Cooking Up HIPAA Compliance

with

Compliancy Group

Table of Contents

The Six Annual Audits

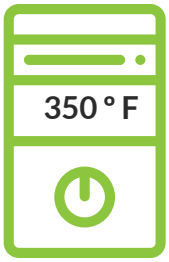
Prep: *Organizations working in healthcare cook-up six self-audits* ***annually,*** *five for business associates. Self-audits are meant to analyze an organization's privacy and security practices to ensure that they adhere to HIPAA standards.*

Ingredients

Required Annually

- Security Risk Assessment (SRA)
- Security Standards Audit
- HITECH Subtitle D Audit
- Asset and Device Audit
- Physical Site Audit
- Privacy Assessment

1. Preheat the Security Risk Assessment (SRA) - Determine gaps, allowing remediation plans to be created to close gaps.



2. Pour in the Security Standards Audit - A required ingredient for security policies.

3. Sprinkle in the HITECH Subtitle D Audit - This ensures that documentation and procedures are in line with HIPAA breach notification requirements.

The Six Annual Audits Continued...

Ingredients

Required Annually

- Security Risk Assessment (SRA)
- Security Standards Audit
- HITECH Subtitle D Audit
- Asset and Device Audit
- Physical Site Audit
- Privacy Assessment

4. Blend in the Asset and Device Audit -

This requires organizations to create a list of all of the devices that access electronic protected health information (ePHI). The device list should include who uses the device and what protections are in place securing the device.

5. Heat up the Physical Site Audit -

Necessary ingredients for secure physical locations are utilizing alarm systems, cameras, and keypad locks, for example.

6. Mix in the Privacy Assessment - (not required for BAs)-

This assesses an organization's privacy policies, ensuring that PHI use and disclosure is in line with HIPAA standards.

Gap Identification & Remediation

PREP: *By baking your self-audits, you identify your organization's gaps in protecting PHI. A remediation plan is meant to address those gaps by creating a plan to fix issues.*

Ingredients

Required Annually

- Remediation plans

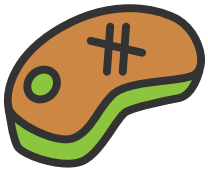
1. Once you've put your audits into the oven, you can begin to **cook** those gaps.

2. Remediation plans should be opened for each gap that your audits have uncovered.

3. **In one big bowl**, stir in your fully documented remediation plans with limited role-based access depending on parties involved.

4. Each remediation plan must assign responsibility to someone on your staff to fix the gap, along with action items and a timeline for completion.

5. As your organization **cooks each gap,** you must document the process until all gaps are closed.

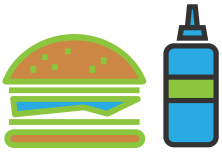


Policies, Procedures, & Training

PREP: *Policies and procedures are the key ingredient for creating an effective HIPAA compliance program. These must be created for an organization's specific needs. An old or bought employee manual will not suffice when it comes to HIPAA compliance.*

Ingredients

- Policies and Procedures
- Training



Required Annually

1. Organizations are required to have policies and procedures in place that address each HIPAA standard.

2. **Plate** those uniform processes across all parts of your organization for handling PHI.

3. Your policies and procedures **must be cooked** to the needs of your organization.

4. If the policies do not apply to the scope of your business, they will not protect you in the event of a HIPAA violation.

Policies, Procedures, & Training Continued...

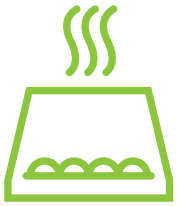
Ingredients

Required Annually

- Policies and Procedures
- Training

5. Once your organization has plated **it's HIPAA policies and procedures,** you must ensure that all employees have been trained.

6. Your organization must have all employees sign an attestation saying they have read and understood each policy.



7. These attestations **should be set to protect your organization** from liability in the event that an employee causes a HIPAA violation.

8. Employee training **MUST be cooked annually.**

9. Any new employees must be trained on policies and procedures as part of their on-boarding process.

Business Associate Agreements

Prep: *Organizations working in healthcare must vet their vendors and secure business associate agreements (BAAs). A BAA must be executed before PHI can be shared between the parties. A BAA also ensures that each party is HIPAA compliant.*

Required Annually

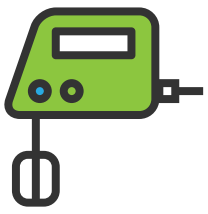
Ingredients

- Business Associate (BA)
- Covered Entity (CE)
- Vendor Questionnaire

1. Before hiring a BA, healthcare entities must vet the BAs security measures to ensure that the PHI is protected.

2. CEs are responsible for **cooking on their own as well.** They must ensure that their BAs are HIPAA compliant before working with them.

3. You are required to send vendor questionnaires to the BA to assess their practices so that security gaps may be identified.



4. It is suggested that healthcare entities require BAs to **whip up remediation plans** to address identified gaps before any PHI is shared with them.

Business Associate Agreements Continued...

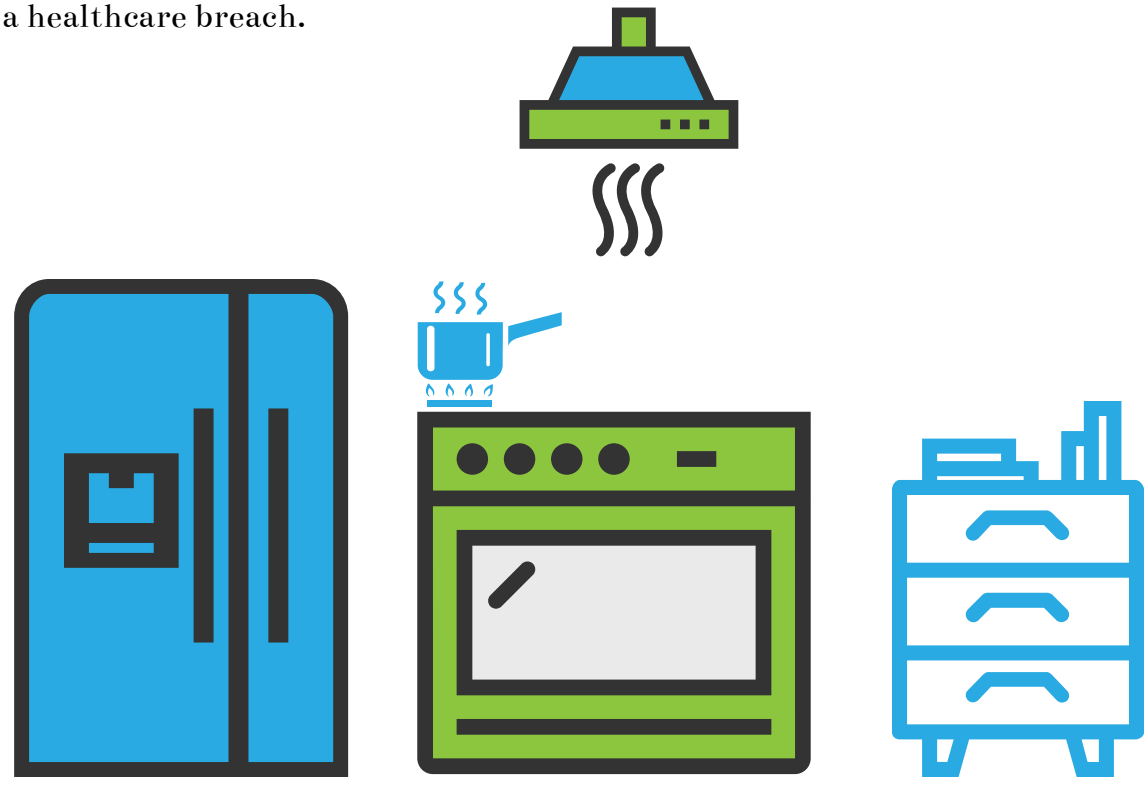
Ingredients

- Business Associate
- Covered Entity
- Vendor Questionnaire

Required Annually

6. By **cooking this for both parties,** it states that each agrees to be HIPAA compliant, and they are both responsible for their own compliance.

7. **Without this BAA recipe,** both parties will be held liable in the event of a healthcare breach.

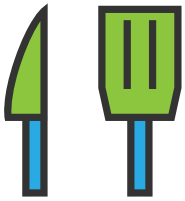


Incident Management

PREP: *Even with a totally effective HIPAA compliance program in place, data breaches can still occur. In that event, your organization should have processes in place to document, track, and report the breach if necessary.*

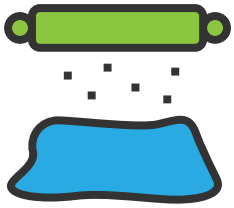
Ingredients

- Minor Breaches
- Meaningful Breaches



Required Annually

1. The HIPAA Breach Notification Rule requires organizations to report breaches to the Department of Health and Human Services (HHS) as well as affected individuals.



2. When organizations experience a Minor Breach (affecting less than 500 individuals), they have until the end of the calendar year to report the incident; they do not have to report the incident to the media.

3. In the case of a Meaningful Breach (affecting more than 500 individuals), organizations must report the incident within 60 days of the discovery to HHS and the media.

4. In the event of a data breach, OCR may open an investigation into your practice.

Thanks for Cooking HIPAA with

Compliancy Group

We hope you enjoyed the recipe book! At Compliancy Group, we strive to give you all the information needed to understand and tackle HIPAA compliance. If HIPAA is still confusing or overwhelming for you to handle on your own, we're here to help. Our software includes all aspects discussed in the recipes to automate/track each piece of compliance. If that didn't simplify it enough, we include a compliance coach to walk you through the regulation, taking all the guesswork, scariness, and uncertainty out of the equation.

Learn More!