P4: Designing an Effective Privacy Program

David Behinfar, Chief Privacy Officer
University of North Carolina Health

Adam Greene, Partner
Davis Wright Tremaine LLP

Katherine Georger, Associate Compliance Officer
Duke University Health System

Christopher Terrell, Deputy Chief Compliance Officer & Privacy Officer
Encompass Health

David J Behinfar, JD., LLM., CHC, CHRC, CCEP, HCISPP CIPP/US

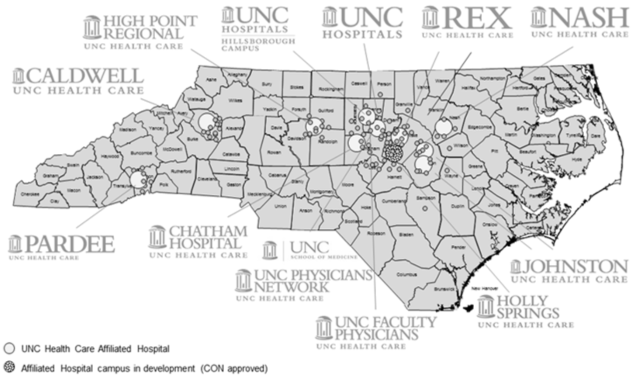
David Behinfar, JD, LLM, CHC,
CHRC, CCEP, HCISPP, CIPP/US
Chief Privacy Officer
UNC Health Care System

UNC HEALTH CARE

Integrated, not-for-profit health care system, owned by the State of North Carolina and based in Chapel Hill

Mission:

To provide comprehensive patient care, facilitate physician education and research excellence and promote the health and well-being of all North Carolinians


HIGH POINT REGIONAL UNC HEALTH CARE
UNC HOSPITALS HILLSBOROUGH CAMPUS
UNC HOSPITALS
REX UNC HEALTH CARE
NASH UNC HEALTH CARE
CALDWELL UNC HEALTH CARE
PARDEE UNC HEALTH CARE
CHATHAM HOSPITAL UNC HEALTH CARE
UNC SCHOOL OF MEDICINE
UNC PHYSICIANS NETWORK UNC HEALTH CARE
UNC FACULTY PHYSICIANS UNC HEALTH CARE
JOHNSTON UNC HEALTH CARE
HOLLY SPRINGS UNC HEALTH CARE

○ UNC Health Care Affiliated Hospital
▨ Affiliated Hospital campus in development (CON approved)
● UNC Health Care Owned or Affiliated Physician Practice

Katherine Georger, JD, CHC, CHRC, CIPP/US

Katherine Georger, JD, CHC,
CHRC, CIPP/US
Associate Compliance Officer
Duke University Health System

DukeHealth

Advancing Health Together

Duke University Health System is a world-class private, not-for profit health care network dedicated to providing outstanding patient care, educating tomorrow's health care leaders, and discovering new and better ways to treat disease through clinical and biomedical research.

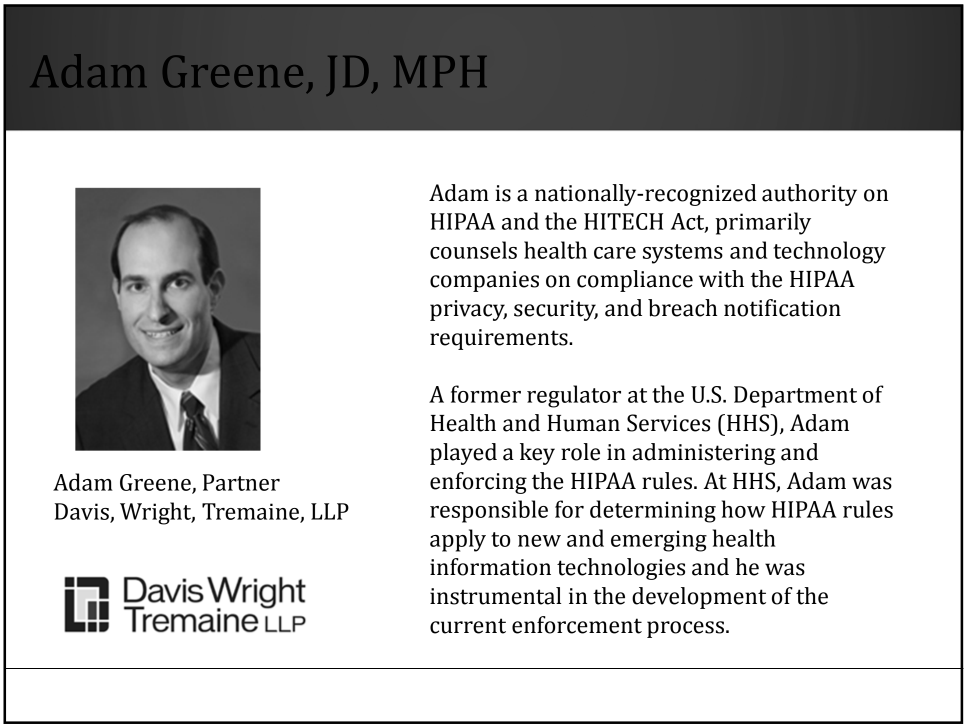
Founded in 1998 to provide efficient, responsive care, the health system offers a full network of health services and encompasses three highly regarded hospitals - Duke University Hospital, Durham Regional Hospital and Duke Raleigh Hospital - physician practices, home hospice care and various support services at locations across North Carolina.

Christopher Terrell, JD, CHC, CHPC

Encompass Health

Christopher T. Terrell, JD, CHC, CHPC
Deputy Chief Compliance Officer & Privacy Officer
Encompass Health Corporation

With a national footprint that spans 127 hospitals and 237 home health & hospice locations in 36 states and Puerto Rico, Encompass Health (NYSE: EHC) offers both facility-based and home-based patient care through its network of inpatient rehabilitation hospitals, home health agencies and hospice agencies.



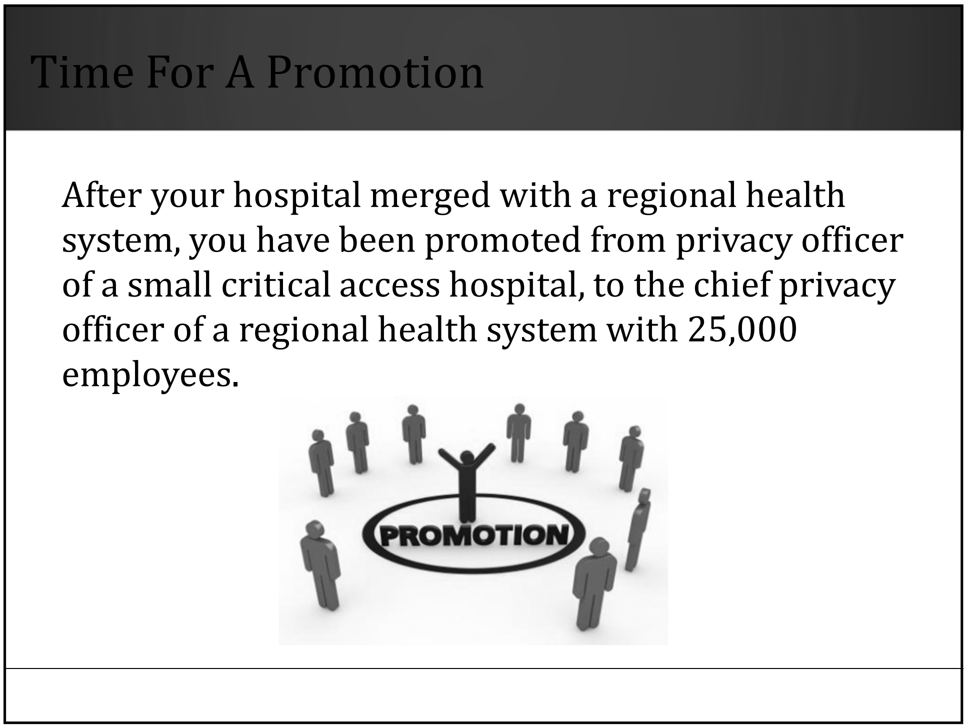
Adam Greene, JD, MPH

Adam Greene, Partner
Davis, Wright, Tremaine, LLP

Davis Wright Tremaine LLP

Adam is a nationally-recognized authority on HIPAA and the HITECH Act, primarily counsels health care systems and technology companies on compliance with the HIPAA privacy, security, and breach notification requirements.

A former regulator at the U.S. Department of Health and Human Services (HHS), Adam played a key role in administering and enforcing the HIPAA rules. At HHS, Adam was responsible for determining how HIPAA rules apply to new and emerging health information technologies and he was instrumental in the development of the current enforcement process.

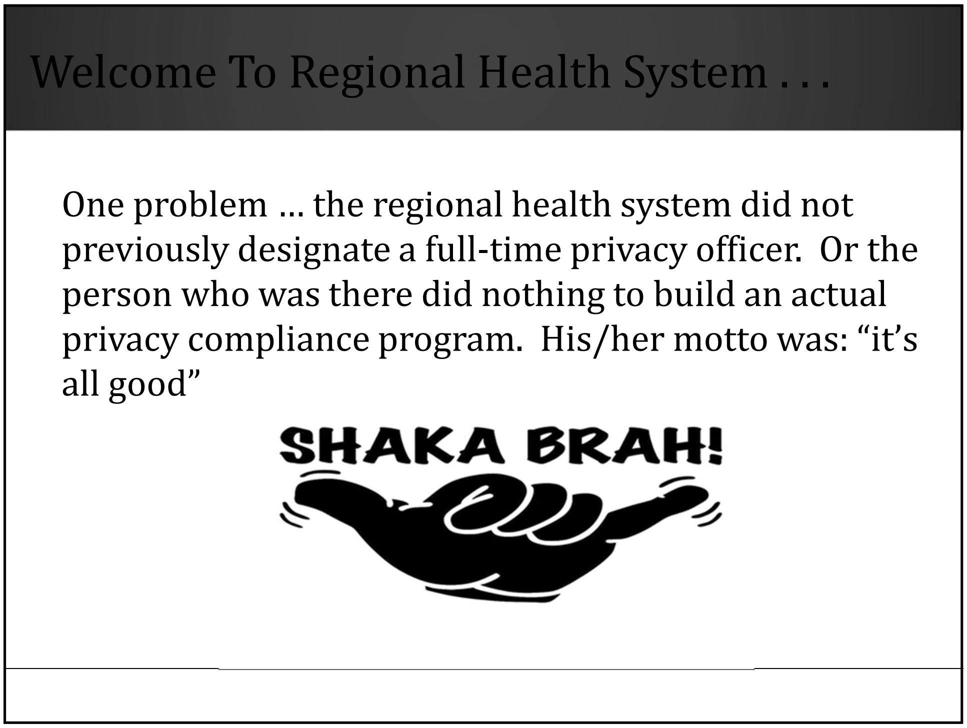


Time For A Promotion

After your hospital merged with a regional health system, you have been promoted from privacy officer of a small critical access hospital, to the chief privacy officer of a regional health system with 25,000 employees.

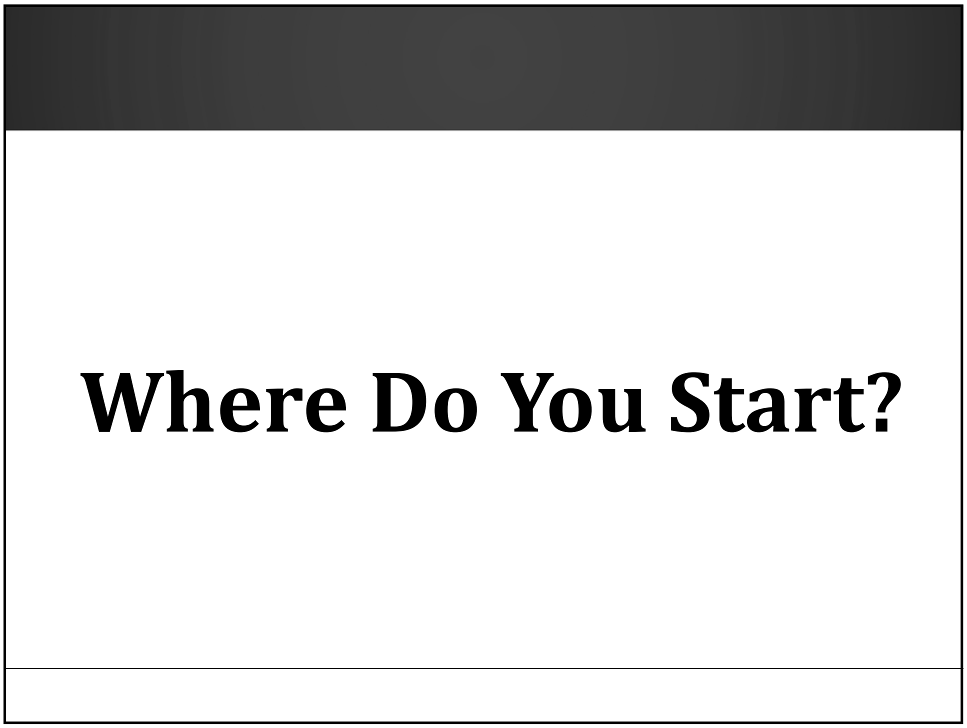
Congratulations!

Our
Deepest
Condolences

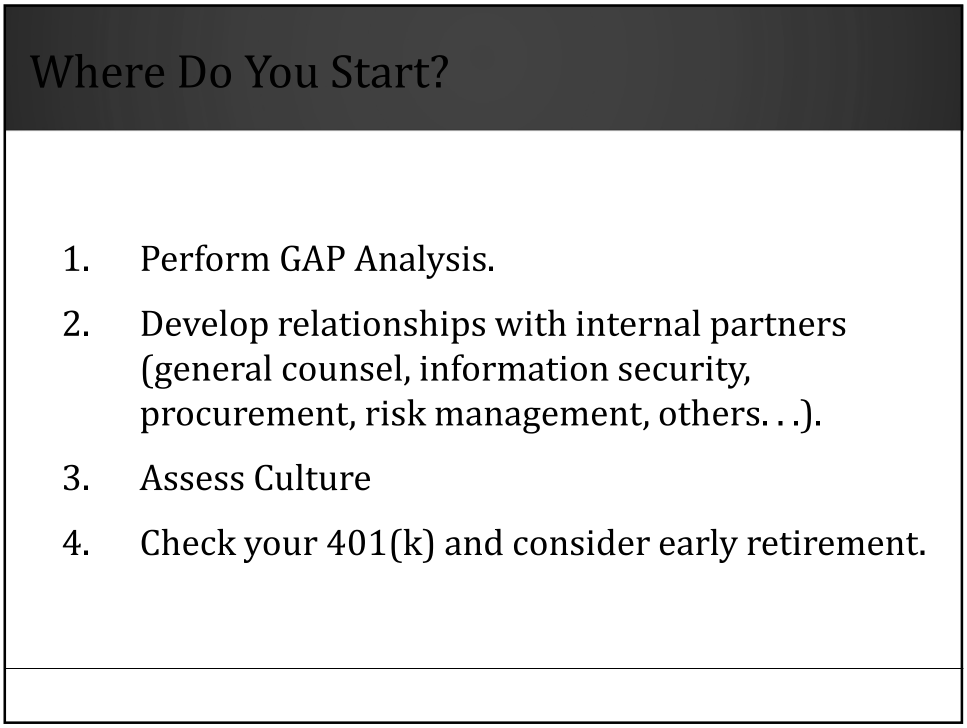


Welcome To Regional Health System . . .

One problem … the regional health system did not previously designate a full-time privacy officer. Or the person who was there did nothing to build an actual privacy compliance program. His/her motto was: “it’s all good”

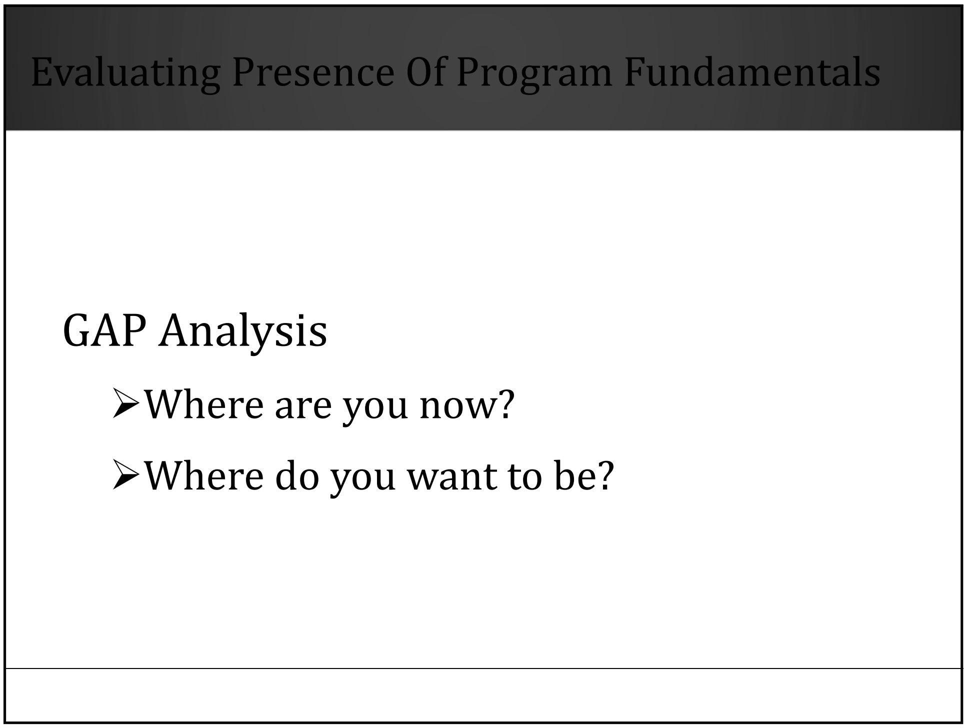


Where Do You Start?



Where Do You Start?

1. Perform GAP Analysis.
2. Develop relationships with internal partners (general counsel, information security, procurement, risk management, others. . .).
3. Assess Culture
4. Check your 401(k) and consider early retirement.



Evaluating Presence Of Program Fundamentals

GAP Analysis

- ➢Where are you now?
- ➢Where do you want to be?

GAP Analysis

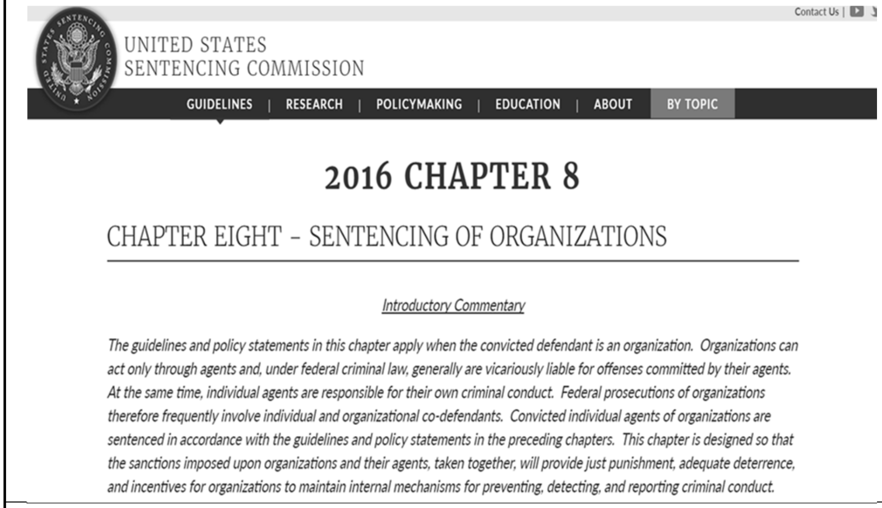
Great idea – we'll take six months to prepare a full analysis of the program! Maybe we can hire a vendor to do this…

Advice From The Front Lines: Use The "Effective Elements Of A Compliance Program" To Quickly Perform A GAP Analysis

How Do I Do That Exactly?

Answer: Let's do a quick recap of the US Sentencing Guidelines – and the Seven Effective Elements of a Compliance Plan.

What Happens When A Health Care Organization Breaks The Law?



Contact Us |
GUIDELINES | RESEARCH | POLICYMAKING | EDUCATION | ABOUT | BY TOPIC

UNITED STATES
SENTENCING COMMISSION

2016 CHAPTER 8

CHAPTER EIGHT – SENTENCING OF ORGANIZATIONS

Introductory Commentary

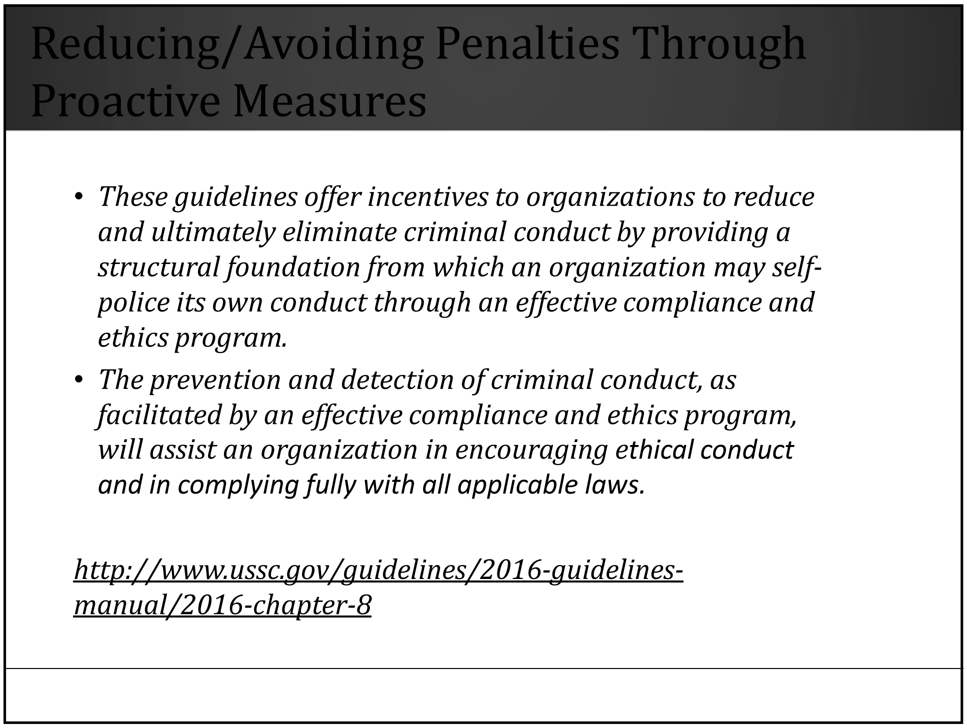
The guidelines and policy statements in this chapter apply when the convicted defendant is an organization. Organizations can act only through agents and, under federal criminal law, generally are vicariously liable for offenses committed by their agents. At the same time, individual agents are responsible for their own criminal conduct. Federal prosecutions of organizations therefore frequently involve individual and organizational co-defendants. Convicted individual agents of organizations are sentenced in accordance with the guidelines and policy statements in the preceding chapters. This chapter is designed so that the sanctions imposed upon organizations and their agents, taken together, will provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct.

Sentencing A Corporation

The four factors that increase the ultimate punishment of an organization are: (i) the involvement in or tolerance of criminal activity; (ii) the prior history of the organization; (iii) the violation of an order; and (iv) the obstruction of justice.

***The two factors that mitigate the ultimate punishment of an organization are**: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility.*

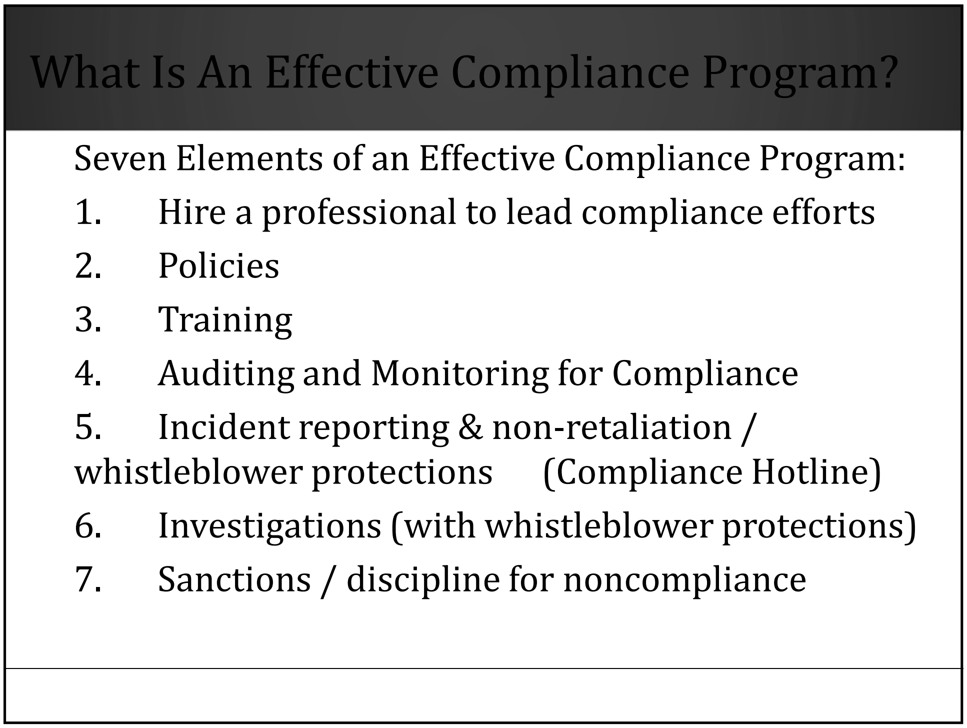
http://www.ussc.gov/guidelines/2016-guidelines-manual/2016-chapter-8



Reducing/Avoiding Penalties Through Proactive Measures

- *These guidelines offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program.*
- *The prevention and detection of criminal conduct, as facilitated by an effective compliance and ethics program, will assist an organization in encouraging ethical conduct and in complying fully with all applicable laws.*

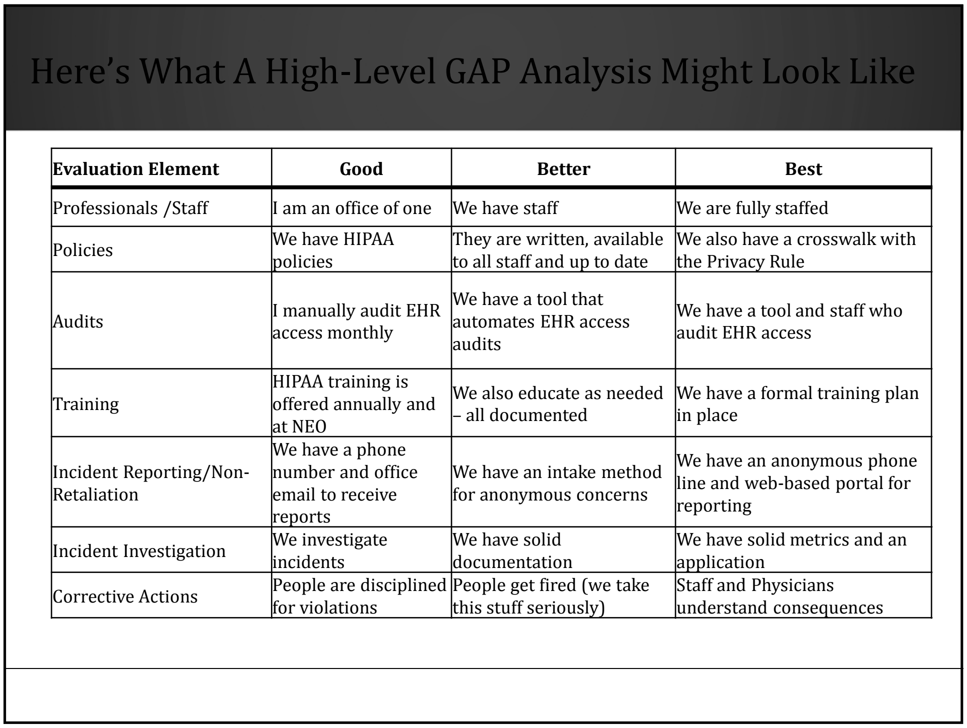
http://www.ussc.gov/guidelines/2016-guidelines-manual/2016-chapter-8



What Is An Effective Compliance Program?

Seven Elements of an Effective Compliance Program:

1. Hire a professional to lead compliance efforts
2. Policies
3. Training
4. Auditing and Monitoring for Compliance
5. Incident reporting & non-retaliation / whistleblower protections (Compliance Hotline)
6. Investigations (with whistleblower protections)
7. Sanctions / discipline for noncompliance

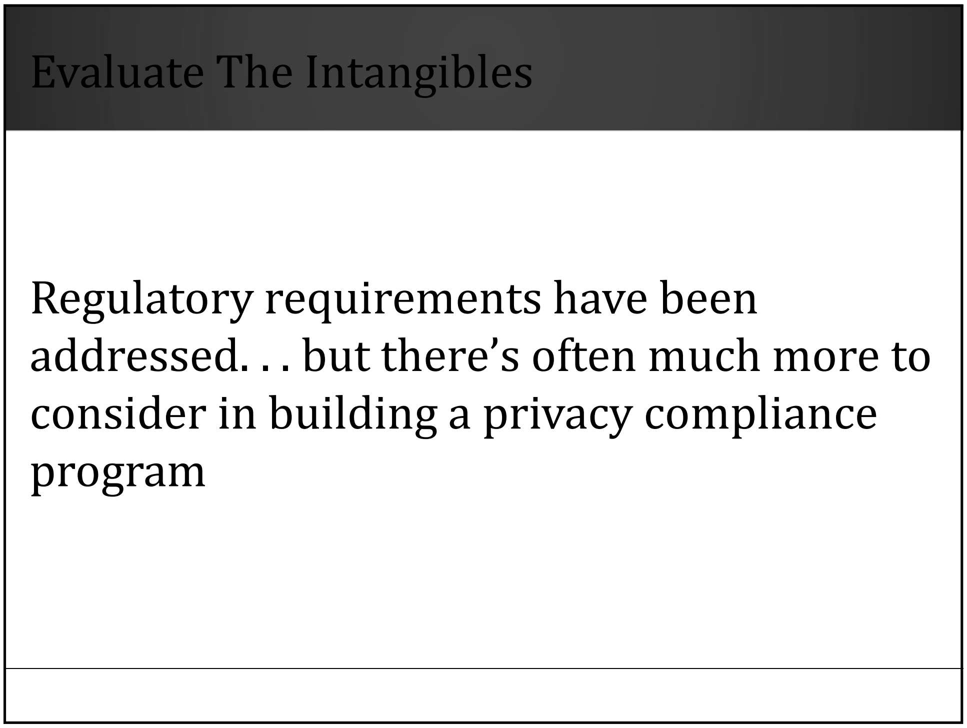


Here's What A High-Level GAP Analysis Might Look Like

Evaluation Element	Good	Better	Best
Professionals /Staff	I am an office of one	We have staff	We are fully staffed
Policies	We have HIPAA policies	They are written, available to all staff and up to date	We also have a crosswalk with the Privacy Rule
Audits	I manually audit EHR access monthly	We have a tool that automates EHR access audits	We have a tool and staff who audit EHR access
Training	HIPAA training is offered annually and at NEO	We also educate as needed – all documented	We have a formal training plan in place
Incident Reporting/Non-Retaliation	We have a phone number and office email to receive reports	We have an intake method for anonymous concerns	We have an anonymous phone line and web-based portal for reporting
Incident Investigation	We investigate incidents	We have solid documentation	We have solid metrics and an application
Corrective Actions	People are disciplined for violations	People get fired (we take this stuff seriously)	Staff and Physicians understand consequences

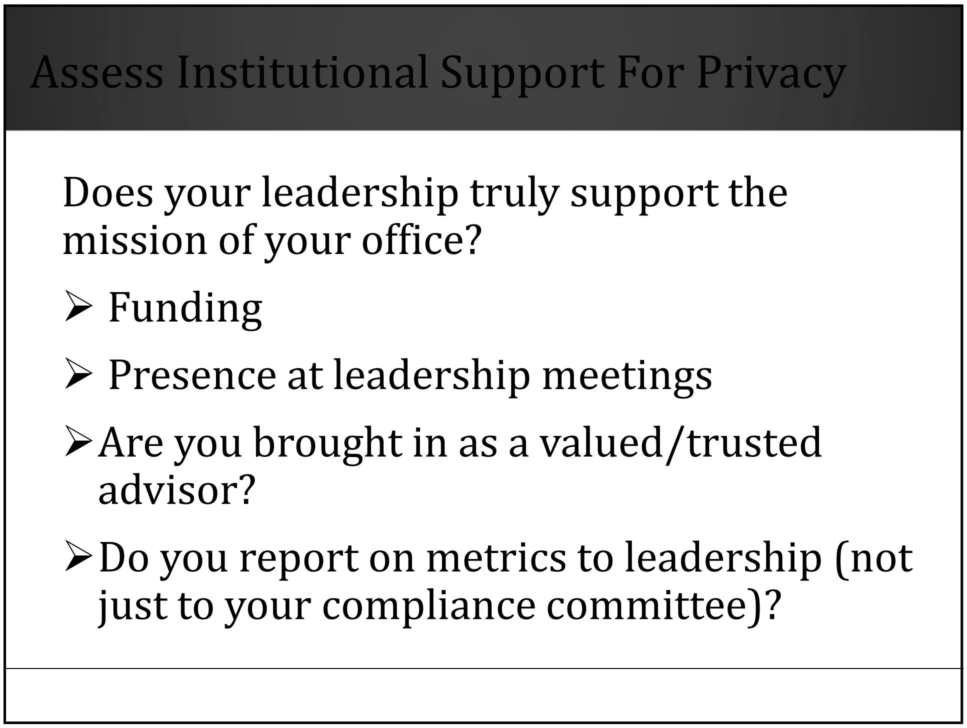
After The GAP Analysis Is Complete

What Should I Do Next?



Evaluate The Intangibles

Regulatory requirements have been addressed. . . but there's often much more to consider in building a privacy compliance program



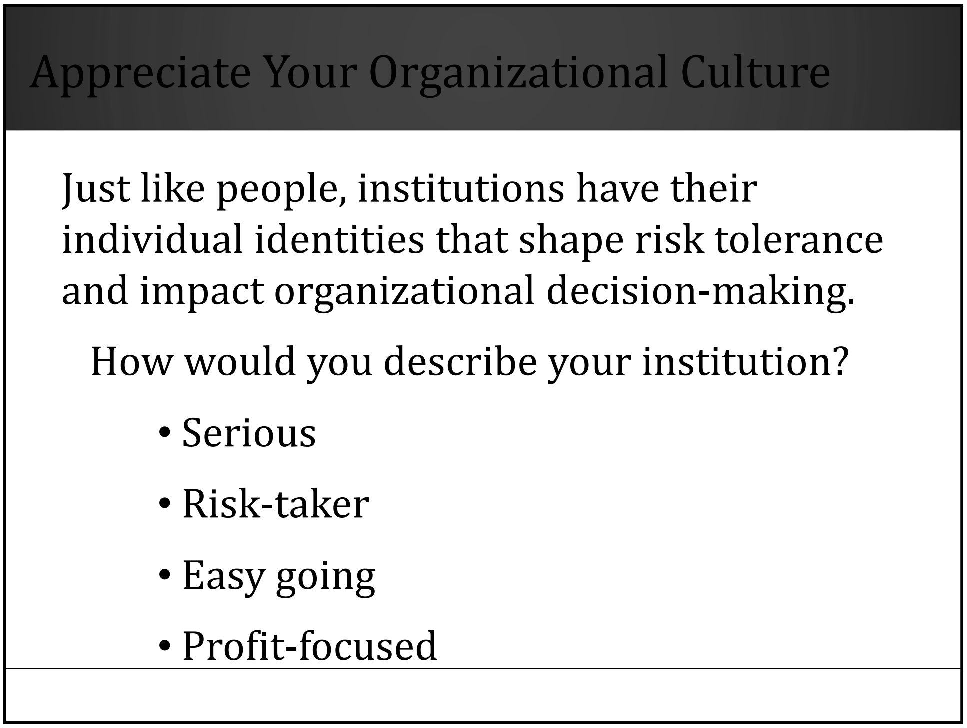
Assess Institutional Support For Privacy

Does your leadership truly support the mission of your office?

- ➢ Funding
- ➢ Presence at leadership meetings
- ➢ Are you brought in as a valued/trusted advisor?
- ➢ Do you report on metrics to leadership (not just to your compliance committee)?

Identify Your Strategic Partners

- ➢ Compliance
- ➢ Legal
- ➢ Procurement/Contracts
- ➢ Risk Management
- ➢ Information Security
- ➢ Medical / Administrative Departments
- ➢ Physicians
- ➢ Members of Administration
- ➢ Outside Counsel

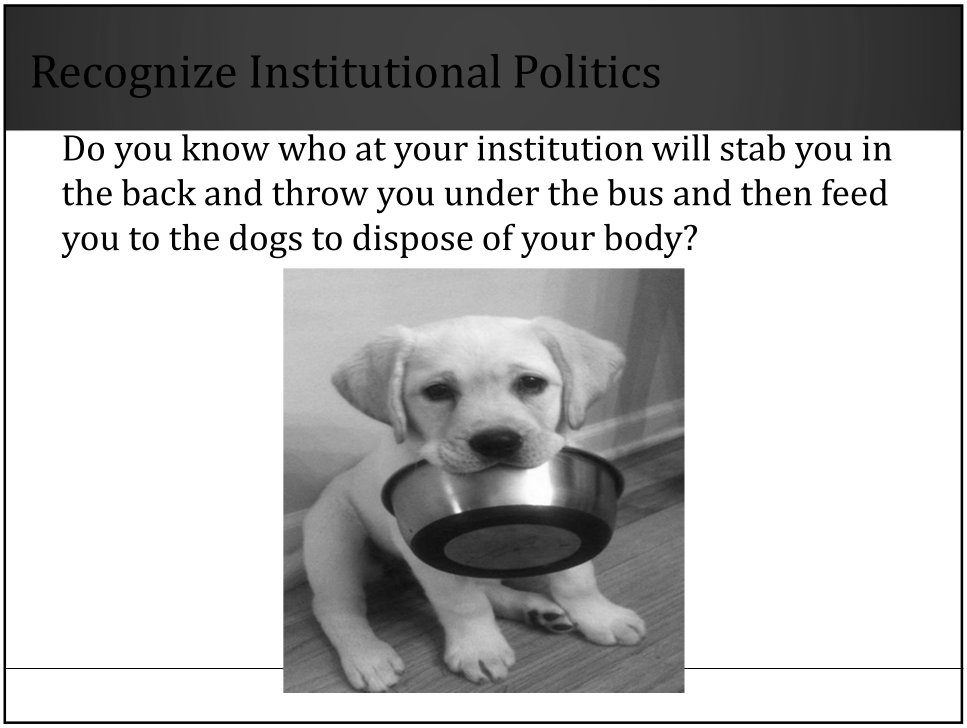


Appreciate Your Organizational Culture

Just like people, institutions have their individual identities that shape risk tolerance and impact organizational decision-making.

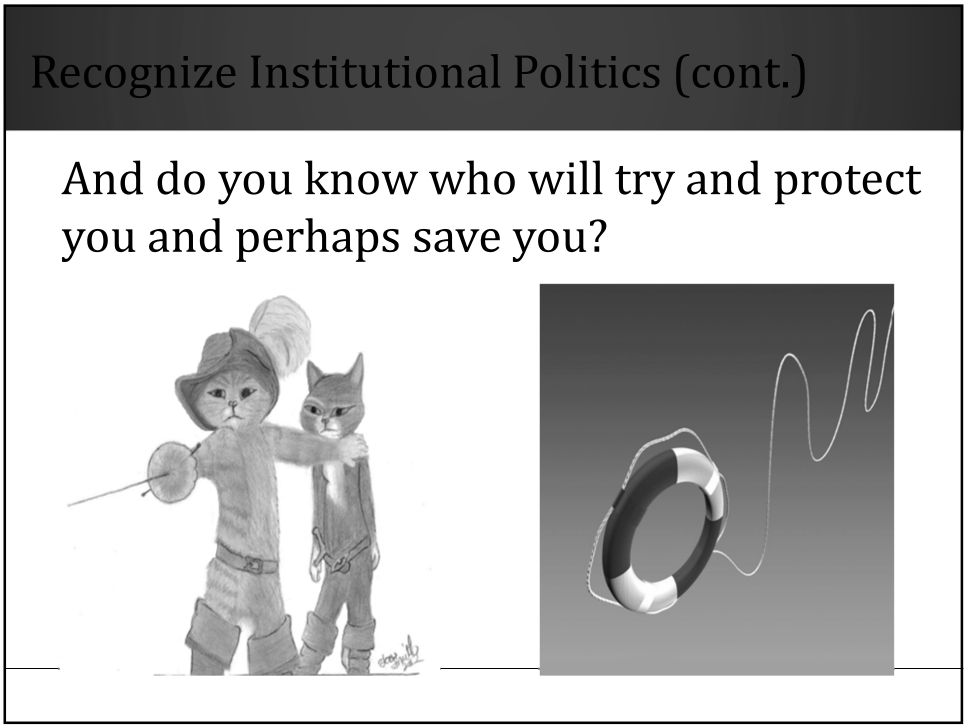
How would you describe your institution?

- Serious
- Risk-taker
- Easy going
- Profit-focused



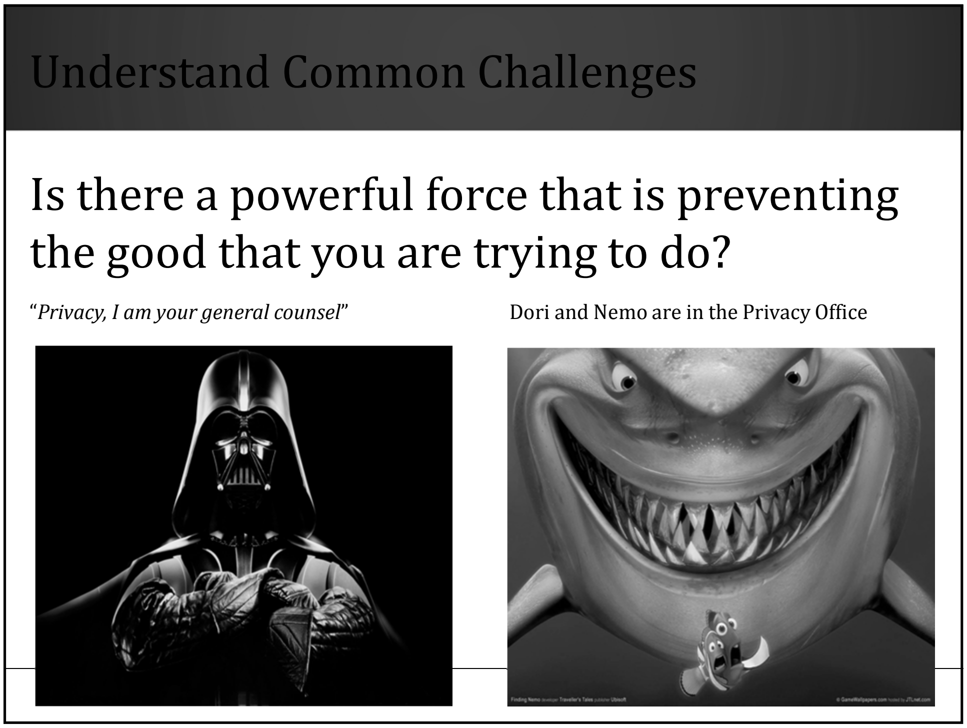
Recognize Institutional Politics

Do you know who at your institution will stab you in the back and throw you under the bus and then feed you to the dogs to dispose of your body?



Recognize Institutional Politics (cont.)

And do you know who will try and protect you and perhaps save you?

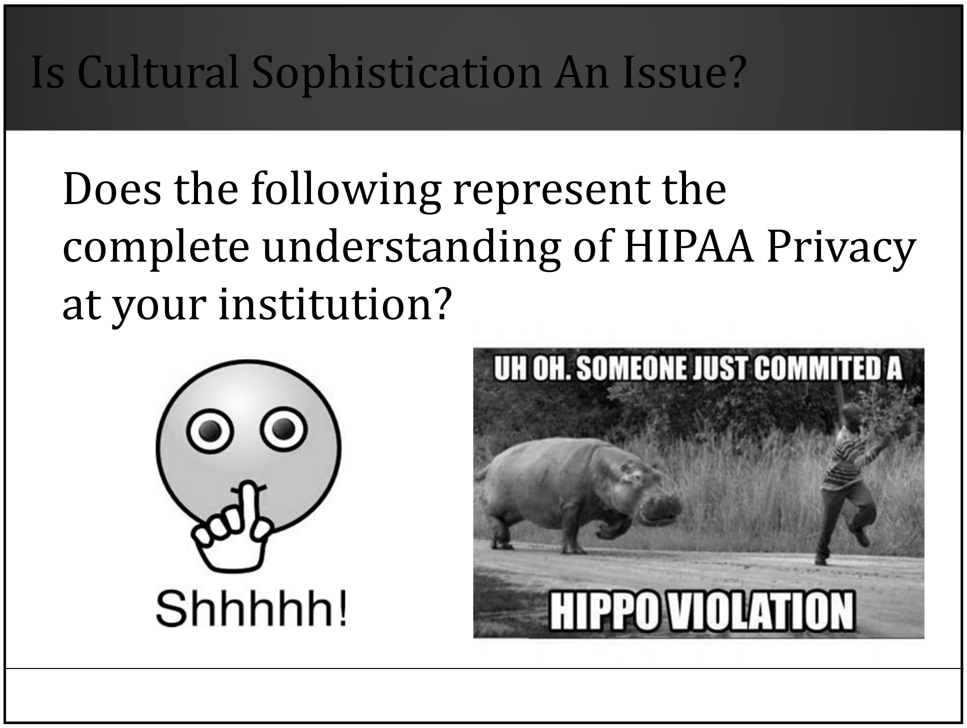


Understand Common Challenges

Is there a powerful force that is preventing the good that you are trying to do?

"Privacy, I am your general counsel"

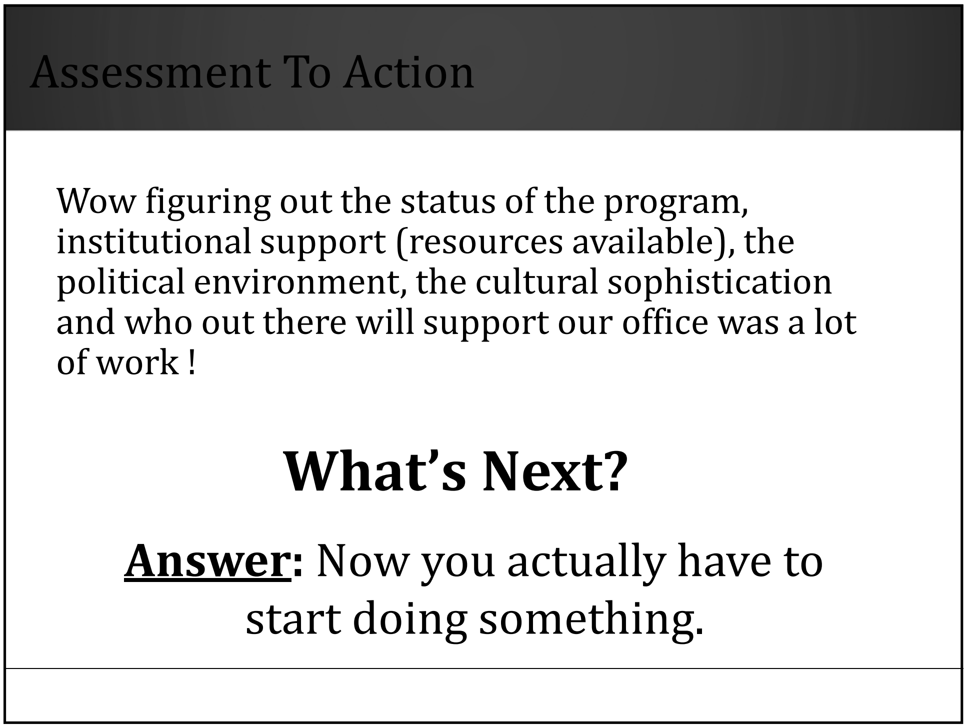
Dori and Nemo are in the Privacy Office



Is Cultural Sophistication An Issue?

Does the following represent the complete understanding of HIPAA Privacy at your institution?

Shhhhh!
UH OH. SOMEONE JUST COMMITED A
HIPPO VIOLATION

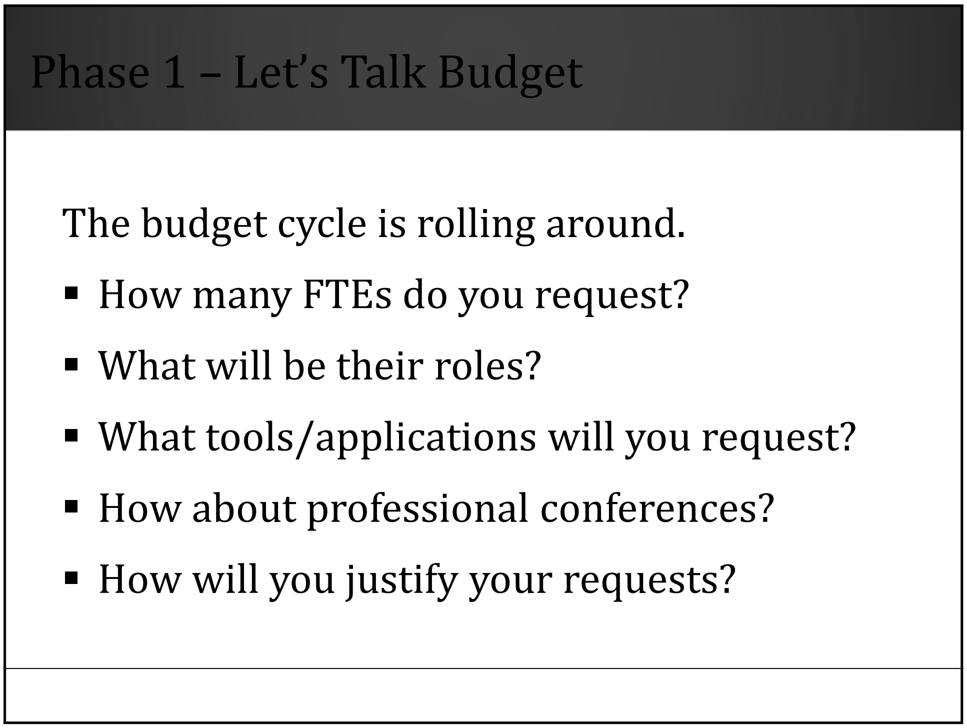


Assessment To Action

Wow figuring out the status of the program, institutional support (resources available), the political environment, the cultural sophistication and who out there will support our office was a lot of work !

What's Next?

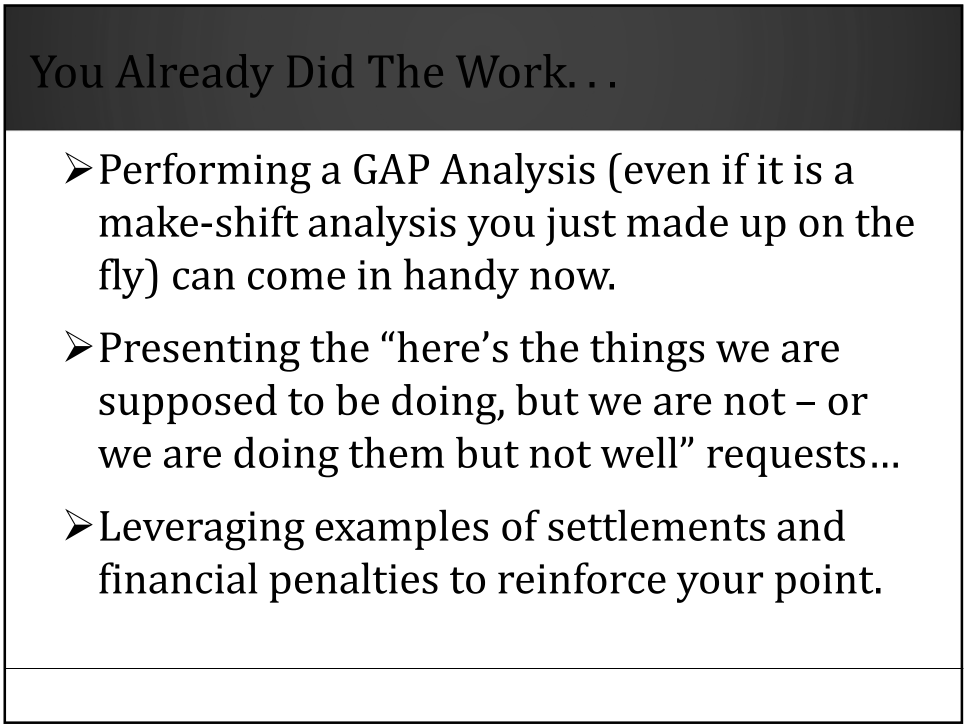
<u>Answer</u>: Now you actually have to start doing something.



Phase 1 – Let's Talk Budget

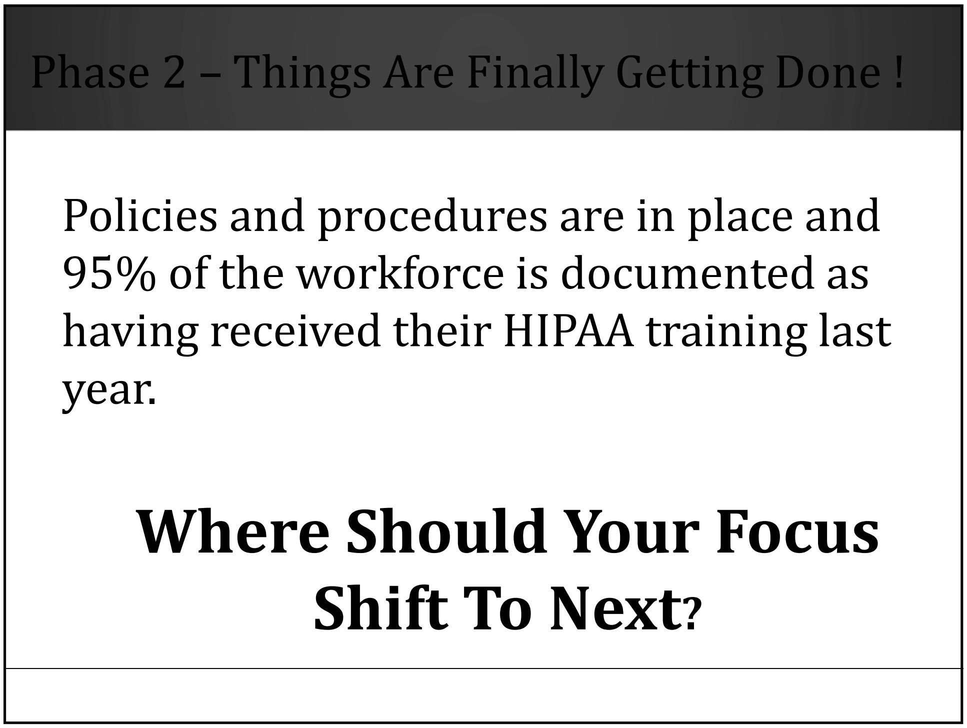
The budget cycle is rolling around.

- How many FTEs do you request?
- What will be their roles?
- What tools/applications will you request?
- How about professional conferences?
- How will you justify your requests?



You Already Did The Work. . .

- Performing a GAP Analysis (even if it is a make-shift analysis you just made up on the fly) can come in handy now.
- Presenting the "here's the things we are supposed to be doing, but we are not – or we are doing them but not well" requests…
- Leveraging examples of settlements and financial penalties to reinforce your point.



Phase 2 – Things Are Finally Getting Done !

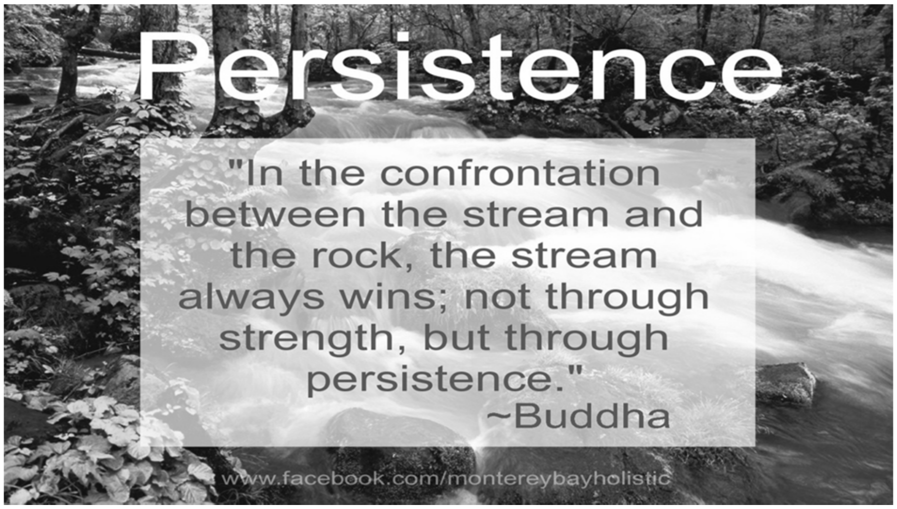
Policies and procedures are in place and 95% of the workforce is documented as having received their HIPAA training last year.

Where Should Your Focus Shift To Next?

How Your Current Program & GAP Analysis Can Continue To Drive Your Focus

- You know whether there may be funds for something like an electronic access audit tool or an incident management tool. If so, this may be where you go next.
- Or, you may need to improve training . . .
- Has OCR been making noise lately?
- The point is your attention and direction should be dictated by your vision and the results of your institutional resources and support as well as your evaluation of risk.

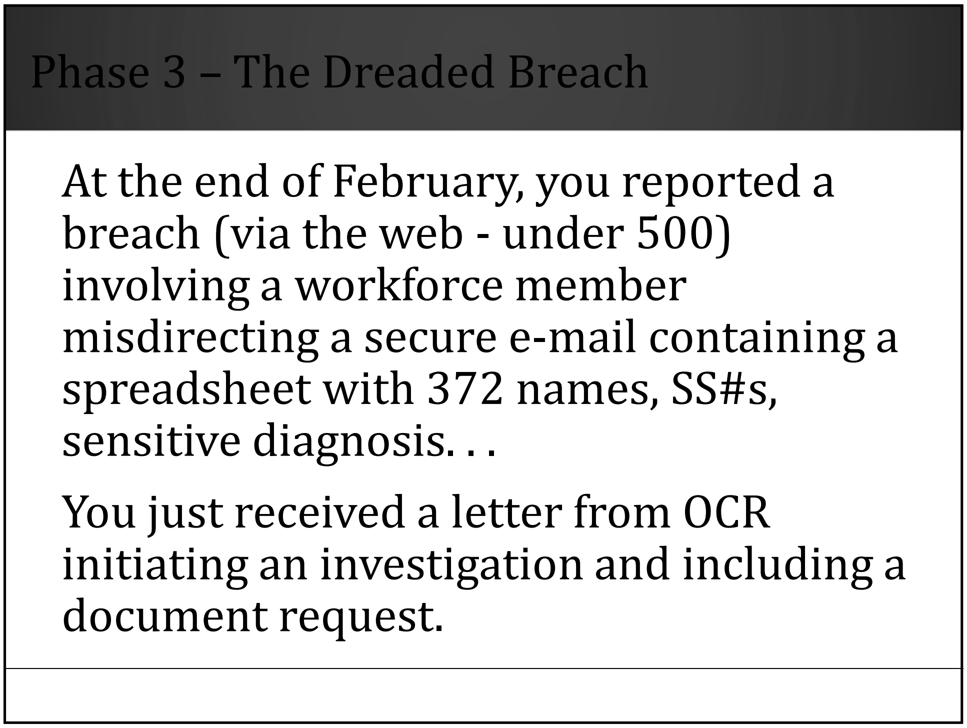
Remember – When Requesting Resources . . . Persistence Is Key



Persistence

"In the confrontation between the stream and the rock, the stream always wins; not through strength, but through persistence."
~Buddha

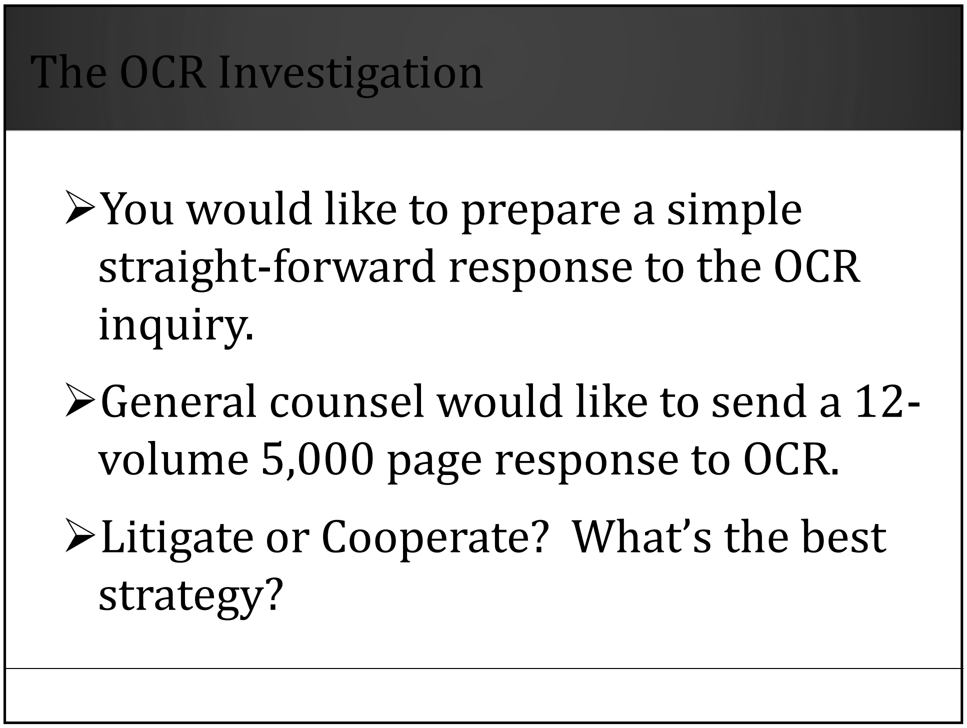
www.facebook.com/montereybayholistic



Phase 3 – The Dreaded Breach

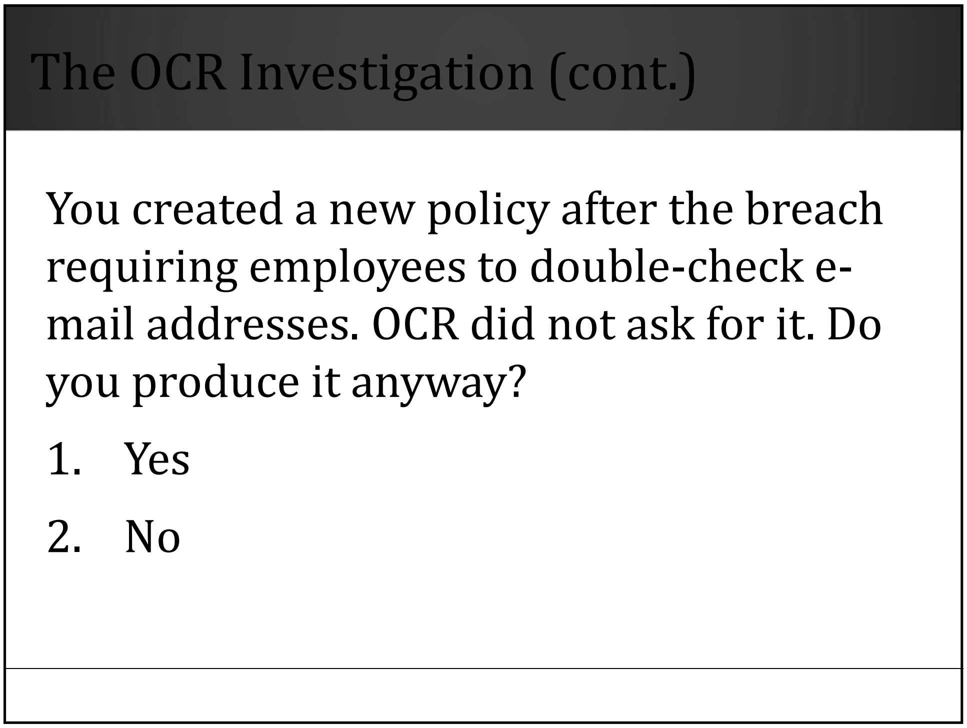
At the end of February, you reported a breach (via the web - under 500) involving a workforce member misdirecting a secure e-mail containing a spreadsheet with 372 names, SS#s, sensitive diagnosis. . .

You just received a letter from OCR initiating an investigation and including a document request.



The OCR Investigation

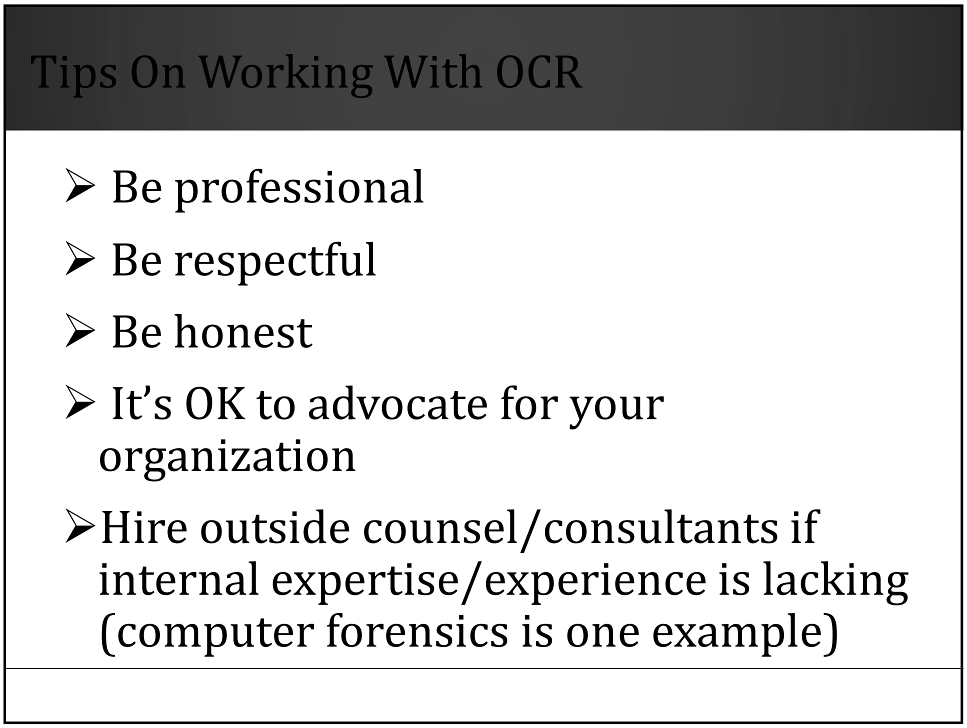
- You would like to prepare a simple straight-forward response to the OCR inquiry.
- General counsel would like to send a 12-volume 5,000 page response to OCR.
- Litigate or Cooperate? What’s the best strategy?



The OCR Investigation (cont.)

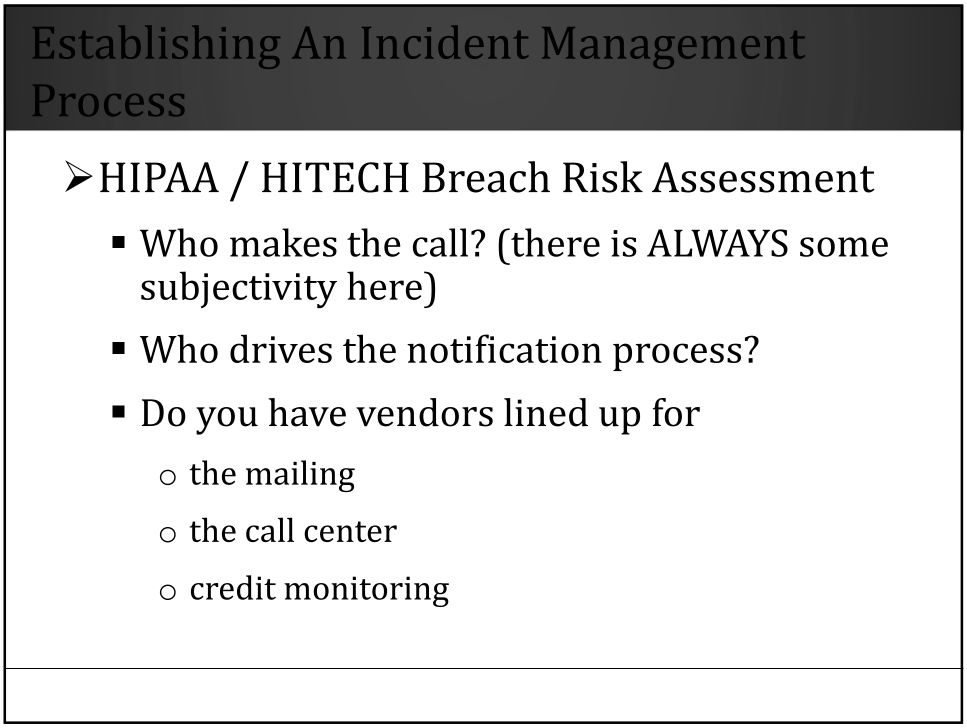
You created a new policy after the breach requiring employees to double-check e-mail addresses. OCR did not ask for it. Do you produce it anyway?

1. Yes
2. No



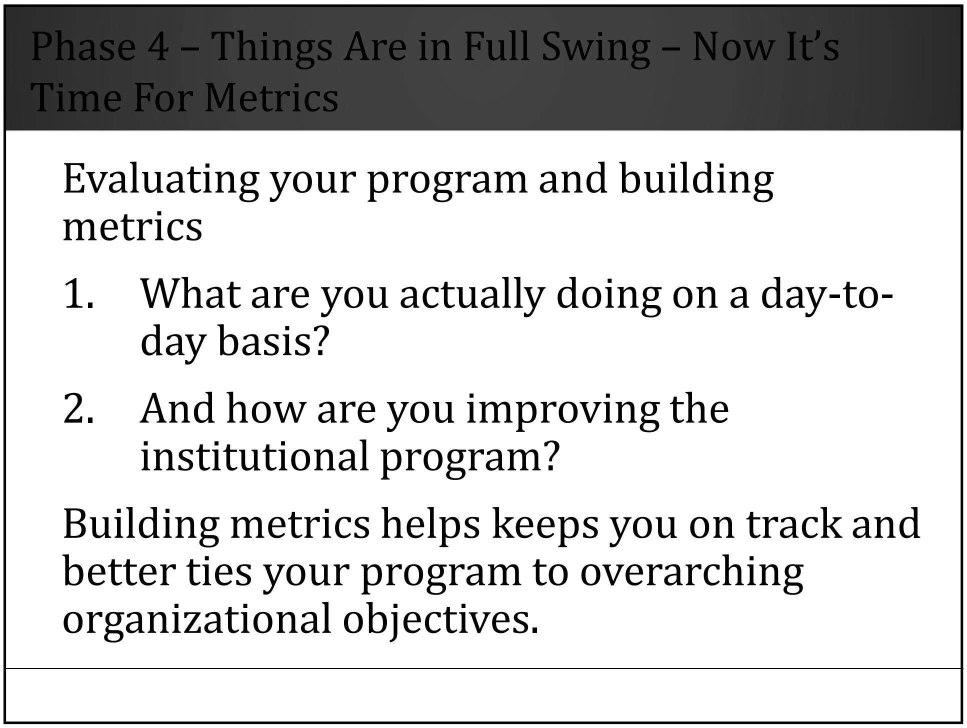
Tips On Working With OCR

- ➢ Be professional
- ➢ Be respectful
- ➢ Be honest
- ➢ It's OK to advocate for your organization
- ➢Hire outside counsel/consultants if internal expertise/experience is lacking (computer forensics is one example)



Establishing An Incident Management Process

- ➢HIPAA / HITECH Breach Risk Assessment
  - Who makes the call? (there is ALWAYS some subjectivity here)
  - Who drives the notification process?
  - Do you have vendors lined up for
    - the mailing
    - the call center
    - credit monitoring

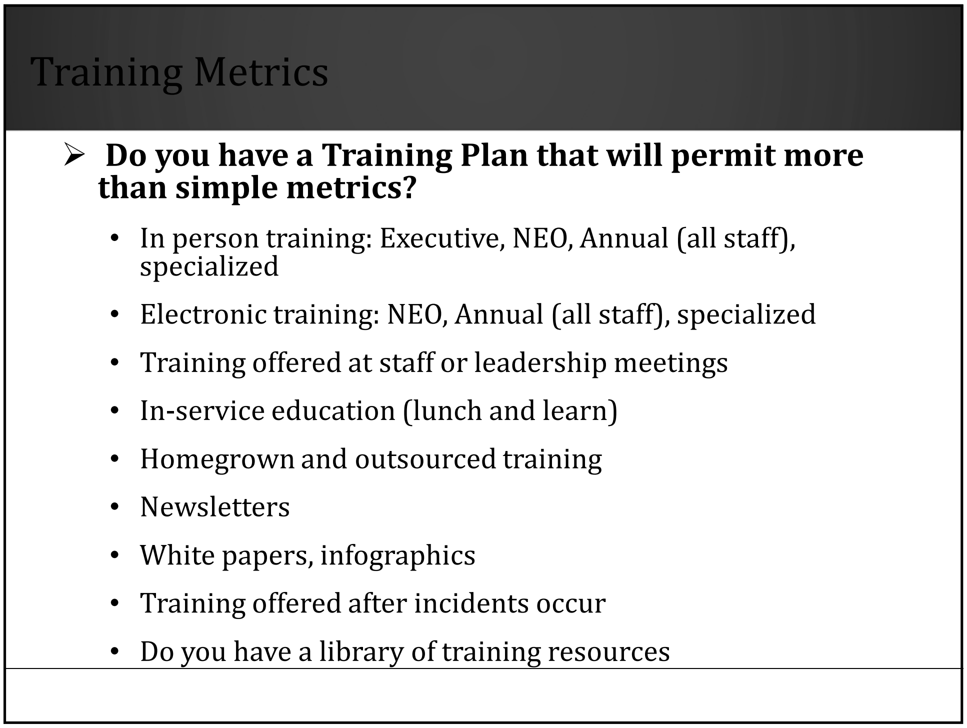


Phase 4 – Things Are in Full Swing – Now It's Time For Metrics

Evaluating your program and building metrics

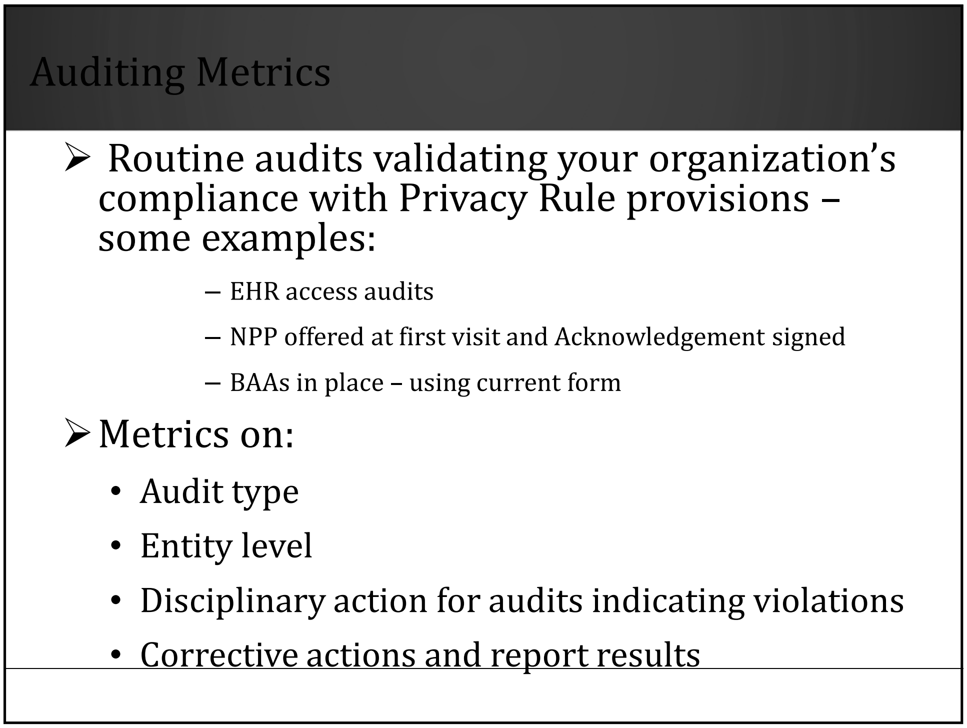
1. What are you actually doing on a day-to-day basis?
2. And how are you improving the institutional program?

Building metrics helps keeps you on track and better ties your program to overarching organizational objectives.



Training Metrics

- **Do you have a Training Plan that will permit more than simple metrics?**
  - In person training: Executive, NEO, Annual (all staff), specialized
  - Electronic training: NEO, Annual (all staff), specialized
  - Training offered at staff or leadership meetings
  - In-service education (lunch and learn)
  - Homegrown and outsourced training
  - Newsletters
  - White papers, infographics
  - Training offered after incidents occur
  - Do you have a library of training resources

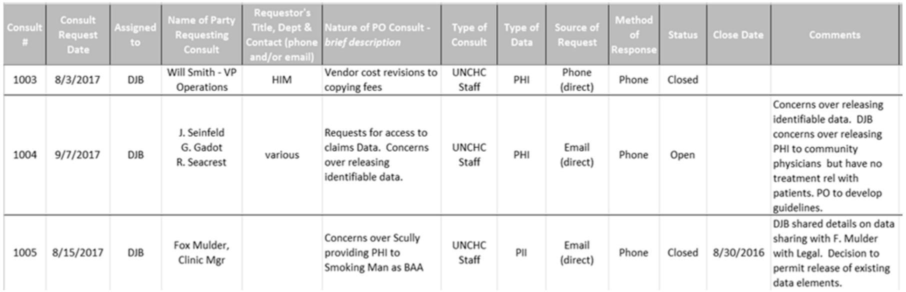


Auditing Metrics

- Routine audits validating your organization's compliance with Privacy Rule provisions – some examples:
  - EHR access audits
  - NPP offered at first visit and Acknowledgement signed
  - BAAs in place – using current form
- Metrics on:
  - Audit type
  - Entity level
  - Disciplinary action for audits indicating violations
  - Corrective actions and report results

Consult And Guidance Metrics

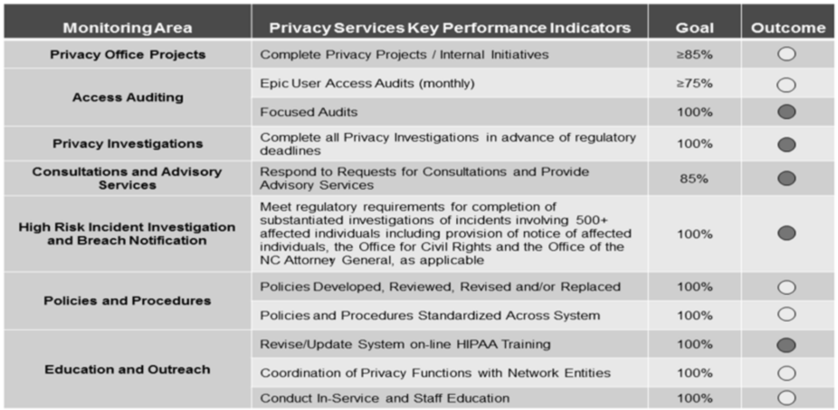
Here is one example for collecting and recording this data



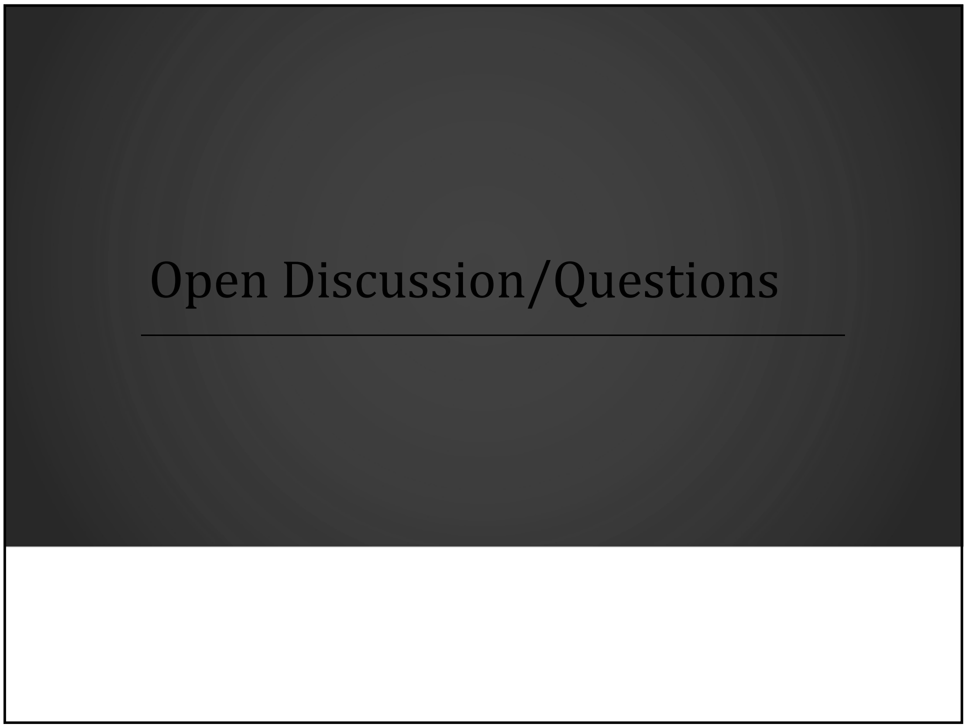
Consult #	Consult Request Date	Assigned to	Name of Party Requesting Consult	Requestor's Title, Dept & Contact (phone and/or email)	Nature of PO Consult - *brief description*	Type of Consult	Type of Data	Source of Request	Method of Response	Status	Close Date	Comments
1003	8/3/2017	DJB	Will Smith - VP Operations	HIM	Vendor cost revisions to copying fees	UNCHC Staff	PHI	Phone (direct)	Phone	Closed		
1004	9/7/2017	DJB	J. Seinfeld G. Gadot R. Seacrest	various	Requests for access to claims Data. Concerns over releasing identifiable data.	UNCHC Staff	PHI	Email (direct)	Phone	Open		Concerns over releasing identifiable data. DJB concerns over releasing PHI to community physicians but have no treatment rel with patients. PO to develop guidelines.
1005	8/15/2017	DJB	Fox Mulder, Clinic Mgr		Concerns over Scully providing PHI to Smoking Man as BAA	UNCHC Staff	PII	Email (direct)	Phone	Closed	8/30/2016	DJB shared details on data sharing with F. Mulder with Legal. Decision to permit release of existing data elements.

Program Metrics (KPIs) – At A Glance

Key Privacy Office Performance Indicators



Monitoring Area	Privacy Services Key Performance Indicators	Goal	Outcome
Privacy Office Projects	Complete Privacy Projects / Internal Initiatives	≥85%	○
Access Auditing	Epic User Access Audits (monthly)	≥75%	○
	Focused Audits	100%	●
Privacy Investigations	Complete all Privacy Investigations in advance of regulatory deadlines	100%	●
Consultations and Advisory Services	Respond to Requests for Consultations and Provide Advisory Services	85%	●
High Risk Incident Investigation and Breach Notification	Meet regulatory requirements for completion of substantiated investigations of incidents involving 500+ affected individuals including provision of notice of affected individuals, the Office for Civil Rights and the Office of the NC Attorney General, as applicable	100%	●
Policies and Procedures	Policies Developed, Reviewed, Revised and/or Replaced	100%	○
	Policies and Procedures Standardized Across System	100%	○
Education and Outreach	Revise/Update System on-line HIPAA Training	100%	●
	Coordination of Privacy Functions with Network Entities	100%	○
	Conduct In-Service and Staff Education	100%	○



Open Discussion/Questions