

MGMA®

Medical Group Management Association

— Louisiana

Billeaud
Technology, llc

Introduction

- **20+ years IT Operational experience**
- **10 years IT Auditing and Risk Assessment (Oil&Gas & Healthcare)**
- **Certified Information Systems Auditor (CISA)**
- **Certified Information Security Manager (CISM)**

Agenda

- **Learn from Others**
- **General Audit Preparation Measures**
- **Specific Audit Preparation Activities**
 - **Meaningful Use (MU)**
 - **HIPAA**
- **HIPAA & MU Audit Process**

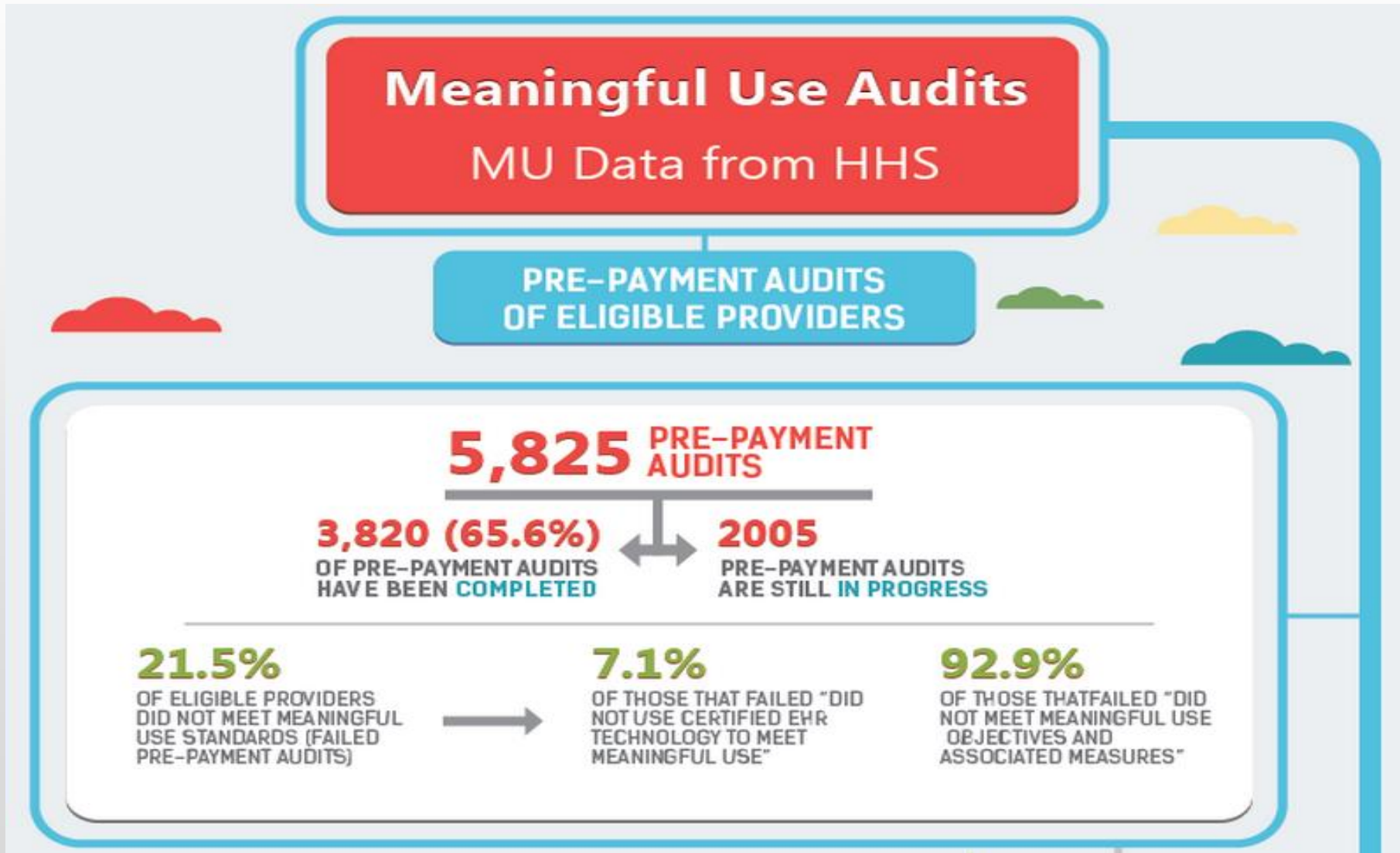
LEARN FROM OTHERS – HIPAA Pilot Audits



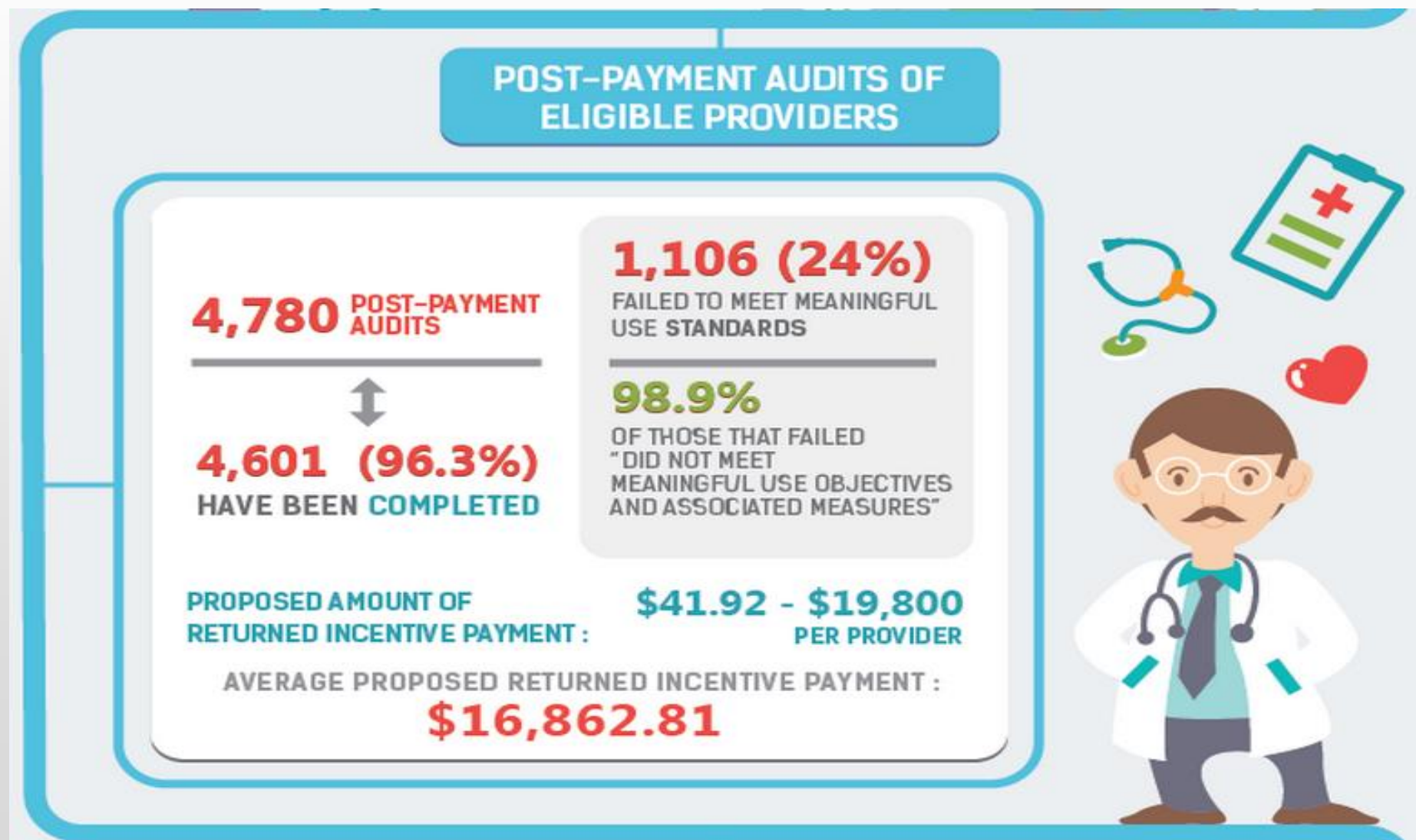
OCR HIPAA PILOT AUDIT PROGRAM

[\(day2-2_Isanches_ocr-audit.pdf\)](#)

LEARN FROM OTHERS – MU Audits



LEARN FROM OTHERS – MU Audits



LEARN FROM OTHERS – MU Audits

HIGHEST FAILURE RATES

PRE-PAYMENT AUDITS
FOR ELIGIBLE PROVIDERS:

PUERTO RICO

81.8% failure
(9 of 11)

NEVADA

52.6% failure
(10 of 19)

POST-PAYMENT AUDITS
FOR ELIGIBLE PROVIDERS:

MONTANA

84.4% failure
(27 of 32)

VERMONT

81.8% failure
(9 of 11)

LEARN FROM OTHERS – MU Audits

The most common problems identified are noncompliance with:

- 1. required data security risk assessment and**
- 2. a lack of adequate documentation to support some of the responses provided in the attestations.**

GENERAL AUDIT PREPARATION

- **Assume you will be Audited**
- **Create a Regulatory Binder**
- **Perform a Risk Analysis**
- **Develop and Execute a Risk Management Plan**
- **Formulate an Audit Response Plan**



GENERAL AUDIT PREPARATION

ASSUME YOU WILL BE AUDITED!

- Providers can be audited for up to six years after MU Attestation
- 22% of audited eligible providers (EPs) failed their first audit
- Consequences of Failed MU Audits:
 - Post-payment audit – Return of incentive payment plus interest
 - Pre-payment audit – Non-receipt of incentive payment for year
 - Subsequent audits of the previous and/or later attestation years
- Failed HIPAA Audits:
 - Possible financial penalties as a result of a Reportable Data Breach
 - OCR imposed monetary penalties, five involved fines of \geq \$1 million



GENERAL AUDIT PREPARATION

REGULATORY BINDER!

- Book of Evidence - each MU Attestation Year and all HIPAA activities
- Why do you need a Regulatory Binder?
- Who should be responsible for the Regulatory Binder?
- What should this binder contain?
- When should the Regulatory Binder be created/updated?
- Where should the Regulatory Binder be stored?
- Perform an independent review of the contents

GENERAL AUDIT PREPARATION

RISK ANALYSIS!

- Why should you perform a Risk Analysis?
- **Who should perform the Risk Analysis?**
- What do you need to document for the Risk Analysis?
- When should the Risk Analysis be performed?
- **Where should we look for ePHI?**

GENERAL AUDIT PREPARATION – RISK ANALYSIS

Where do we look for ePHI?

- **EVERYWHERE!**
- **Electronic Health Records (EHR) System**
 - Server in-house or Provider outsourced
 - System backup media (in-house or outsourced)
- **Map data flow - Incoming or outgoing ePHI**
 - Secure ePHI at rest and in transit
- **Devices**
 - Smartphones, Tablets, Laptops
 - Fax, printer, copier and/or scanner machines with hard drive or other media
 - Portable media which ePHI can be saved on



GENERAL AUDIT PREPARATION – RISK ANALYSIS

Who should perform Risk Analysis?

Someone who is,

- Independent, experienced and qualified
- Knowledgeable on how to document the process
- Unbiased for identification of risks to ePHI
- Able to formulate a practical and effective action plan to mitigate risk

GENERAL AUDIT PREPARATION – Risk Analysis

SCREENING QUESTIONS

Topic	Question	Response	Threat Vulnerability Statement	People/Processes	Technology
1. Security Program					
1.1	Roles & Responsibilities	[1.1] Has your organization formally appointed a central point of contact for security coordination? a) If so, whom, and what is their position within the organization? b) Responsibilities clearly documented? i.e. job descriptions, information security policy		Management has not defined responsibilities for the information security program. [TVS001]	N/A
1.2	External Parties	[1.2] Do you work with third parties, such as IT service providers, that have access to your patient's information? a) Does your organization have Business Associate agreements in place with these third parties? i.e. REC, IT Vendor, EHR Vendor, etc. b) If not, what controls does your organization have in place to monitor and assess third parties? i.e. Logging of VPN connections, EHR logs, etc.		Security breaches occur when dealing with third parties due to a lack of security considerations in the related third party agreement. [TVS002]	
2. Security Policy					

GENERAL AUDIT PREPARATION – Risk Analysis

PEOPLE and PROCESSES

		Perform Control Analysis		Exposure		Assess Risk		
Asset Management Category	Threat-Vulnerability Statement	Recommended Control Measures	Existing Control	Existing Control Effectiveness	Exposure Potential	Likelihood	Impact	Risk Rating
Security Program	Management has not defined responsibilities for the information security program. [TVS001]	All information security responsibilities are clearly documented . This is to ensure timely, safe and effective handling of all situations, administration user accounts-including additions, deletions, and modifications. [RCM001] - Ensure responsibilities are formalized within the employee(s) job descriptions as well as within relevant IS policies. - The Information Security Policy Template provided by the REC could help formalize this role.		0				
Security Program	Security breaches occur when dealing with third parties due to a lack of security considerations in the related third party agreement. [TVS002]	Agreements with third parties, such as IT vendors, which involve accessing, processing, communicating with or managing the organization's information or information processing facilities, or adding products or services to		0				

GENERAL AUDIT PREPARATION – Risk Analysis

TECHNOLOGY

Asset Management Category	Threat-Vulnerability Statement	Recommended Control Measures	Perform Control Analysis		Exposure	Assess Risk		
			Existing Control	Existing Control Effectiveness	Exposure Potential	Likelihood	Impact	Risk Rating
Security Program	Security breaches occur when dealing with third parties due to a lack of security considerations in the related third party agreement. [TVS002]	<p>Agreements with third parties, such as IT vendors, which involve accessing, processing, communicating with or managing the organization's information or information processing facilities, or adding products or services to information processing facilities cover all relevant security requirements.</p> <p>Contracts between business associates and covered entities address administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of information. [RCM002]</p> <ul style="list-style-type: none"> - Controls should be in place to help monitor any access by third parties. This can include the regular review of VPN logs, EHR logs, server logs, etc. - Automated alerts when certain criteria is met within a system can greatly help monitor third party connections to internal systems. 		0				
Risk Management & Compliance	Information around risks and related control options are not presented to management before management decisions are made. [TVS004]	<p>Risk assessments are conducted to identify, quantify, prioritize and manage risks. The prioritization is accomplished by creating and using criteria for risk acceptance and objectives which are important to the organization. [RCM004]</p> <ul style="list-style-type: none"> - It is important to expand upon this risk assessment by assessing the risk of each asset itself. 	- No regular assessments of technology is performed; including vulnerability testing, patch management, or other review of systems to help determine risks associated with them so appropriate action(s) can be taken.					

GENERAL AUDIT PREPARATION – Risk Analysis

FINDINGS-REMEDIATION

Number of High Risks	0					
Number of Medium Risks	0					
Total Number of High and Medium Risks	0					
High and Medium Risks Findings and Remediation						
Risks Found (High and Medium Only)	Risk Rating	Existing Control Measures Applied	Recommended Control Measures	Owner	Remediation Steps	Target Date
People and Processes						
Technology						

GENERAL AUDIT PREPARATION

RISK MANAGEMENT PLAN!

- **What is a Risk Management Plan (RMP)?**
- **Why is a RMP necessary?**
- **Who is responsible for the RMP?**
- **When should the RMP be developed/updated?**
- **Where should RMP reside?**
- **How should the RMP be used?**

GENERAL AUDIT PREPARATION

- Resources – HHS Security Rule Educational Paper Series
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>



Security Topics

1. Security 101 for Covered Entities

2.

6 Basics of Risk Analysis and Risk Management

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The

GENERAL AUDIT PREPARATION

AUDIT RESPONSE PLAN!

- **Why is an Audit Response Plan (ARP) necessary?**
- **Who is responsible & involved in the ARP?**
- **What are the duties and responsibilities of ARP?**
- **When should the ARP be developed and initiated?**
- **Where should ARP reside?**
- **How should the ARP be used?**

SPECIFIC AUDIT PREPARATION

- **MU Audit**



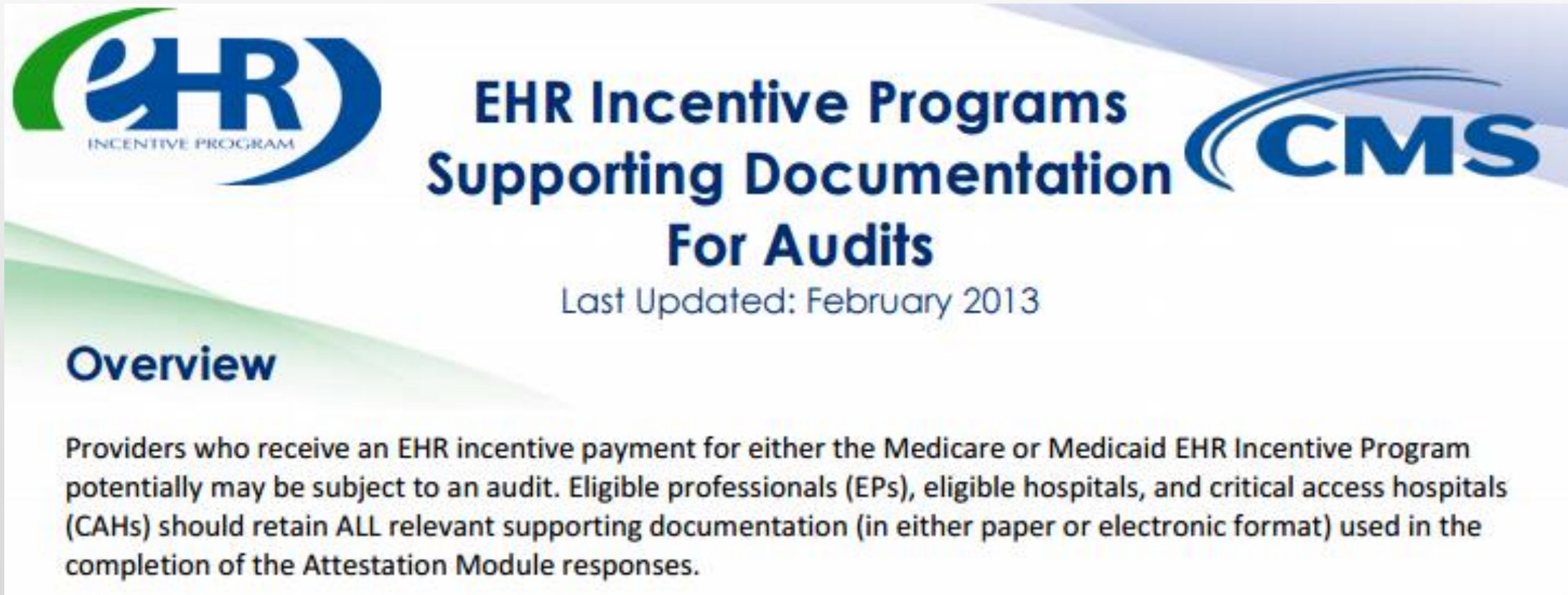
- **HIPAA Audit**

SPECIFIC AUDIT PREPARATION – MU Audit Prep

- **Program selection and eligibility requirements**
- **Ensure EHR certification – Certified Health IT Product List (CHPL)**
- **MU Core/Menu Objectives and Measures**
 - **Numerator/Denominator measures**
 - **Yes/No objective response**
 - **Exclusion response**

SPECIFIC AUDIT PREPARATION – MU Audit Prep

- **Resources – CMS EHR Supporting Documentation for Audits**



The image shows the cover of a document titled "EHR Incentive Programs Supporting Documentation For Audits". The cover features the EHR Incentive Program logo on the left and the CMS logo on the right. The title is centered in large blue font, with the date "Last Updated: February 2013" below it. The word "Overview" is written in a smaller blue font on the left side. The main text at the bottom explains that providers who receive an EHR incentive payment for either the Medicare or Medicaid EHR Incentive Program potentially may be subject to an audit. Eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) should retain ALL relevant supporting documentation (in either paper or electronic format) used in the completion of the Attestation Module responses.

**EHR Incentive Programs
Supporting Documentation
For Audits**

Last Updated: February 2013

Overview

Providers who receive an EHR incentive payment for either the Medicare or Medicaid EHR Incentive Program potentially may be subject to an audit. Eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) should retain ALL relevant supporting documentation (in either paper or electronic format) used in the completion of the Attestation Module responses.

SPECIFIC AUDIT PREPARATION – MU Audit Prep

▪ Resources – CMS EHR Supporting Documentation for Audits

Providers who use a source document other than a report from the certified EHR system to attest to meaningful use data (e.g., non-clinical quality measure data) should retain all documentation that demonstrates how the data was accumulated and calculated.

This primary document will be the starting point of most reviews and should include, at minimum:

- ✓ The numerators and denominators for the measures
- ✓ The time period the report covers
- ✓ Evidence to support that it was generated for that EP, eligible hospital, or CAH (e.g., identified by National Provider Identifier (NPI), CMS Certification Number (CCN), provider name, practice name, etc.)

SPECIFIC AUDIT PREPARATION – MU Audit Prep

▪ Resources – CMS EHR Supporting Documentation for Audits

Documentation for Non-Percentage-Based Objectives

In addition, not all certified EHR systems currently track compliance for non-percentage-based meaningful use objectives. These objectives typically require a “Yes” attestation in order for a provider to be successful in meeting meaningful use. To validate provider attestation for these objectives, CMS and its contractor may request additional supporting documentation. A few examples of suggested documentation are listed below. Please note that the suggested documentation does not preclude CMS or its contractor from requesting additional information to validate attestation data.

Meaningful Use Objective	Audit Validation	Suggested Documentation
Drug-Drug/Drug-Allergy Interaction Checks and Clinical Decision Support	Functionality is available, enabled, and active in the system for the duration of the EHR reporting period.	One or more screenshots from the certified EHR system that are dated during the EHR reporting period selected for attestation.
Report ambulatory or hospital clinical quality measures	Clinical quality measure data is reported directly from certified EHR systems.	Report from the certified EHR system to validate all clinical quality measure data entered during attestation.

SPECIFIC AUDIT PREPARATION – MU Audit Prep

- **Resources – CMS EHR Supporting Documentation for Audits**

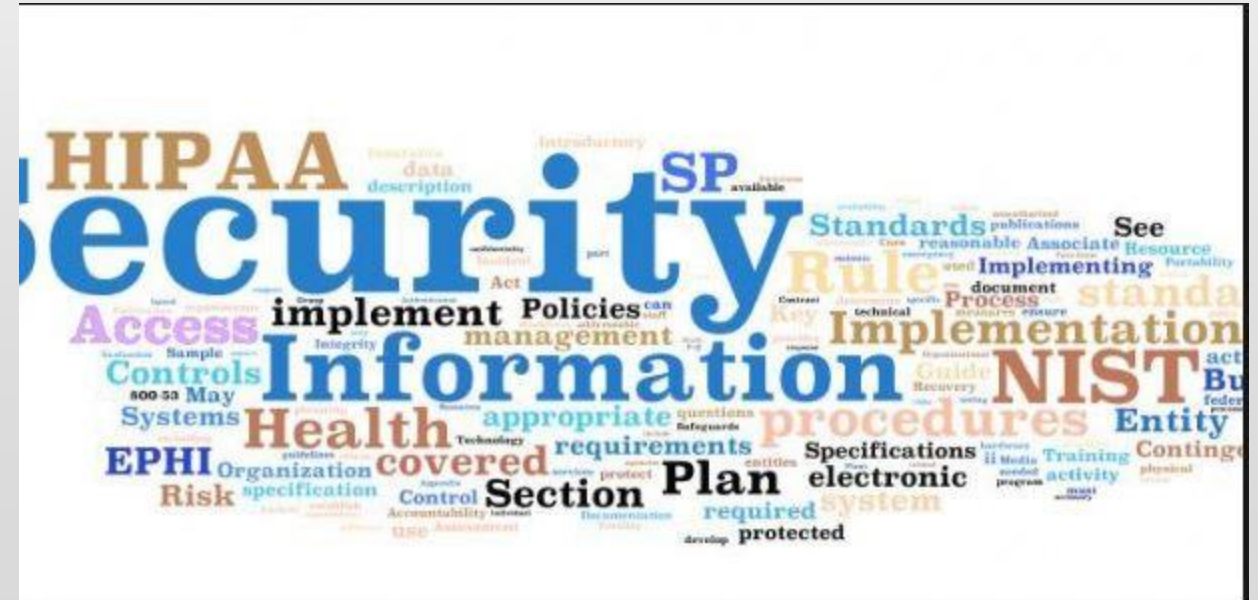
		failure of receipt) of the submitted data, including the date of the submission, name of parties involved, and whether the test was successful.
Exclusions	Documentation to support each exclusion to a measure claimed by the provider.	Report from the certified EHR system that shows a zero denominator for the measure or otherwise documents that the provider qualifies for the exclusion.

SPECIFIC AUDIT PREPARATION – HIPAA Audit Prep

- **OCR HIPAA Audit Pilot Program**
 - **Phase I (2011 – 2012)**
 - **Phase II (2015 ?)**
- **HIPAA Privacy Rule**
- **HIPAA Security Rule**
 - **Administrative, Physical and Technical safeguards**
 - **Organizational, Policies & Procedures, Documentation**
- **Omnibus Rule Sept 23, 2013**

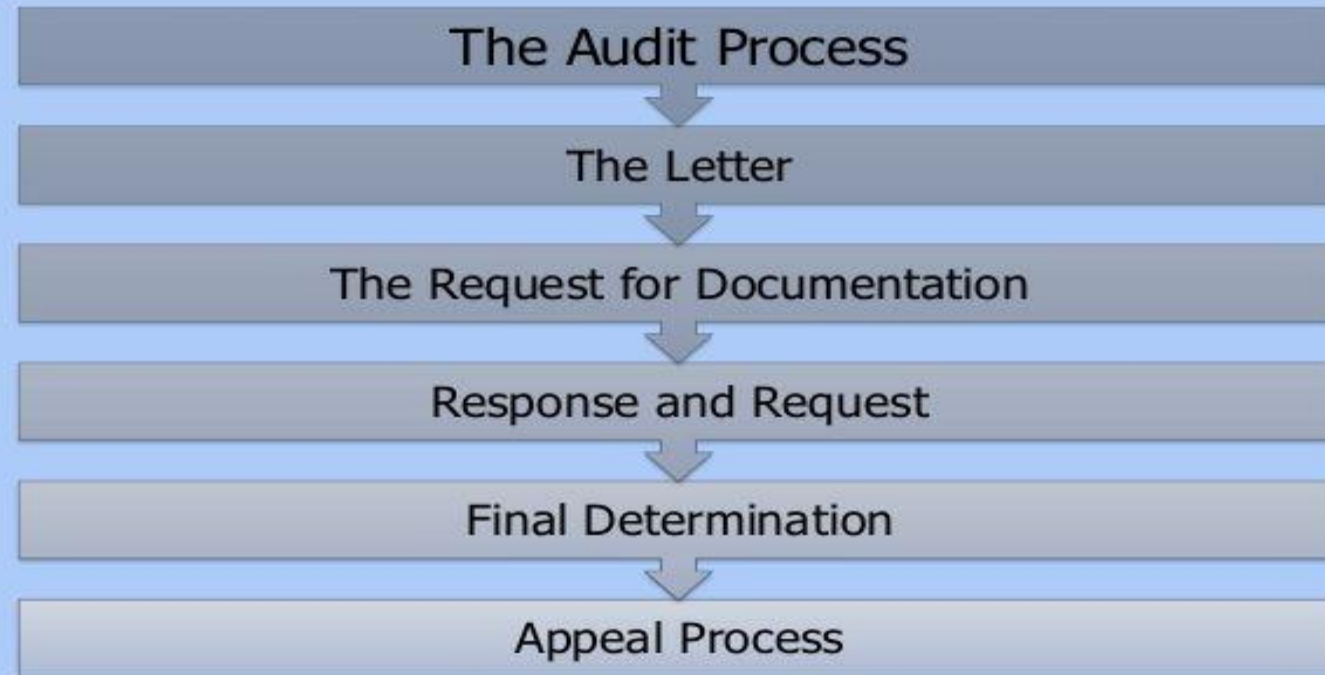
SPECIFIC AUDIT PREPARATION – HIPAA Audit Prep

- **HIPAA Security Rule – Organizational, Policies & Procedures, Documentation**
- **Business Associate Contracts or other Arrangements**
- **Policies and Procedures**
- **Documentation**
 - **Time Limit**
 - **Availability**
 - **Updates**

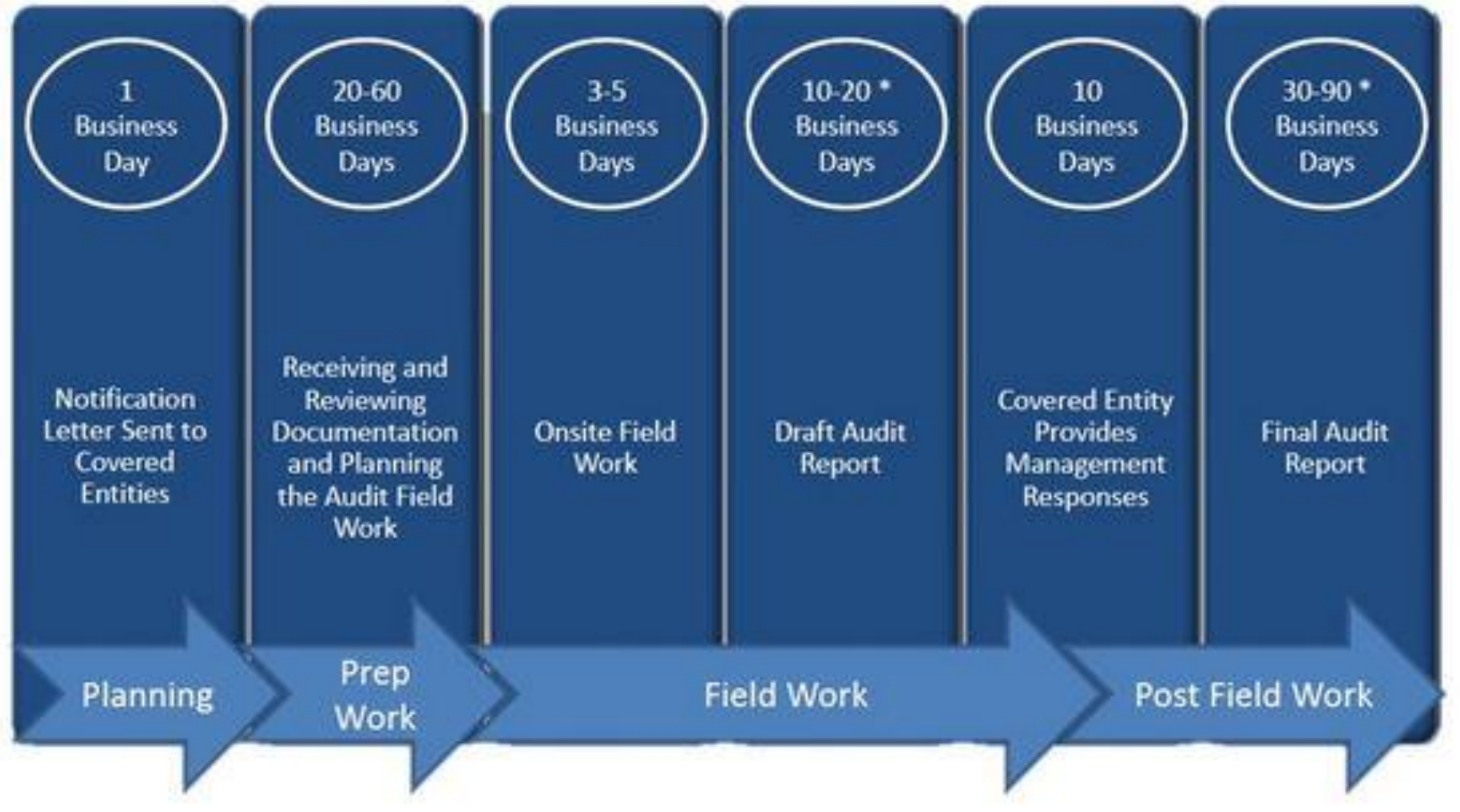


AUDIT PROCESS - MU

Audit Program Process



AUDIT PROCESS - HIPAA



RECAP - GENERAL AUDIT PREPARATION

- **Assume you will be Audited**
- **Create a Regulatory Binder**
- **Perform a Risk Analysis**
- **Develop and Execute a Risk Management Plan**
- **Formulate an Audit Response Plan**

WHY SHOULD I DO THIS?

- **Income verse Expense**
- **Heighten assurance, e.g. Insurance Policy**
- **Ensure receipt of MU stimulus funds**
- **Evade additional MU audits**
- **Avoid HIPAA fines and penalties**
- **Escape damaged professional reputation**

CONCLUSION

Questions?

HEALTHCARE COMPLIANCE



Debra Billeaud, CISA, CISM

337.849.6354

Debra@BilleaudTechnology.com

Your Healthcare Compliance Resource