- ▶ The Talent



- Ask yourself, What are some of the ancillary services attached to the site?
  - What risks do they introduce and what mitigations are necessary?
- A Web Server is easy to turn on without securing
- Beware of self-updating
- What else is this machine doing?
  - Consider a LAMP machine (with Linux, Apache, MySQL, PHP, Perl, Python)
    - What else is the machine doing? Are these functions necessary? Are they secured?
    - If email is running — STOP
- Is DNS recursion disabled?
- Does your guy know what he's doing?

## HOSTING mySQL DATA

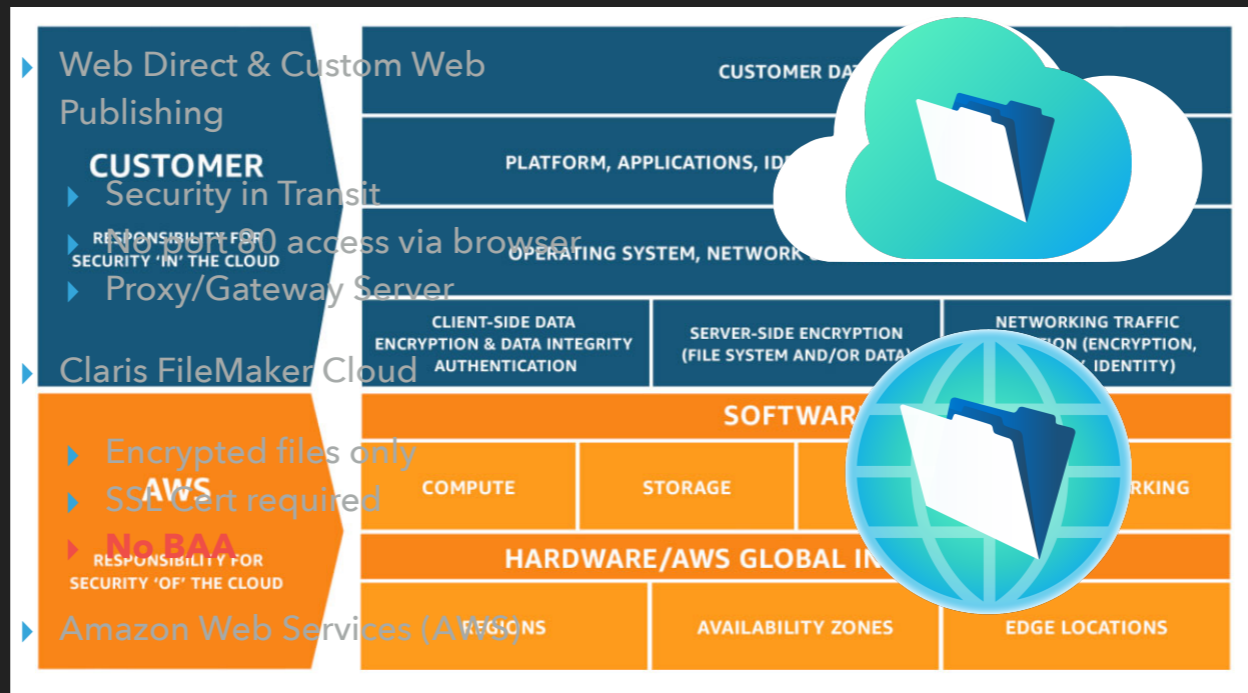
- ▶ Separate machine
- ▶ No public access
- ▶ VPN-only access
- ▶ Encrypted At Rest



- At Harmonic, we host mySQL data on a separate machine
- The mySQL machine is not available to the public at all
- VPN-only access via port 3306
- All data is Encrypted At Rest
  - mySQL Resource: [percona.com](http://percona.com)

## WEB &amp; CLOUD

## AWS Shared Responsibility Model



- Remember that when deploying via Web Direct or Custom Web Publishing,
  - SSL must be applied in addition to all other access and authentication requirements
  - Port 80 is no longer accessible via web browsers
  - Consider using a gateway proxy server that re-routes to the real server
- I'm often asked about FileMaker Cloud, and the good news is that
  - It won't host an unencrypted file, and
  - It **requires** an SSL Certificate
  - Unfortunately, << CLICK >> Claris does not currently offer a path for obtaining the required Business Associate Agreement, so it is not a viable option for Apps containing PHI — which brings us to ...
- Amazon Web Services (AWS)
  - What is the difference between FileMaker Cloud and FileMaker Cloud for AWS?
    - FileMaker Cloud for AWS was the first-generation cloud-hosting service offered through the AWS Marketplace (deprecation was announced in October of 2018), and
    - FileMaker Cloud is the newest Platform as a Service offered by Claris.
  - In case you're wondering why the BAA is required, or you're confused because you thought it wasn't, let me explain ...
  - Some cloud providers claimed that they were simply "**conduits**" – only housing, but never accessing PHI on their servers, but with the final ruling, HHS made it clear that conduits are considered Business Associates, subject to HIPAA compliance if they have "**persistence of custody**" of PHI.
    - In other words, if PHI data is stored in a data center, or on a cloud server, then the hosting provider is considered a business associate *[and must be able to demonstrate that they can meet the HIPAA administrative, physical and technical requirements to assure the confidentiality, integrity and availability of*

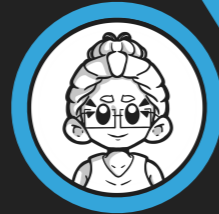
*electronic PHI*.

AWS has adopted a Shared Responsibility Model, [<<CLICK>>](#) and with this delineation of responsibilities, AWS will sign a BAA. I've provided links for this on our resource page.

IN CONCLUSION...

---

**THANK YOU!  
IT'S BEEN A PLEASURE.**



**Heather McCue**

## RESOURCES — [har.fm/hipaa](https://har.fm/hipaa)

- ▶ FileMaker and HIPAA—A Tool of Compliance  
*White Paper*
- ▶ Compliance Is a Process: FileMaker Is Your Toolbox  
*DevCon 2019*
- ▶ HITECH Breach Notification Rule  
*with relevant passages called out; includes a sample Breach Notification Letter*
- ▶ Links
  - ▶ Multiple HIPAA- and HITECH-specific Links  
*Including Business Associate Agreements*
  - ▶ AWS Compliance Links

A variety of downloads and links are available for your reference at "[har.fm/HIPAA](https://har.fm/HIPAA)"