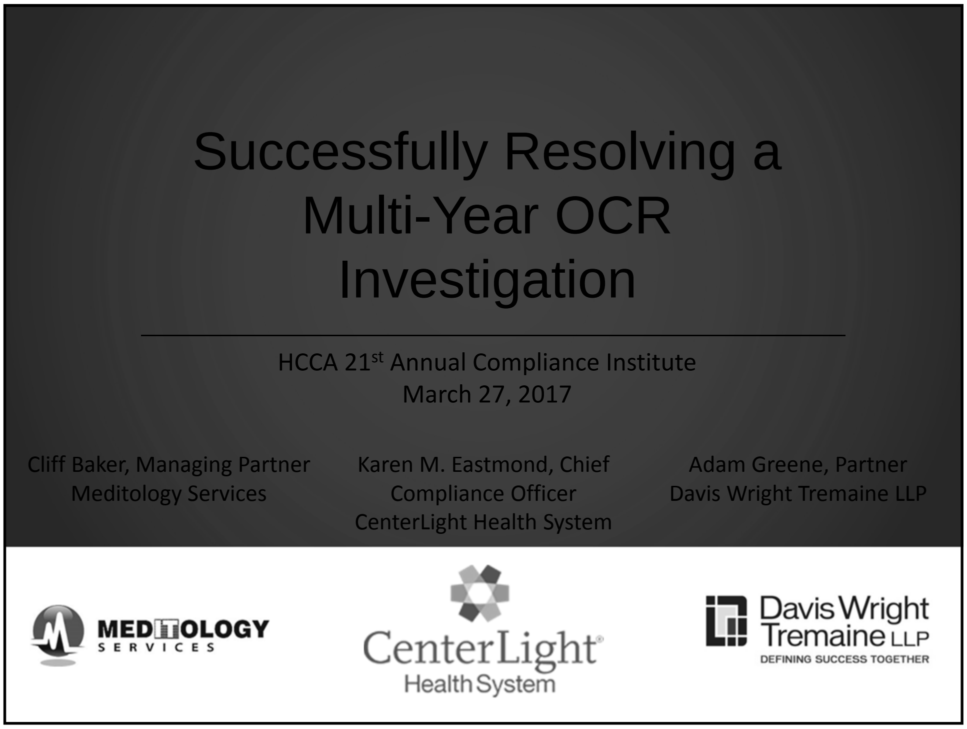


Successfully Resolving a Multi-Year OCR Investigation

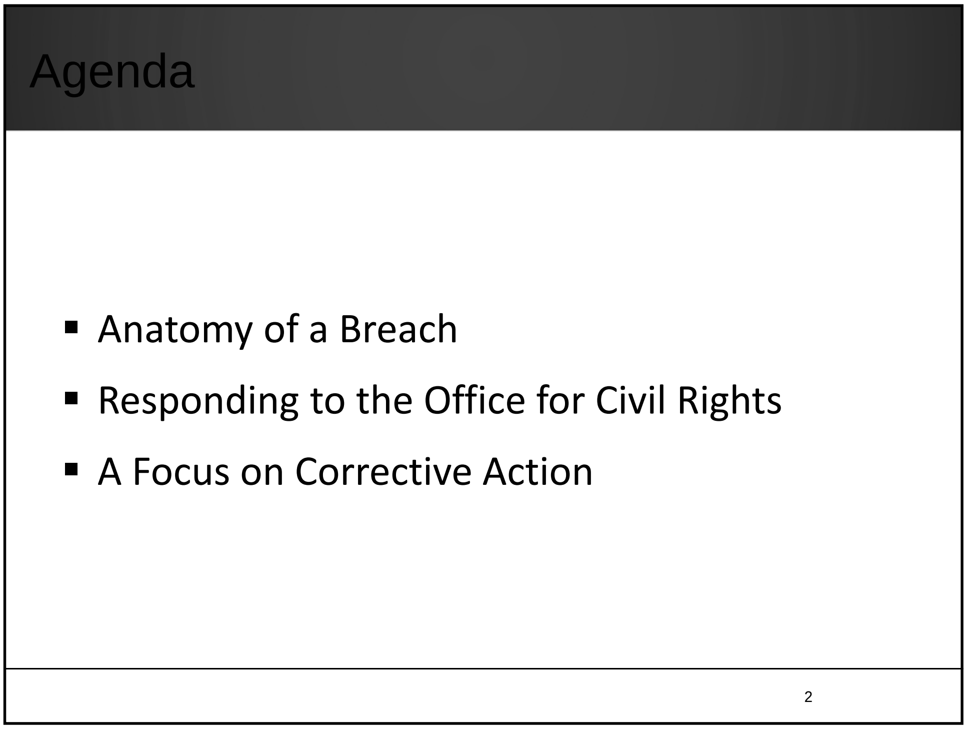
HCCA 21st Annual Compliance Institute
March 27, 2017

Cliff Baker, Managing Partner
Meditology Services

Karen M. Eastmond, Chief Compliance Officer
CenterLight Health System

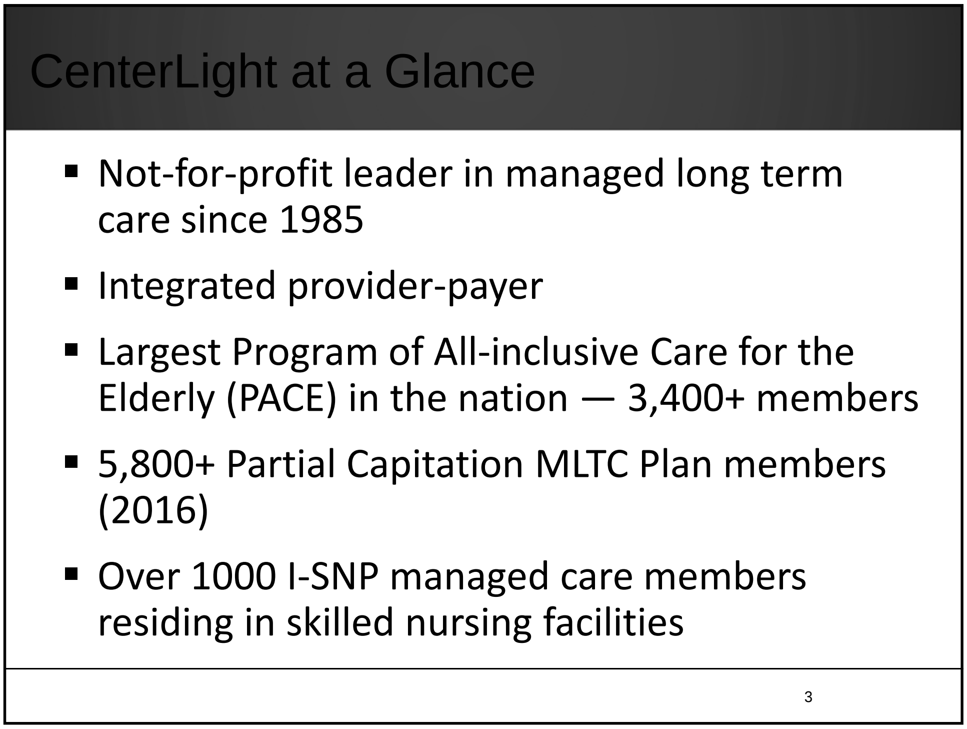
Adam Greene, Partner
Davis Wright Tremaine LLP

MEDITOLOGY SERVICES
CenterLight Health System
Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER



Agenda

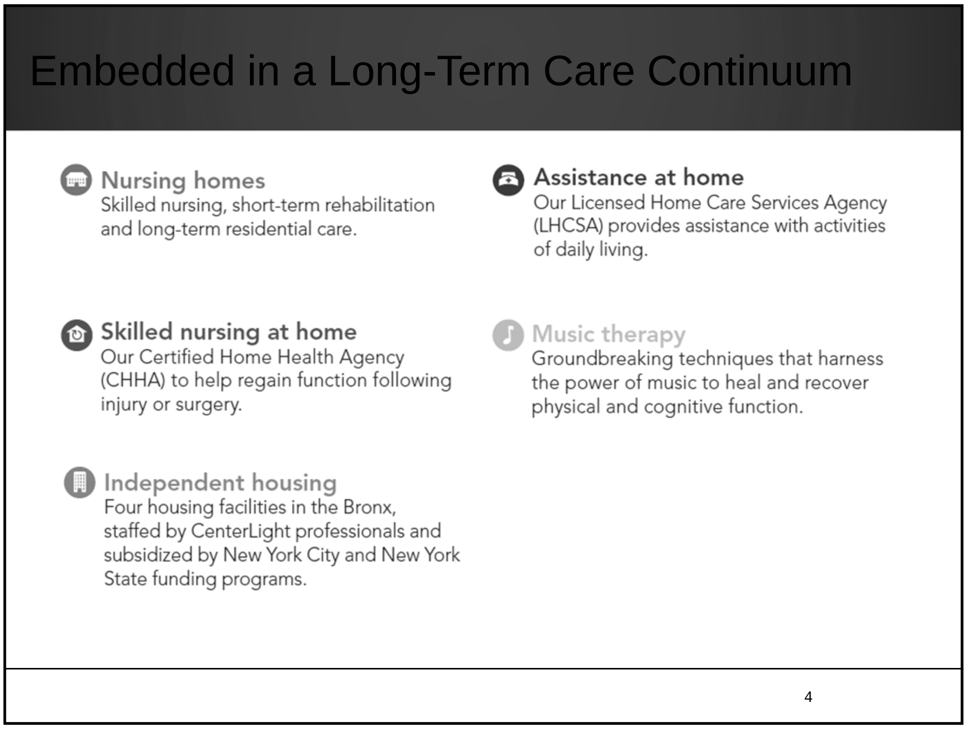
- Anatomy of a Breach
- Responding to the Office for Civil Rights
- A Focus on Corrective Action



CenterLight at a Glance

- Not-for-profit leader in managed long term care since 1985
- Integrated provider-payer
- Largest Program of All-inclusive Care for the Elderly (PACE) in the nation — 3,400+ members
- 5,800+ Partial Capitation MLTC Plan members (2016)
- Over 1000 I-SNP managed care members residing in skilled nursing facilities

3



Embedded in a Long-Term Care Continuum

Nursing homes
Skilled nursing, short-term rehabilitation and long-term residential care.

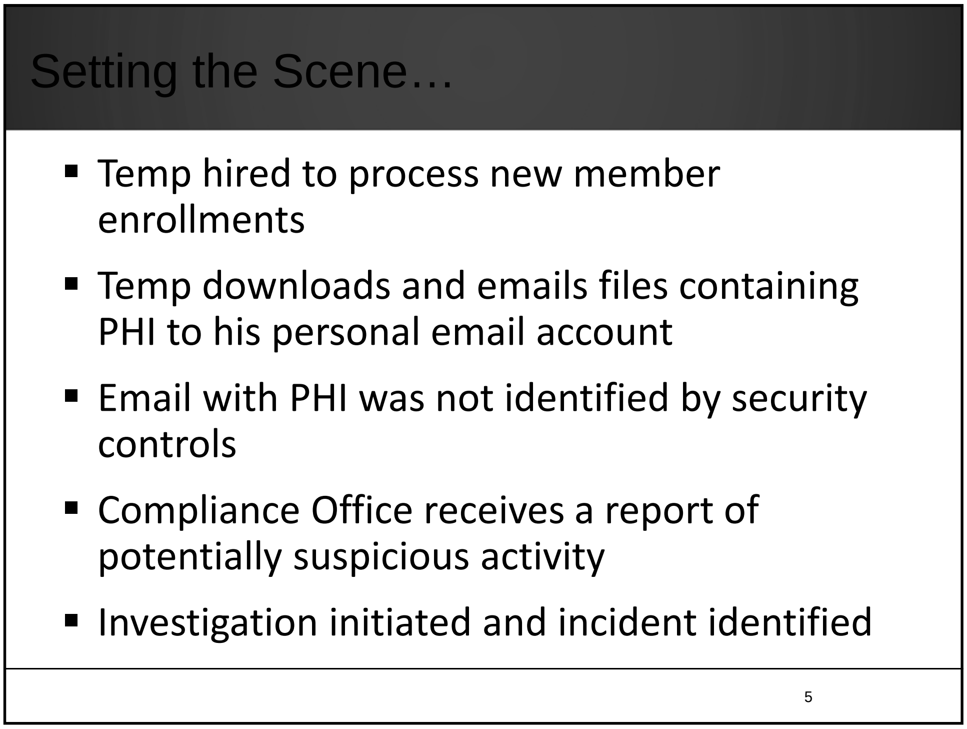
Assistance at home
Our Licensed Home Care Services Agency (LHCSA) provides assistance with activities of daily living.

Skilled nursing at home
Our Certified Home Health Agency (CHHA) to help regain function following injury or surgery.

Music therapy
Groundbreaking techniques that harness the power of music to heal and recover physical and cognitive function.

Independent housing
Four housing facilities in the Bronx, staffed by CenterLight professionals and subsidized by New York City and New York State funding programs.

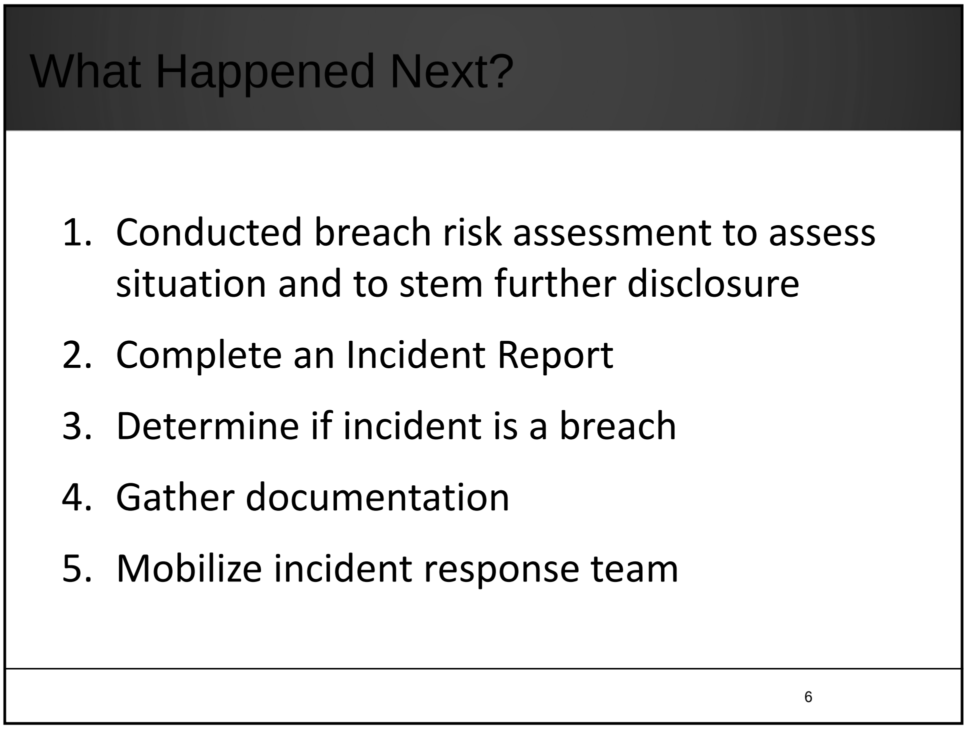
4



Setting the Scene…

- Temp hired to process new member enrollments
- Temp downloads and emails files containing PHI to his personal email account
- Email with PHI was not identified by security controls
- Compliance Office receives a report of potentially suspicious activity
- Investigation initiated and incident identified

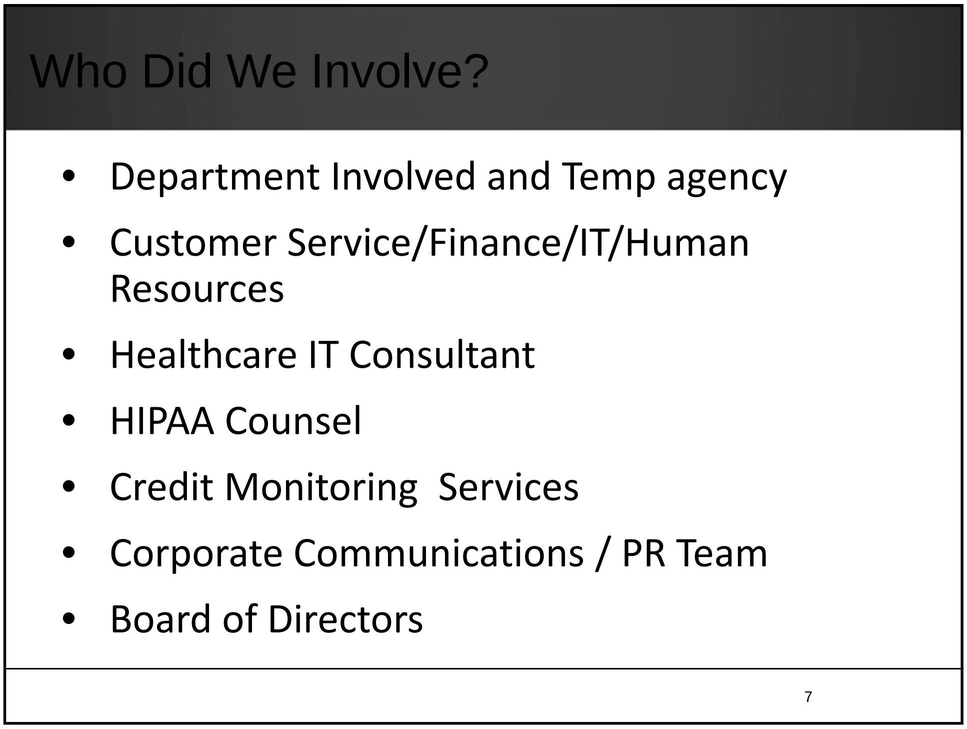
5



What Happened Next?

1. Conducted breach risk assessment to assess situation and to stem further disclosure
2. Complete an Incident Report
3. Determine if incident is a breach
4. Gather documentation
5. Mobilize incident response team

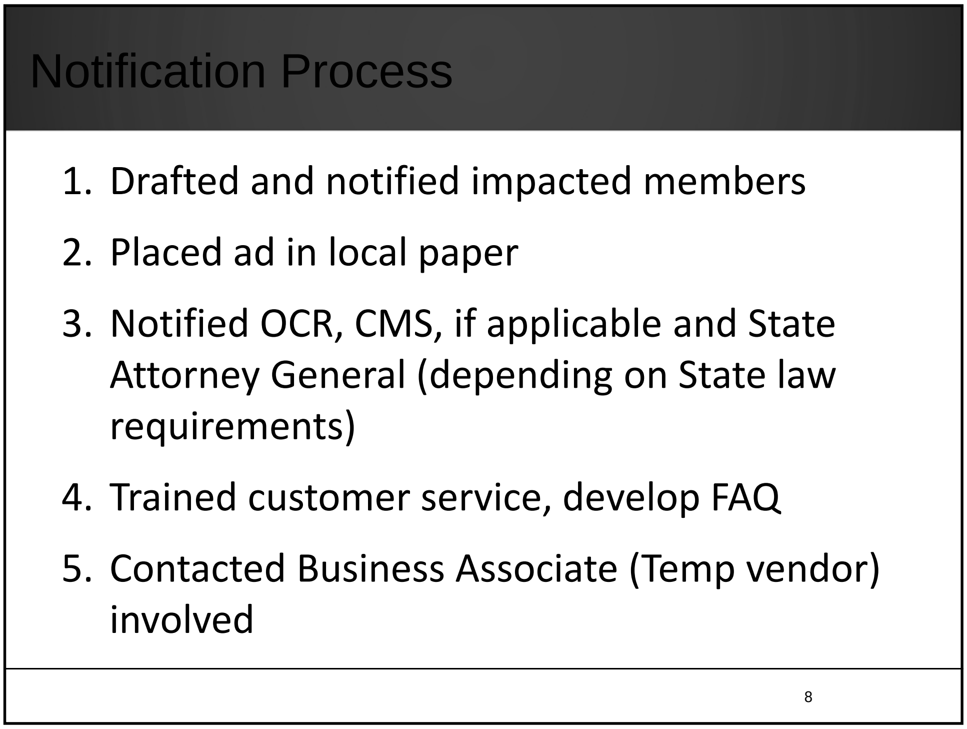
6



Who Did We Involve?

- Department Involved and Temp agency
- Customer Service/Finance/IT/Human Resources
- Healthcare IT Consultant
- HIPAA Counsel
- Credit Monitoring Services
- Corporate Communications / PR Team
- Board of Directors

7



Notification Process

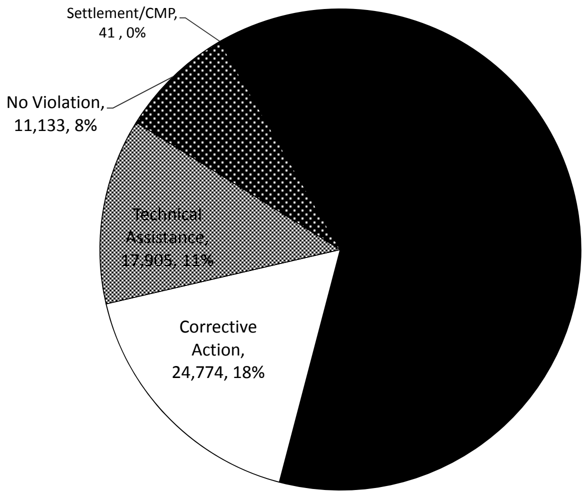
1. Drafted and notified impacted members
2. Placed ad in local paper
3. Notified OCR, CMS, if applicable and State Attorney General (depending on State law requirements)
4. Trained customer service, develop FAQ
5. Contacted Business Associate (Temp vendor) involved

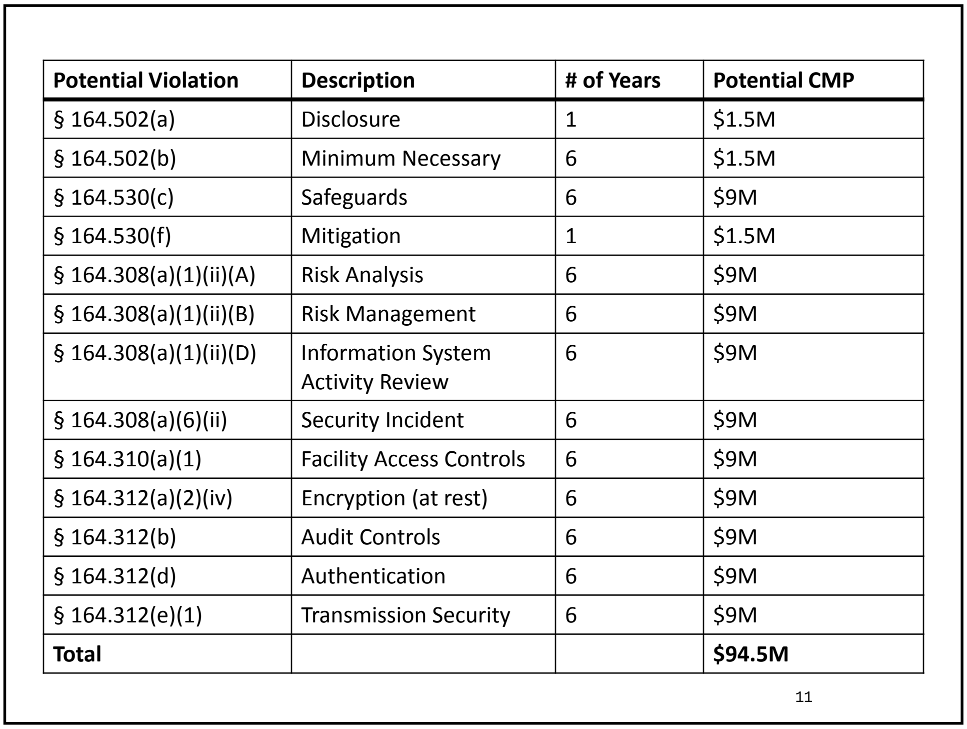
8

Be Prepared to Wait…

- Gather documentation to support your case
  - Training materials
  - Privacy & Security policies and procedures
  - Disciplinary action policies
- Further assess risks - consider whether you have adequate resources to do risk assessment or hire consultant with expertise in HIPAA Privacy & Security
- Consult with HIPAA counsel

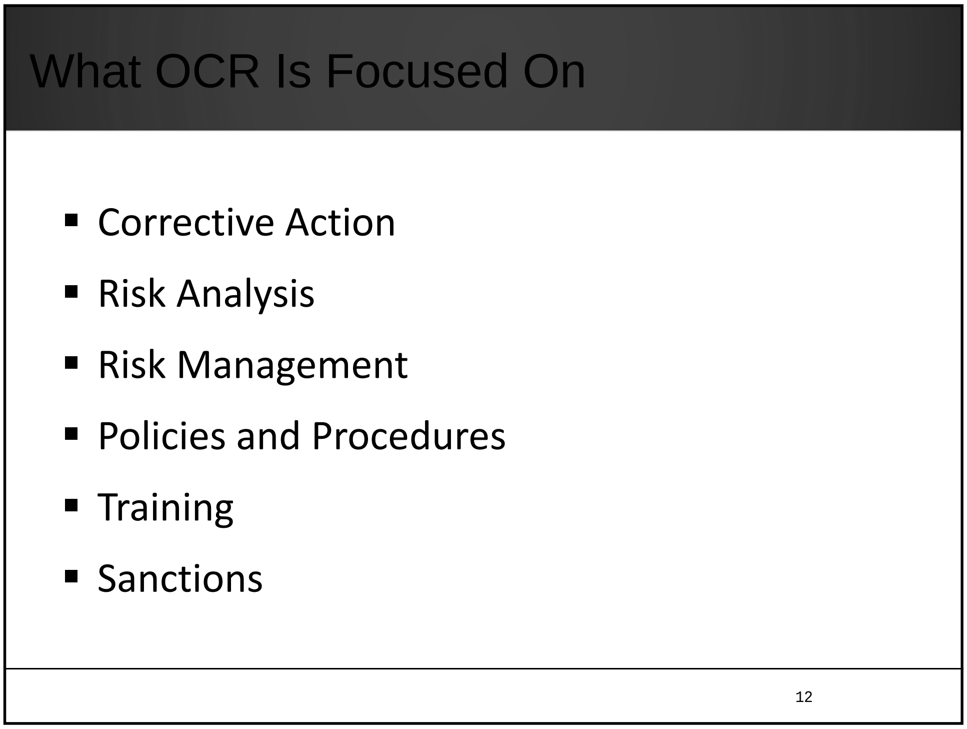
Enforcement Highlights (as of 12/31/16)





Potential Violation	Description	# of Years	Potential CMP
§ 164.502(a)	Disclosure	1	$1.5M
§ 164.502(b)	Minimum Necessary	6	$1.5M
§ 164.530(c)	Safeguards	6	$9M
§ 164.530(f)	Mitigation	1	$1.5M
§ 164.308(a)(1)(ii)(A)	Risk Analysis	6	$9M
§ 164.308(a)(1)(ii)(B)	Risk Management	6	$9M
§ 164.308(a)(1)(ii)(D)	Information System Activity Review	6	$9M
§ 164.308(a)(6)(ii)	Security Incident	6	$9M
§ 164.310(a)(1)	Facility Access Controls	6	$9M
§ 164.312(a)(2)(iv)	Encryption (at rest)	6	$9M
§ 164.312(b)	Audit Controls	6	$9M
§ 164.312(d)	Authentication	6	$9M
§ 164.312(e)(1)	Transmission Security	6	$9M
Total			**$94.5M**

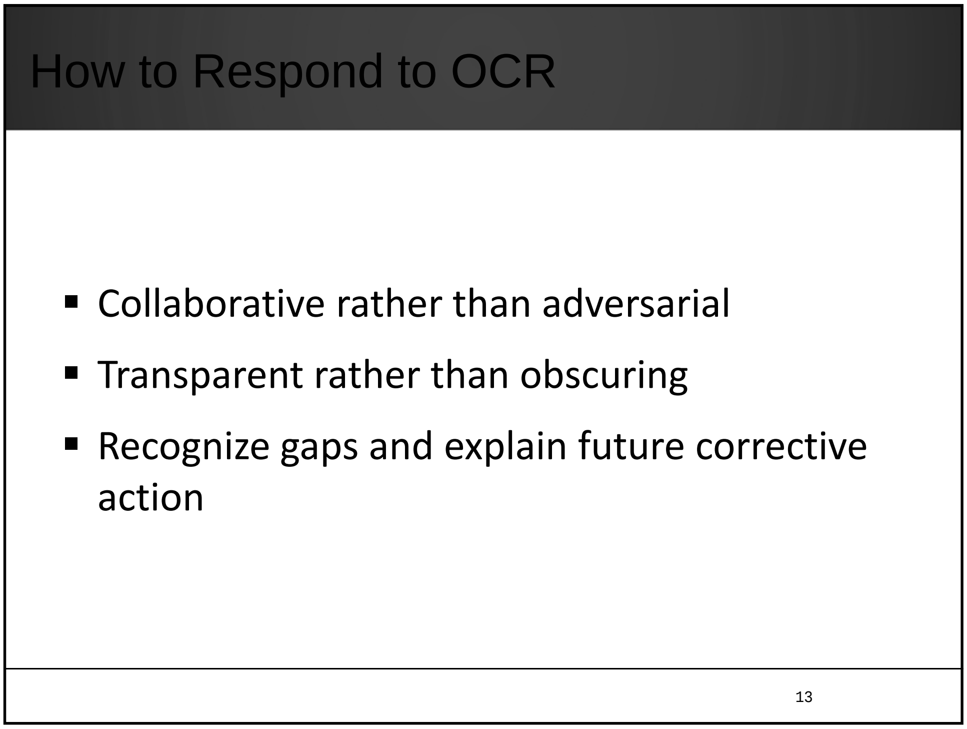
11



What OCR Is Focused On

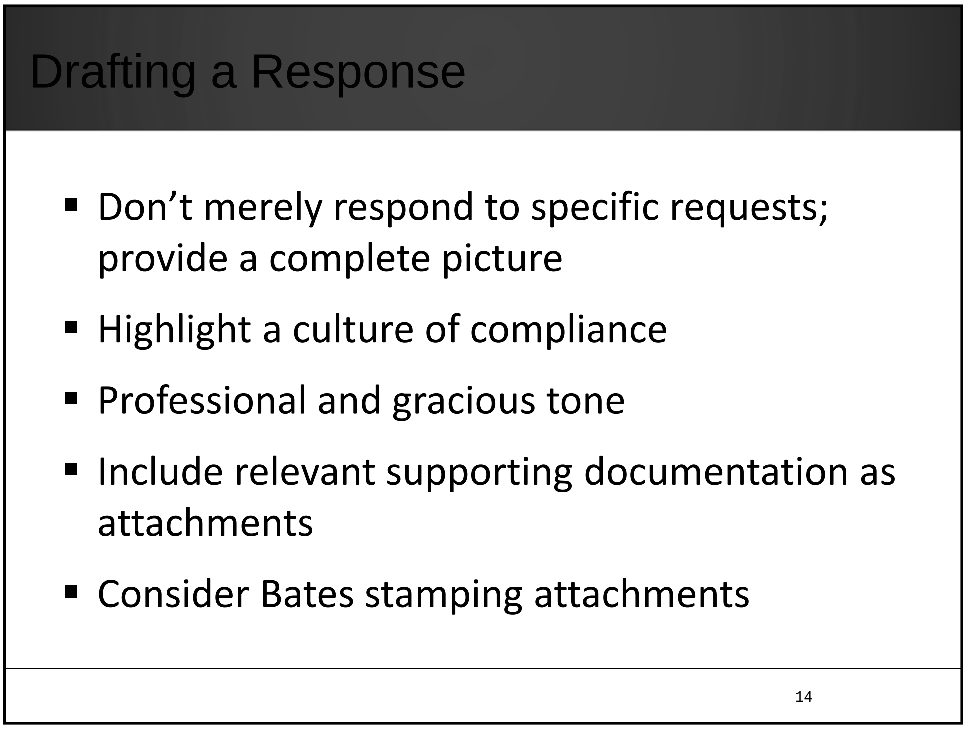
- Corrective Action
- Risk Analysis
- Risk Management
- Policies and Procedures
- Training
- Sanctions

12



How to Respond to OCR

- Collaborative rather than adversarial
- Transparent rather than obscuring
- Recognize gaps and explain future corrective action



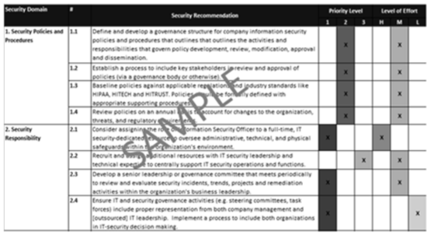
Drafting a Response

- Don’t merely respond to specific requests; provide a complete picture
- Highlight a culture of compliance
- Professional and gracious tone
- Include relevant supporting documentation as attachments
- Consider Bates stamping attachments

Corrective Action Plan

If you don't provide a solution a solution will be provided for you that you may not like

- Corrective Action Plan Characteristics
  - Identified Risk
  - Risk level (e.g., High, Med, Low)
  - Remediation Steps
  - Owner
  - Timeframe
  - Status and progress



Security Domain	#	Security Recommendation	Priority Level			Level of Effort		
			1	2	3	H	M	L
1. Security Policies and Procedures	1.1	Define and develop a governance structure for company information security policies and procedures that outlines that outlines the activities and responsibilities that govern policy development, review, modification, approval and dissemination.		X			X	
	1.2	Establish a process to include key stakeholders in review and approval of policies (via a governance body or otherwise).		X			X	
	1.3	Baseline policies against applicable regulations and industry standards like HIPAA, HITECH and HITRUST. Policies should be formally defined with appropriate supporting procedures.		X			X	
	1.4	Review policies on an annual basis to account for changes to the organization, threats, and regulatory requirements.		X			X	
2. Security Responsibility	2.1	Consider assigning the role of Information Security Officer to a full-time, IT security-dedicated resource to oversee administrative, technical, and physical safeguards within the organization's environment.	X			X		
	2.2	Recruit and assign additional resources with IT security leadership and technical expertise to centrally support IT security operations and functions.			X		X	
	2.3	Develop a senior leadership or governance committee that meets periodically to review and evaluate security incidents, trends, projects and remediation activities within the organization's business leadership.	X				X	
	2.4	Ensure IT and security governance activities (e.g. steering committees, task forces) include proper representation from both company management and [outsourced] IT leadership. Implement a process to include both organizations in IT-security decision making.	X					X

Corrective Action Plan - Governance

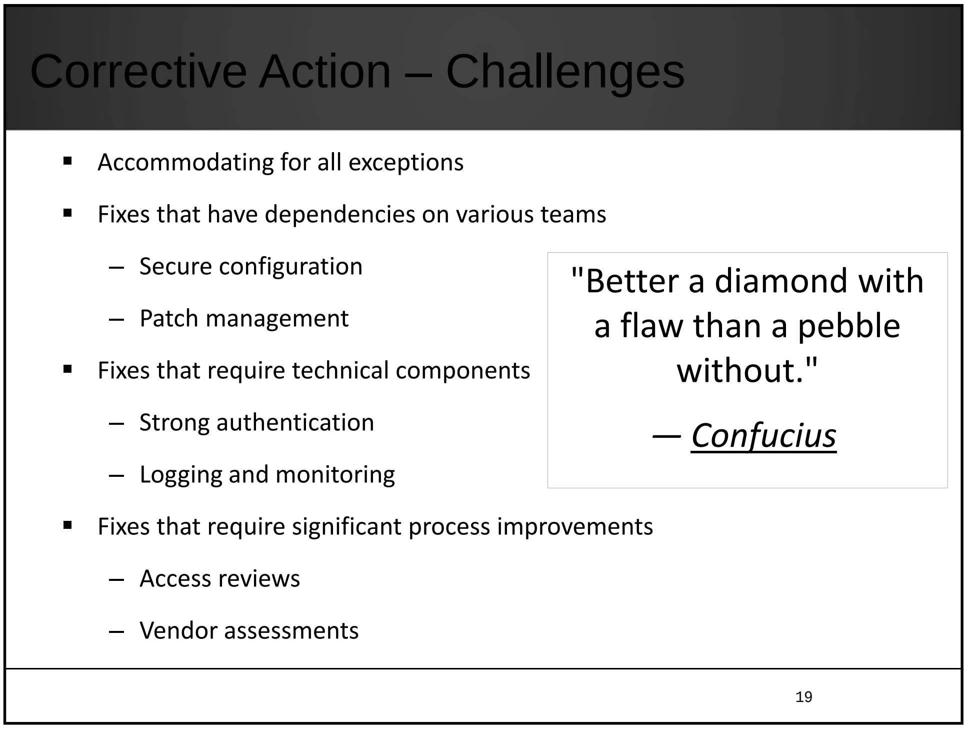
- Executive accountability
- Project management
- Roles and responsibilities
- Regular status updates and progress reporting

Corrective Action Plan - Scope

- Policy updates
- Process documentation
- People
  - Skillsets
  - Contract resources
  - Consulting
- Technology Solutions
  - Patch management
  - Two factor authentication
  - Monitoring solution

Corrective Action Plan – Key Considerations

- Don’t set yourself up to fail:
  - Timing (i.e., start and end dates)
  - Level of effort (i.e., FTE effort to get the work done)
  - Investment (i.e., budget)
  - Skillsets
  - Dependencies
  - At first focus on quick wins

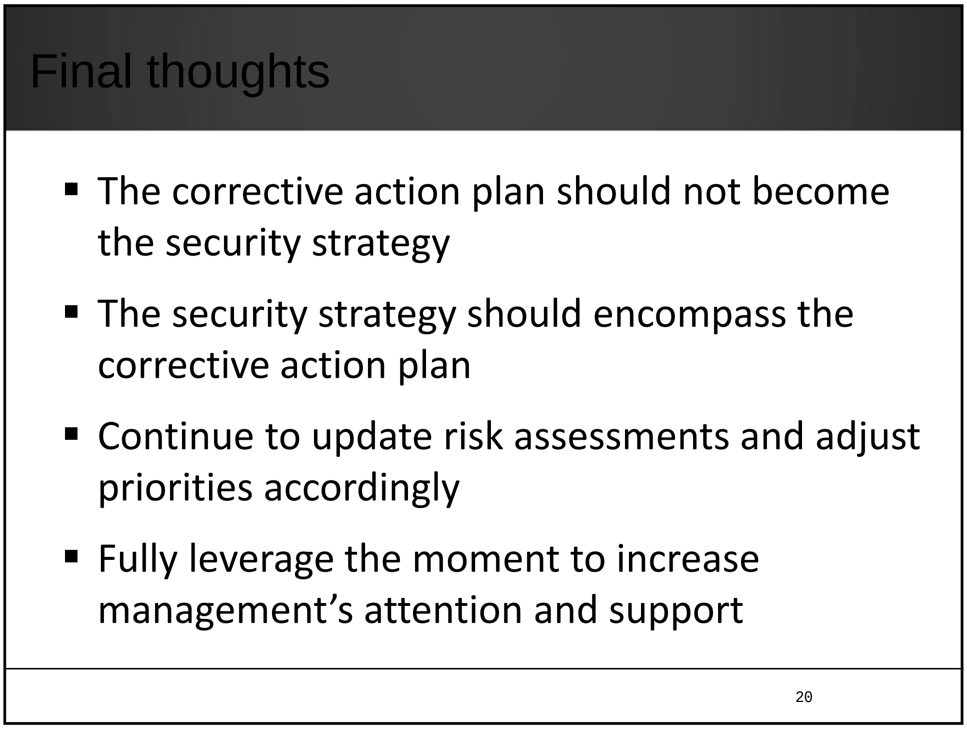


Corrective Action – Challenges

- Accommodating for all exceptions
- Fixes that have dependencies on various teams
  - Secure configuration
  - Patch management
- Fixes that require technical components
  - Strong authentication
  - Logging and monitoring
- Fixes that require significant process improvements
  - Access reviews
  - Vendor assessments

> "Better a diamond with a flaw than a pebble without."
>
> — *Confucius*

19

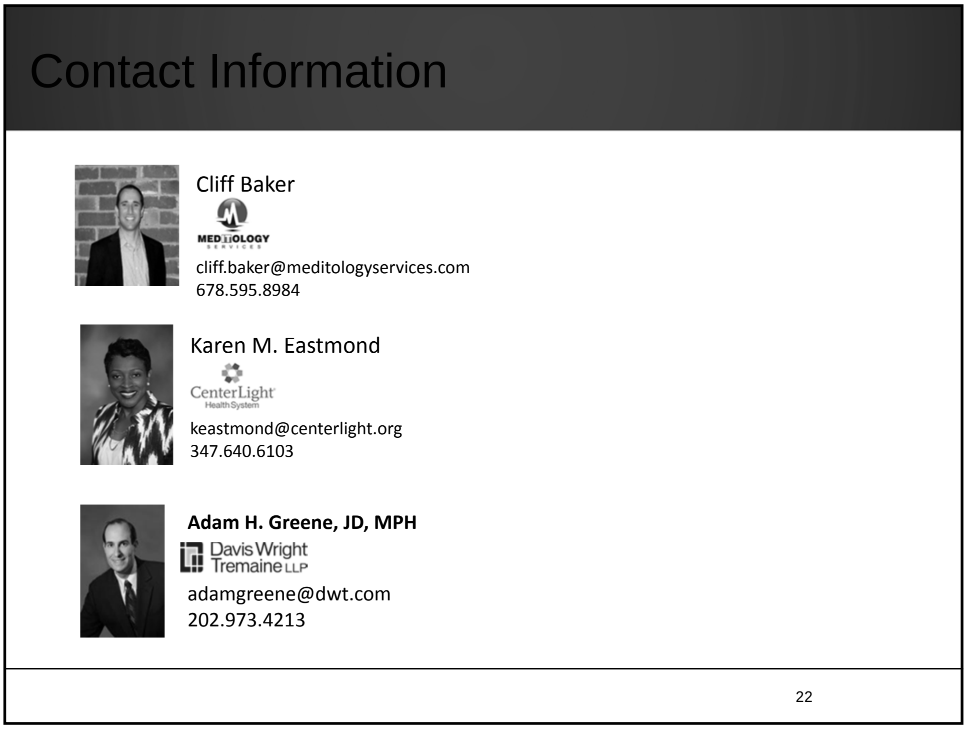


Final thoughts

- The corrective action plan should not become the security strategy
- The security strategy should encompass the corrective action plan
- Continue to update risk assessments and adjust priorities accordingly
- Fully leverage the moment to increase management’s attention and support

20

Questions?



Contact Information

Cliff Baker

MEDITOLOGY SERVICES

cliff.baker@meditologyservices.com
678.595.8984

Karen M. Eastmond

CenterLight Health System

keastmond@centerlight.org
347.640.6103

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213