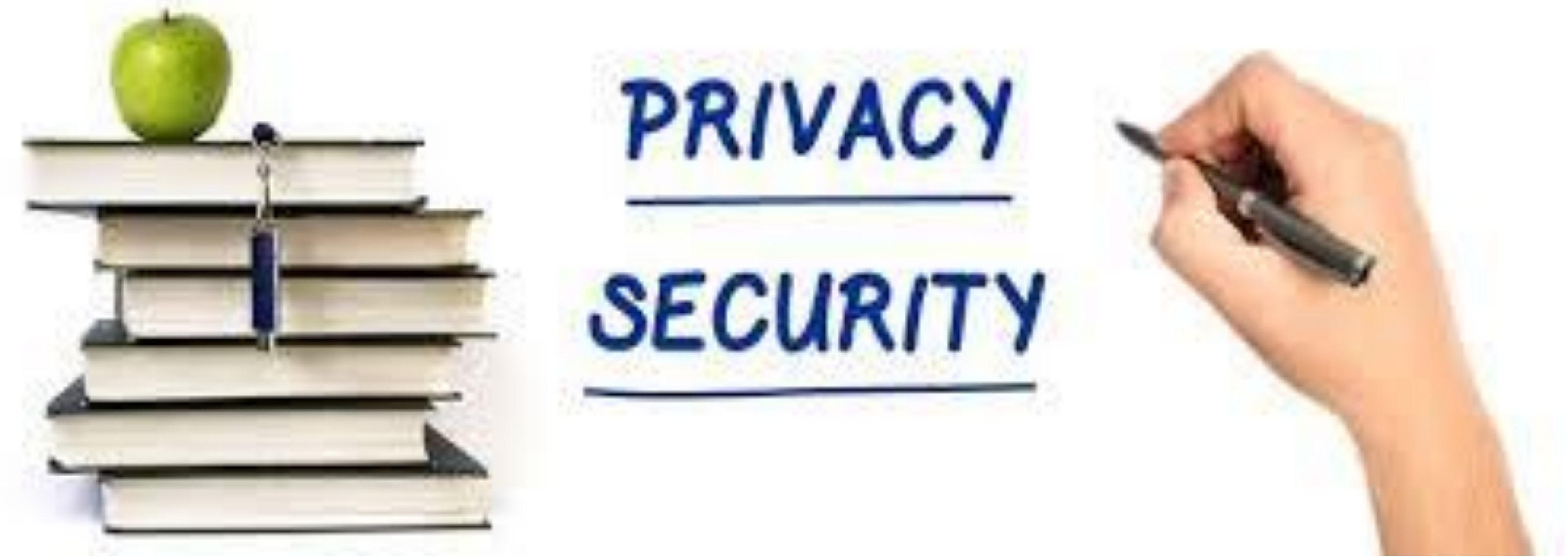


# Increasing Security Literacy: Supporting Your Staff in Understanding their Role in HIPAA HITECH Compliance

NHCHC May 7, 2015

Washington DC

# HIPAA Guidance Can Be Overwhelming

Integrity

Risk Assessment

HIPAA Privacy

Confidentiality

Risk Management

Breach Notification

Mobile Media

Access Control

Availability

Contingency Planning

Encryption

Business Associates

Authentication

Patient Access

Disaster Recovery

Fines

Audits

# What is the greatest risk?

*"No, it's not a female Hippopotamus, anyone else know?"*

75% of organizations say the greatest risk to security and privacy of patient information is employee negligence.

# Phishing season

1,981 patients were recently affected when their data was compromised by providers responding to phishing e-mails.

# Policies and procedures not enough

Without proper training, policies and procedures are just a stack of documents.

To be effective, you must provide staff with proper training and awareness programs appropriate to their role and responsibilities.

# Who, when, How?

## Who

- Employees (full-time, part-time, temp) with access to PHI (electronic or paper)

## When

- Onboarding new employees
- Supplemental training throughout the year (targeted reminders, or new job duty, new policy, new procedure, new technology, a security incident )
- Annual review of general HIPAA concepts

## How

- Onsite – classroom training
- Virtual – elearning (videos, interactive online training software, kiosk)
- Email, posters, flyers

QiP Security and Privacy Solutions for the Healthcare Industry

# Creating a Culture of Privacy and Security

✓ Prioritize culture of awareness of privacy and security within the organization

✓ Accountability and responsibility core value

✓ Commitment to personnel and training

✓ Implementation of structured simple resource tools

# Blueprint for Building a HIPAA Privacy and Security Compliant Practice

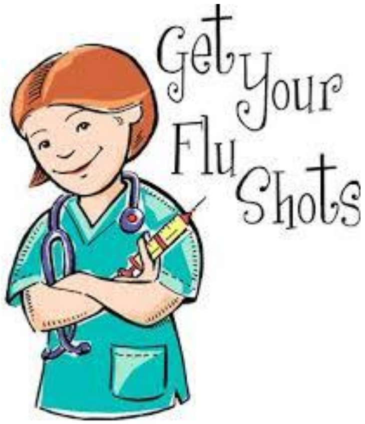
- ✓ Engaged Leadership
- ✓ Strategic risk management planning
- ✓ Process Improvement
- ✓ Workforce Training
- ✓ Communication- Patient Engagement

# Ensuring Full Compliance with Federal, State and Local Regulations

# The Skills I Acquired as a Fed Transferred to the World of Corporate Compliance

# Since 1985

PHMC's Health Care for the Homeless Program has been providing health care and social services to the homeless population.

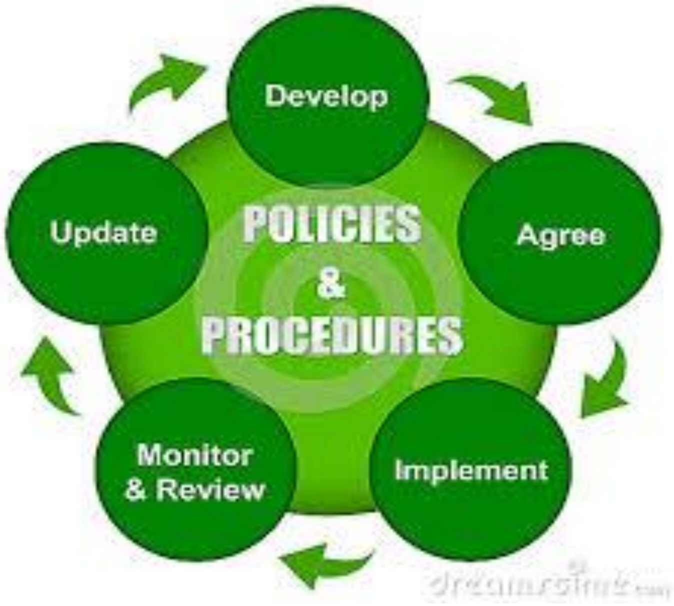


# OMG!!!!!!
# What Did I Get Myself Into?????

- I hit the ground running!!!!!
- What’s encryption?
- BA and covered entities….explain that again…..for the 5th time!!
- ePHI…..what’s that and why is the “e” lower-cased?
- Minimum Necessary….for whom does this apply?
- HIPAA HITECH….I never heard of that company before!

# What Am I Saying…..
# That You Don’t Understand????

# Policies & Procedures



# Embrace Information Technology

- Encryption
- Configuration
- Local Networks
- Decommission Process
- VPN (Virtual Private Network)
- Firewalls

This was me

# Help Is On The Way!!!!!!

This is QI Partners

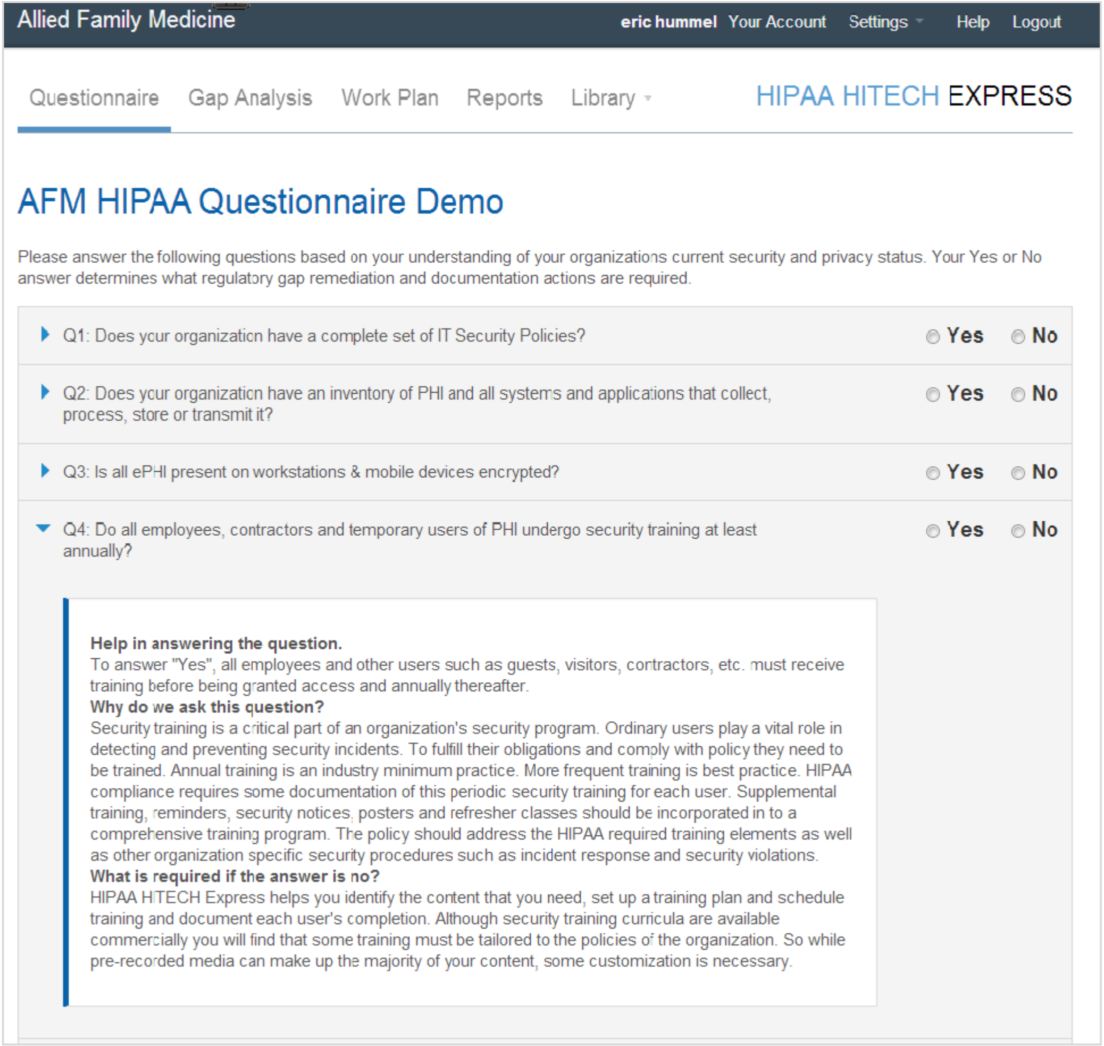
# HIPAA HITECH EXPRESS

- ✓ Helps to store, organize and track security documentation in one place
- ✓ Helps create a schedule for periodic review of policies and procedures and identify when they are missing, out-of-date or ineffective.
- ✓ Helps implement policies and procedures to prevent, detect, contain, and correct security violations.

© Can Stock Photo - csp20619984

# Rapid Risk Analysis: Quick How Am I Doing Diagnostic

- Guided Questions
- Yes/No only. No ambiguity!
- Built-in help, integrated training
- Quickly move from Assessment to Action


Allied Family Medicine
eric hummel Your Account Settings Help Logout
Questionnaire Gap Analysis Work Plan Reports Library
HIPAA HITECH EXPRESS

## AFM HIPAA Questionnaire Demo

Please answer the following questions based on your understanding of your organizations current security and privacy status. Your Yes or No answer determines what regulatory gap remediation and documentation actions are required.

▸ Q1: Does your organization have a complete set of IT Security Policies? ○ Yes ○ No

▸ Q2: Does your organization have an inventory of PHI and all systems and applications that collect, process, store or transmit it? ○ Yes ○ No

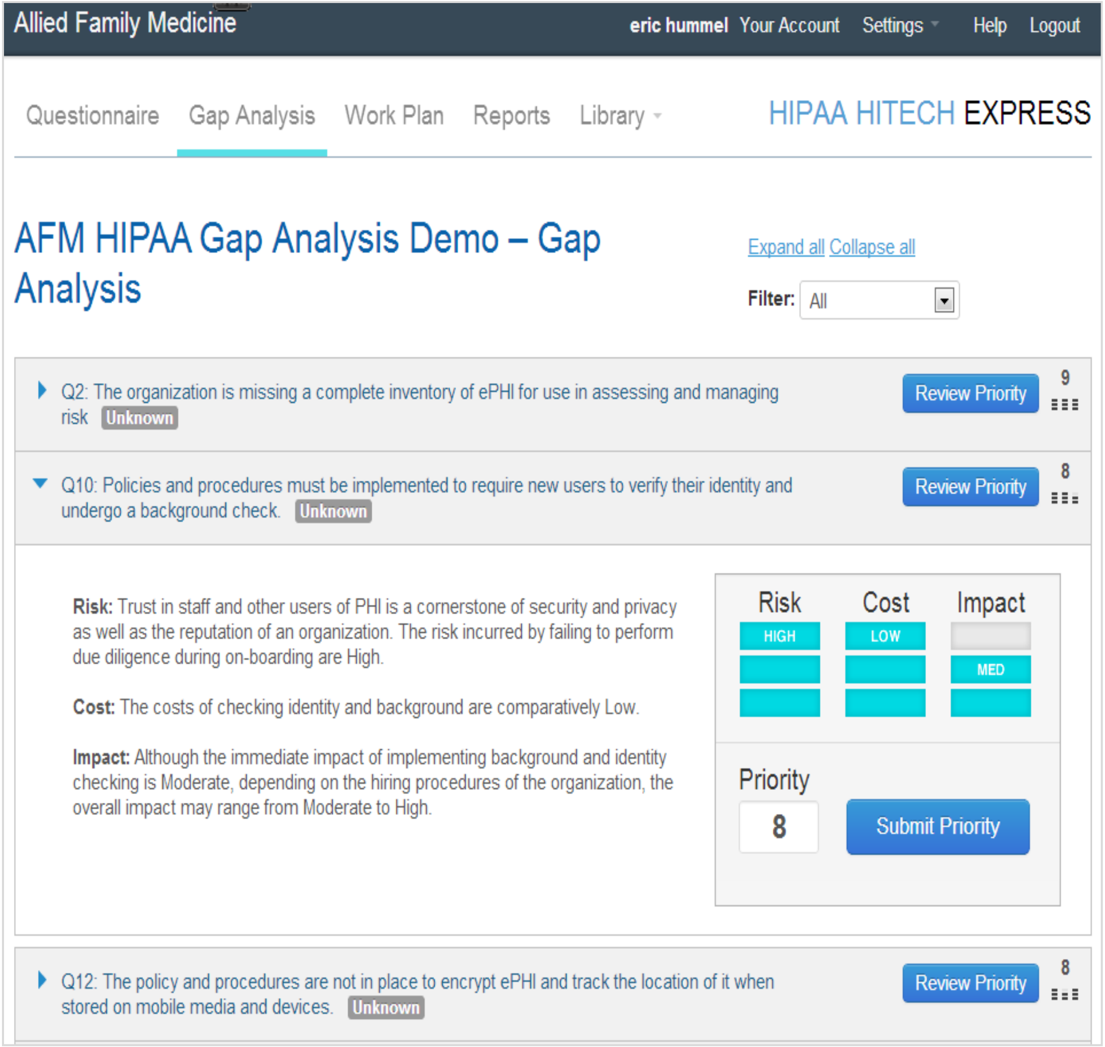
▸ Q3: Is all ePHI present on workstations & mobile devices encrypted? ○ Yes ○ No

▾ Q4: Do all employees, contractors and temporary users of PHI undergo security training at least annually? ○ Yes ○ No

**Help in answering the question.**
To answer "Yes", all employees and other users such as guests, visitors, contractors, etc. must receive training before being granted access and annually thereafter.
**Why do we ask this question?**
Security training is a critical part of an organization's security program. Ordinary users play a vital role in detecting and preventing security incidents. To fulfill their obligations and comply with policy they need to be trained. Annual training is an industry minimum practice. More frequent training is best practice. HIPAA compliance requires some documentation of this periodic security training for each user. Supplemental training, reminders, security notices, posters and refresher classes should be incorporated in to a comprehensive training program. The policy should address the HIPAA required training elements as well as other organization specific security procedures such as incident response and security violations.
**What is required if the answer is no?**
HIPAA HITECH Express helps you identify the content that you need, set up a training plan and schedule training and document each user's completion. Although security training curricula are available commercially you will find that some training must be tailored to the policies of the organization. So while pre-recorded media can make up the majority of your content, some customization is necessary.

# Gap Analysis: Prioritize Risks to Focus on What's Important

- Expert-guided
- Priority based on Risk, Cost and Impact
- Built-in help, integrated training
- Accommodates varying organizational Goals and Objectives


Allied Family Medicine
eric hummel Your Account Settings Help Logout
Questionnaire Gap Analysis Work Plan Reports Library
HIPAA HITECH EXPRESS
Expand all Collapse all
Filter: All

AFM HIPAA Gap Analysis Demo – Gap Analysis

Q2: The organization is missing a complete inventory of ePHI for use in assessing and managing risk Unknown

Q10: Policies and procedures must be implemented to require new users to verify their identity and undergo a background check. Unknown

**Risk:** Trust in staff and other users of PHI is a cornerstone of security and privacy as well as the reputation of an organization. The risk incurred by failing to perform due diligence during on-boarding are High.

**Cost:** The costs of checking identity and background are comparatively Low.

**Impact:** Although the immediate impact of implementing background and identity checking is Moderate, depending on the hiring procedures of the organization, the overall impact may range from Moderate to High.

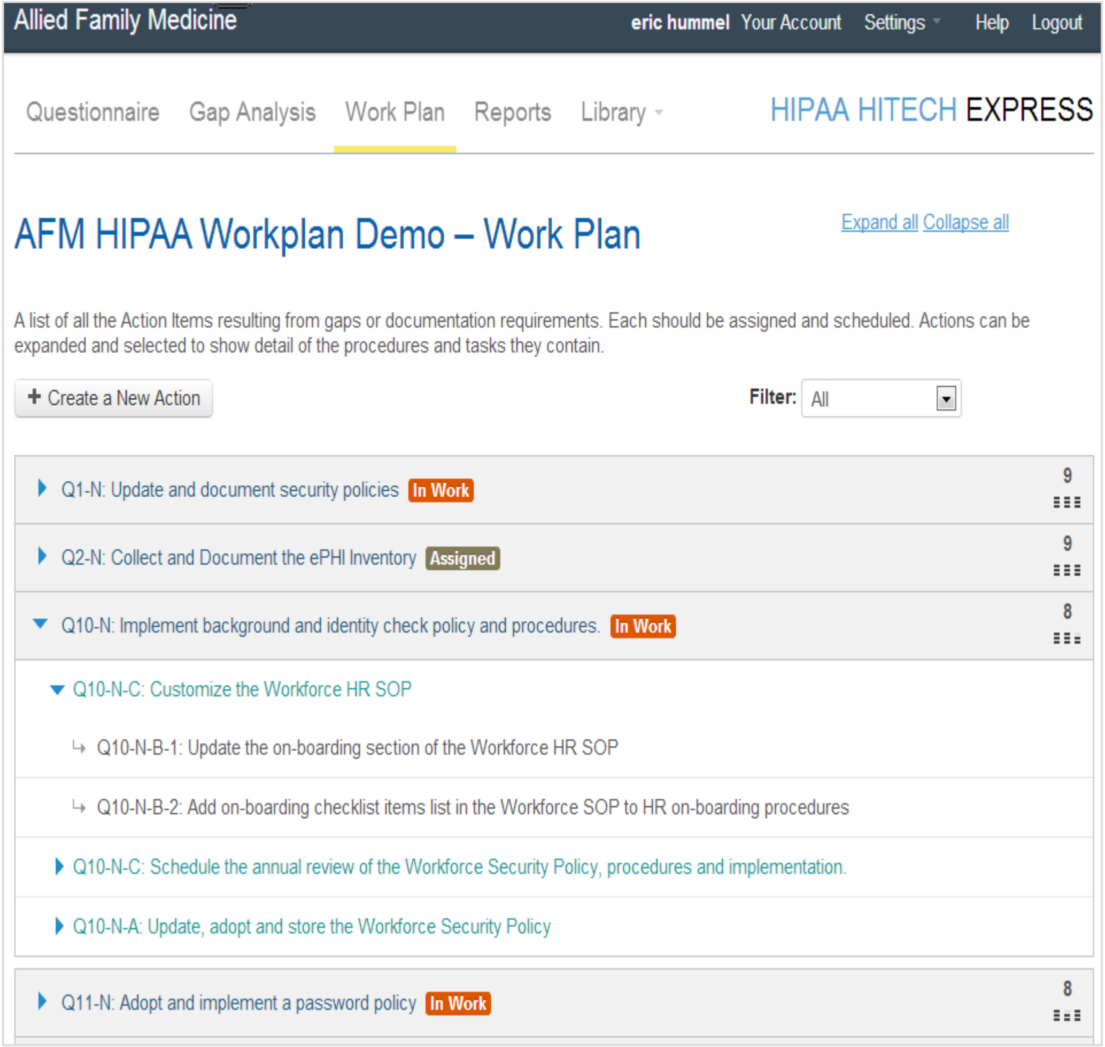
| Risk | Cost | Impact |
|---|---|---|
| HIGH | LOW | MED |

Priority: 8

Q12: The policy and procedures are not in place to encrypt ePHI and track the location of it when stored on mobile media and devices. Unknown

# Rapid Risk Remediation: Mitigate Risks and Develop Required Documentation

- Detailed Task-by-Task Work plan
- Simple Workflow
- Web and email integration
- Task ownership and scheduling
- Self-documenting



## AFM HIPAA Workplan Demo – Work Plan

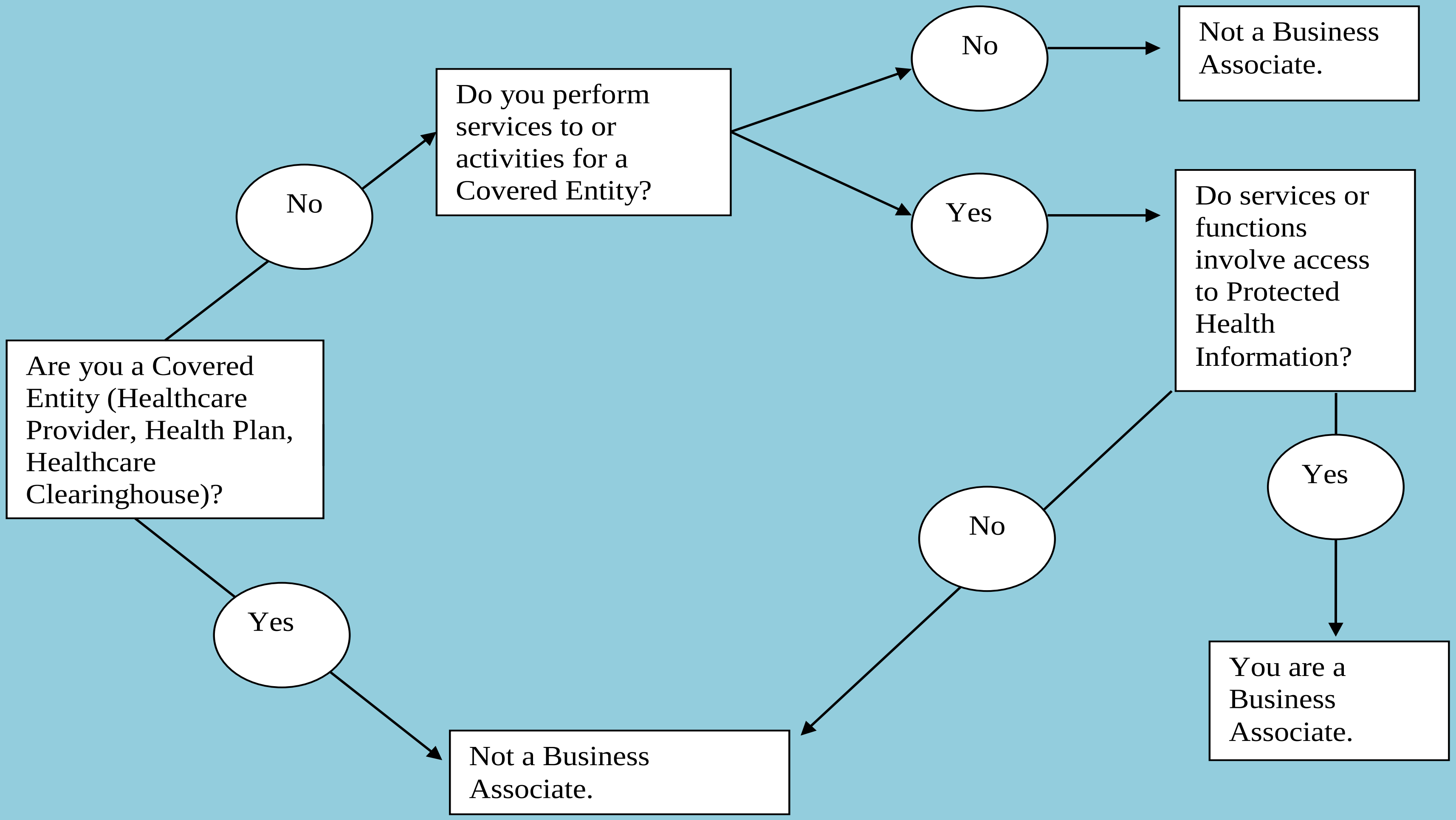
A list of all the Action Items resulting from gaps or documentation requirements. Each should be assigned and scheduled. Actions can be expanded and selected to show detail of the procedures and tasks they contain.

- Q1-N: Update and document security policies In Work — 9
- Q2-N: Collect and Document the ePHI Inventory Assigned — 9
- Q10-N: Implement background and identity check policy and procedures. In Work — 8
  - Q10-N-C: Customize the Workforce HR SOP
    - ↳ Q10-N-B-1: Update the on-boarding section of the Workforce HR SOP
    - ↳ Q10-N-B-2: Add on-boarding checklist items list in the Workforce SOP to HR on-boarding procedures
  - Q10-N-C: Schedule the annual review of the Workforce Security Policy, procedures and implementation.
  - Q10-N-A: Update, adopt and store the Workforce Security Policy
- Q11-N: Adopt and implement a password policy In Work — 8

# Who are Business Associates?

| Healthcare Entity | Business Associate | Comment |
|---|---|---|
| Claims Clearinghouse | no | Covered entity |
| Hospital Systems | no | Covered entity |
| Health Information Exchange | yes | |
| IT Service Provider | yes | |
| Reference lab | no | Covered entity |
| Radiology Service Provider | no | Covered entity |
| Referring/Referred to Provider (any specialty) | no | Covered Entity |
| Answering Service | yes | |
| Commercial Insurer | No/Yes | Covered Entity/if adm self-insured benefit plan |
| Lawyer | yes | If litigating patient cases |
| Accounting Firm | yes | If reviewing/managing claims data |
| Off-site Med Records Storage Facility | yes | |
| Housekeeping Service | no | Incidental contact with PHI |

# Who ??



Are you a Covered Entity (Healthcare Provider, Health Plan, Healthcare Clearinghouse)?

Yes

Not a Business Associate.

No

Do you perform services to or activities for a Covered Entity?

No

Not a Business Associate.

Yes

Do services or functions involve access to Protected Health Information?

Yes

You are a Business Associate.

No

Not a Business Associate.

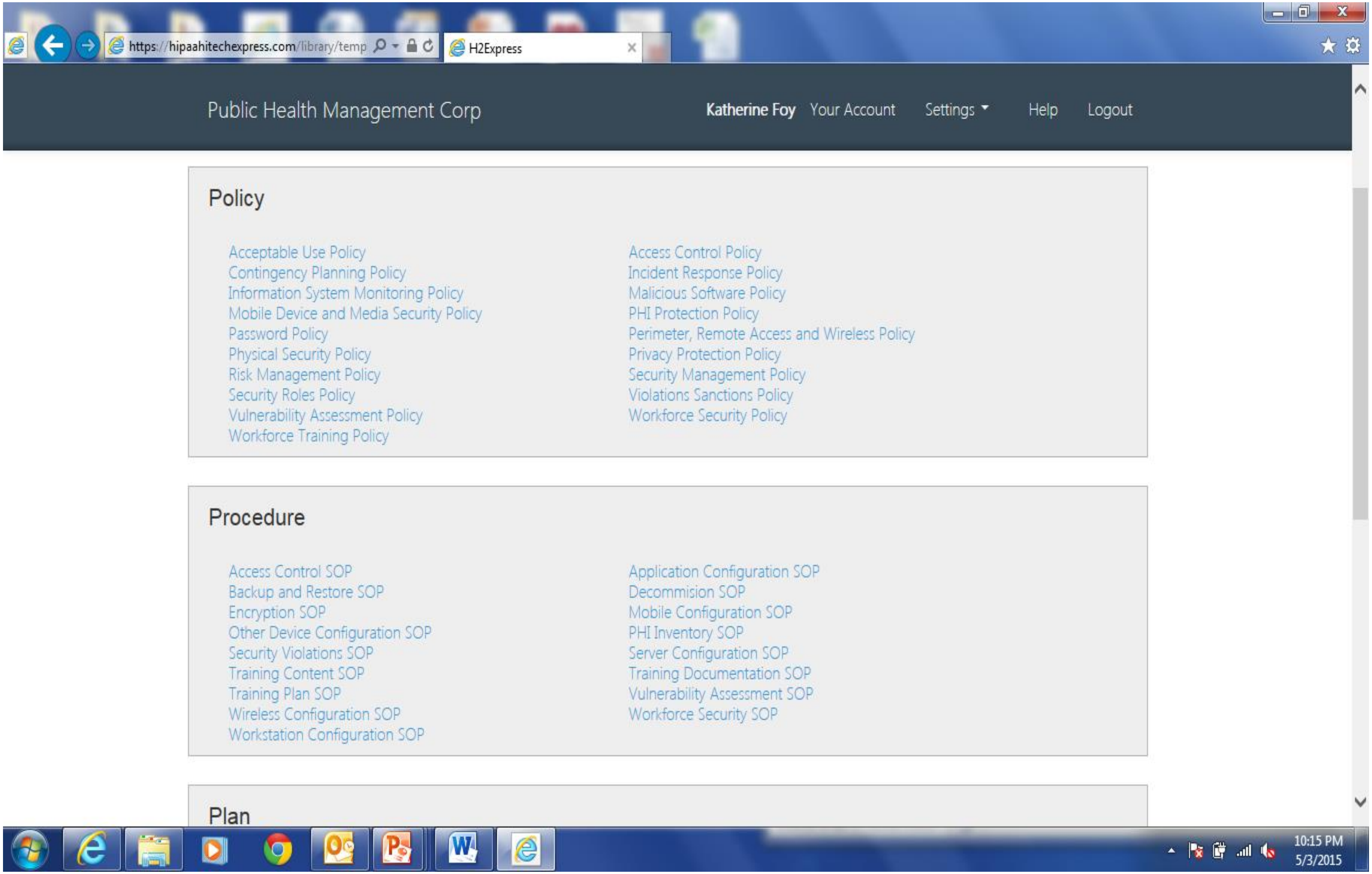
# The Ten BAA Essentials

1. Establish Permitted Uses and Disclosures.
2. State BA will not use or disclose PHI for reasons not permitted or required.
3. Require BA implement HIPAA safeguards to prevent unauthorized use or disclosure.
4. Require BA to report to CE unauthorized use or disclosure.
5. Require BA to disclose PHI to satisfy CE's obligation to provide individuals access to their PHI, for amendments,
6. Require BA to comply with CE's Privacy Rule obligations, as agreed.
7. Require BA to make available to HHS information needed to show CE's compliance with HIPAA.
8. At the termination of the contract, require BA to return or destroy the PHI.
9. Require BAs ensure their subcontractors agree to the same provisions as the BA agreed.
10. Authorize the termination of the contract if BA violates any material term, (i.e. #'s 1-9).

# Top Risk Areas That you should CONSIDER And MITIGATE

1. Do you have a complete and up-to-date set of security and privacy policies?
2. Do you have an inventory that identifies the devices, network and software that process, store and transmit PHI?
3. Have you conducted a risk assessment in the past 12 months and acted on it?
4. Do you have business associate agreements in place with all BAs you share PHI with?
5. Do you have a Business Continuity plan in place in case of a disaster or breach?
6. Do you conduct required security and privacy awareness training?
7. Is all patient information encrypted on mobile devices?
8. Do you have a documented policy for granting, changing or terminating PHI access?
9. Have you designated one person as security officer in your organization?
10. Do you track who has been assigned/has access to mobile devices, keys and physical tokens?

# I didn't have to reinvent the wheel



Public Health Management Corp

## Policy

Acceptable Use Policy
Contingency Planning Policy
Information System Monitoring Policy
Mobile Device and Media Security Policy
Password Policy
Physical Security Policy
Risk Management Policy
Security Roles Policy
Vulnerability Assessment Policy
Workforce Training Policy

Access Control Policy
Incident Response Policy
Malicious Software Policy
PHI Protection Policy
Perimeter, Remote Access and Wireless Policy
Privacy Protection Policy
Security Management Policy
Violations Sanctions Policy
Workforce Security Policy

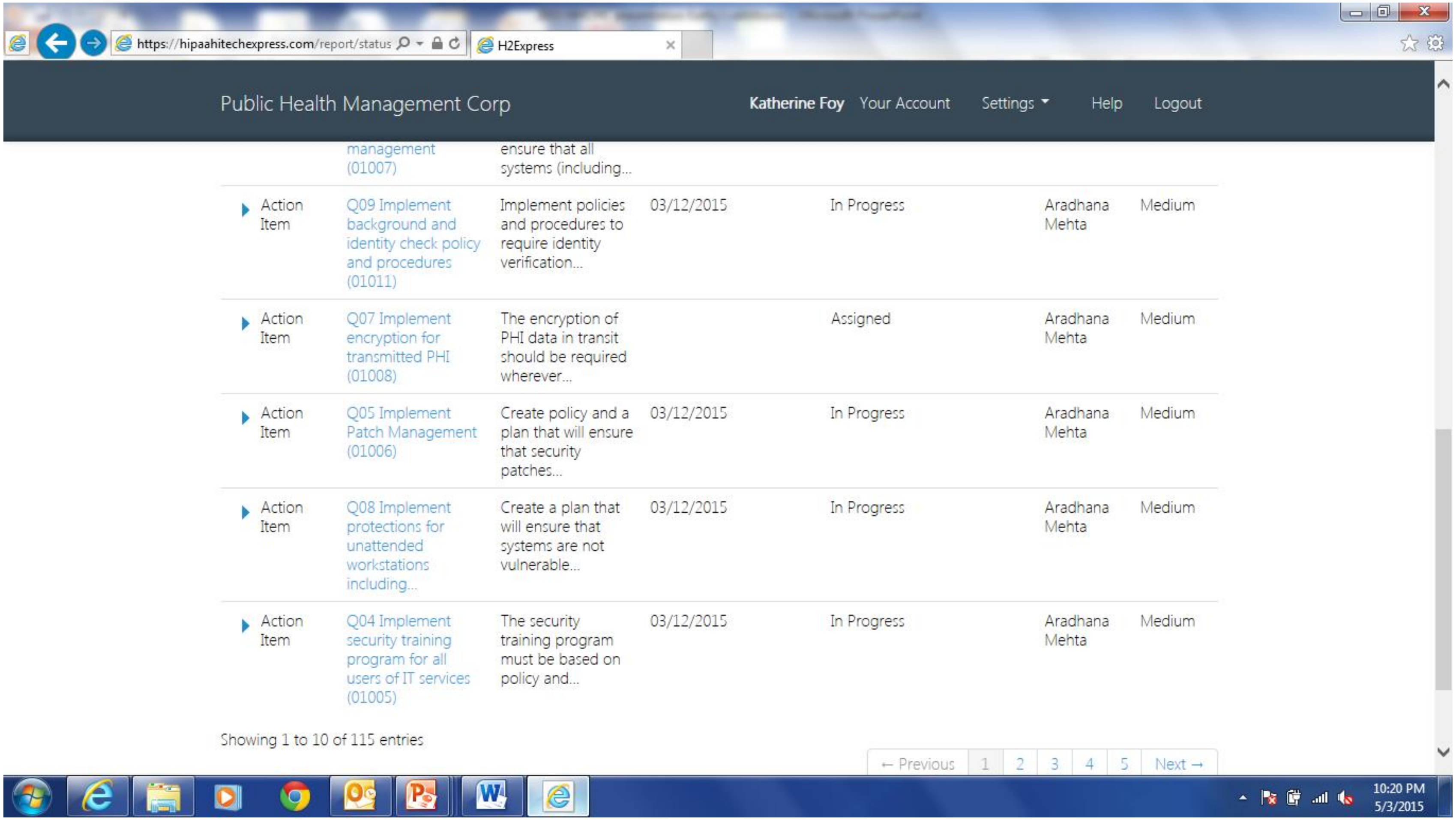
## Procedure

Access Control SOP
Backup and Restore SOP
Encryption SOP
Other Device Configuration SOP
Security Violations SOP
Training Content SOP
Training Plan SOP
Wireless Configuration SOP
Workstation Configuration SOP

Application Configuration SOP
Decommision SOP
Mobile Configuration SOP
PHI Inventory SOP
Server Configuration SOP
Training Documentation SOP
Vulnerability Assessment SOP
Workforce Security SOP

## Plan

# Security Privacy 2015
# Detail – Status Report



| | | | | | | |
|---|---|---|---|---|---|---|
| | management (01007) | ensure that all systems (including... | | | | |
| Action Item | Q09 Implement background and identity check policy and procedures (01011) | Implement policies and procedures to require identity verification... | 03/12/2015 | In Progress | Aradhana Mehta | Medium |
| Action Item | Q07 Implement encryption for transmitted PHI (01008) | The encryption of PHI data in transit should be required wherever... | | Assigned | Aradhana Mehta | Medium |
| Action Item | Q05 Implement Patch Management (01006) | Create policy and a plan that will ensure that security patches... | 03/12/2015 | In Progress | Aradhana Mehta | Medium |
| Action Item | Q08 Implement protections for unattended workstations including... | Create a plan that will ensure that systems are not vulnerable... | 03/12/2015 | In Progress | Aradhana Mehta | Medium |
| Action Item | Q04 Implement security training program for all users of IT services (01005) | The security training program must be based on policy and... | 03/12/2015 | In Progress | Aradhana Mehta | Medium |

Showing 1 to 10 of 115 entries

# Collaborations with Internal & External Partners is the Key to Successful Implementation

My new BFFs are:

- Information Technology Department
- Facilities Department
- Legal Departments
- Departmental Managers
- Volunteers
- Student Interns
- QI Partners

# Leadership Support Is Essential

© Can Stock Photo - csp18437217

# Parting Words of Wisdom

- Don’t be discouraged
- Follow the laws/regulations
- Keep abreast of policy updates on regulatory websites
- Network with fellow Compliance Directors
- Engage in professional development opportunities

# Resources

Katherine Foy, MSW

Public Health Management Corporation

Kfoy@PHMC.org

Anna Gard, FNP-BC

AMG Consulting

gardanna@gmail.com

Robert Zimmerman

Managing partner QiP Solutions

rzimmerman@qipsolutions.com

www.qipsolutions.com

Adam J. Bullian, JD

Director QIP Solutions

abullian@qipsolutions.com

QiP Security and Privacy
Solutions for the
Healthcare Industry