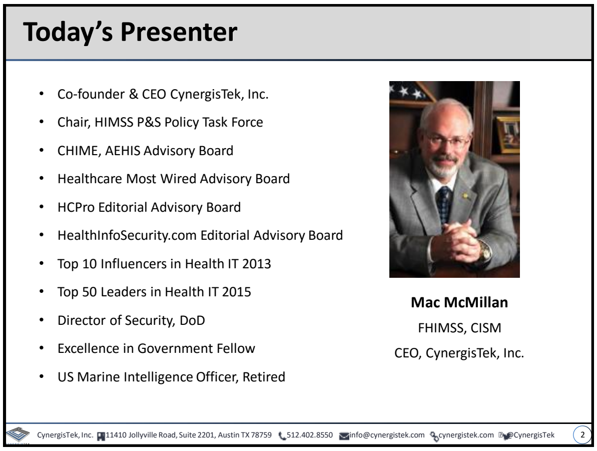
Cyber Forum Webinar

Presented by:
Mac McMillan
CEO, CynergisTek

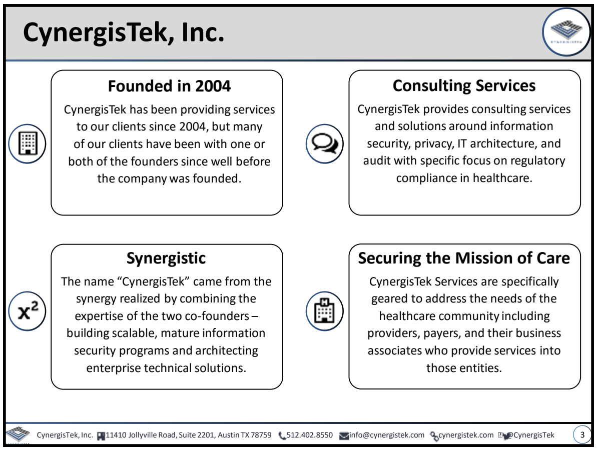
CYNERGISTEK



Today's Presenter

- Co-founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- CHIME, AEHIS Advisory Board
- Healthcare Most Wired Advisory Board
- HCPro Editorial Advisory Board
- HealthInfoSecurity.com Editorial Advisory Board
- Top 10 Influencers in Health IT 2013
- Top 50 Leaders in Health IT 2015
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired

Mac McMillan
FHIMSS, CISM
CEO, CynergisTek, Inc.



CynergisTek, Inc.

Founded in 2004

CynergisTek has been providing services to our clients since 2004, but many of our clients have been with one or both of the founders since well before the company was founded.

Consulting Services

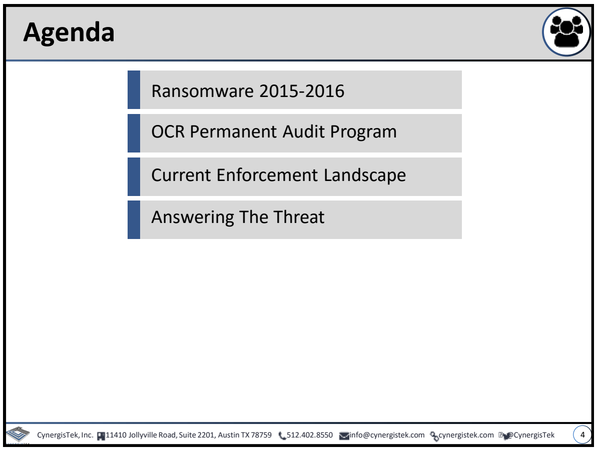
CynergisTek provides consulting services and solutions around information security, privacy, IT architecture, and audit with specific focus on regulatory compliance in healthcare.

Synergistic

The name "CynergisTek" came from the synergy realized by combining the expertise of the two co-founders – building scalable, mature information security programs and architecting enterprise technical solutions.

Securing the Mission of Care

CynergisTek Services are specifically geared to address the needs of the healthcare community including providers, payers, and their business associates who provide services into those entities.



Agenda

- Ransomware 2015-2016
- OCR Permanent Audit Program
- Current Enforcement Landscape
- Answering The Threat

Ransomware 2015/2016

Cybersecurity Incidents Rise

- Breaches in healthcare rose for the third straight quarter in 2016 with Q3 reporting 118 versus 89 and 63 in both the second and first quarters respectively.
- 32% of the breaches reported in Q3 involved hacking, including ransomware and other malware attacks.
- While insider attacks still outnumber hacking incidents, hacking continues to represent the highest number of records exposed.
- Ransomware attack volumes remain approximately 4000 a day, with 1000 new variants a day being identified.
- More than 80% of all ransomware attacks target healthcare.

The Stakes Are Higher

- Cyber extortion
- Cyber espionage
- Hacktivism
- Targeted attacks
- Cyber terrorism
- APTs & malware

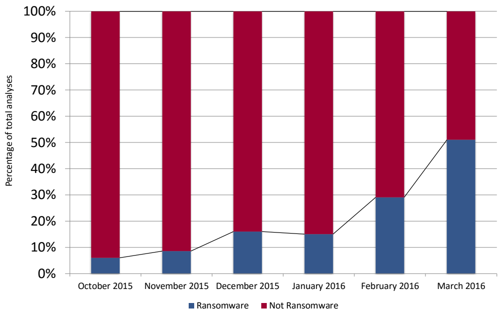
Motivated, Persistent & Disruptive

Cyber Extortion is Rampant

- Multiple Forms: Crypto ransomware (data) and Locker ransomware (system)
- Sophisticated attacks use:
  - New asymmetric keys for each infection
  - Industrial strength & private/public key encryption
  - Privacy enabling services like TOR and bitcoins for payments
- Indifferent to target, everyone is a target (home/business)
- Multiple extortion approaches
- Malvertising, spam email, downloaders/botnets & social engineering

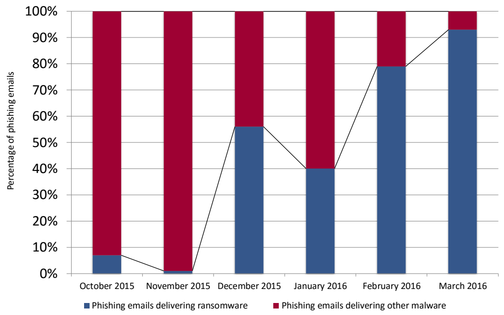
The United States is the largest target worldwide by a huge margin.
SOCs worldwide report as much as a 10X increase in ransomware attacks from December to January with no abatement.

Growth of Encryption Ransomware Against All Other Malware



Source: *PhishMe Q1 Malware Review*

Percentage of Phishing Emails Delivering Ransomware



Source: *PhishMe Q1 Malware Review*

Your Adversary Has Changed

655,000 health records for sale on the dark web (June 28, 2016)

“Next time an ADVERSARY comes to you and offers you an opportunity to cover this up and make it go away for a small fee to prevent the leak, take the offer. There is a lot more to come.”

9 million plus more health records online (June 30, 2016)

Healthcare HL7 Interoperability Software Source Code, Signing Keys & Licensing Database for sale (July 12, 2016)

“There will likely be two buyers for this, someone with nefarious intentions or someone from a small country wanting to use it for business.”

Responding to Cybersecurity Incidents

- Determine scope of incident to identify what networks, systems or applications are affected
- Determine the origination of the incident
  - Who/what/where/when
- Determine whether is incident is finished, ongoing or has propagated additional incidents throughout the environment
- Determine how the incident occurred
- Contain the impact and propagation of the ransomware
  - Tools and attacks methods used, vulnerabilities exploited
- Eradicate the instance of the ransomware

Should You Pay Ransom for Your Data?

- US Dept. of Justice Guidance on Ransomware says “No”
- Paying a ransom does not guarantee an organization will regain access to its data; in fact, some victims were never provided with decryption keys after paying ransom
- Some victims who paid the demand have reported being targeted again by cyber actors
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key
- Paying ransom could inadvertently encourage this criminal business model to continue

OCR Ransomeware Guidance

- Only two things you need to know:
  - A ransomware event is considered a breach, when someone or something takes control of your data and renders is unavailable (no matter for how long) you have been breached
  - Notification is tied to “compromise” not the event itself. If after investigation you find:
    - The manner in which the malware was deployed on your network involved physical access by the hacker, or
    - You data is rendered unavailable to you (you cannot recover) then you have been compromised

And They Saw Opportunity…

- A little initiative, a curious nature, a deviant behavior, a Bitcoin wallet, PGP for encrypted communication, and a TOR browser and you are in business…

Answering The Threat

Taking Back The Advantage

- ***Educate and inform***, ensure users know how to identify and avoid common threats
- ***Remain current***, refresh, harden, patch and manage system configurations with diligence
- ***Employ layers***, protections at the endpoint, network, file layers, etc. can make it more difficult for hackers
- ***Deploy complimentary controls***, use both signature or rule based solutions with heuristic solutions
- ***Enhance detection***, deploy NGFWs, malware filters, A/V filters, IDS/IPS, etc.
- ***Prioritize contingency planning***, back up everything, offline as well, practice incident response
- ***Be ready***, establish relationships, acquire tools
- ***Be objective***, use independent third parties to perform readiness audits, tests and assessments

Strengthening Your Defenses

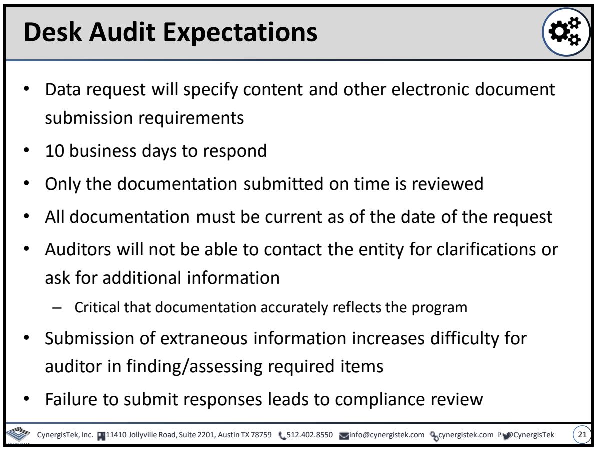
- ***Improve the perimeter:*** remote access connections, firewalls/UTM, IPS, web apps, sandboxing, SaaS & public/private clouds
- ***Focus on malware detection:*** secure email gateways and secure web gateways
- ***Reinforce endpoint detection:*** admin privileges, regular testing, anti-virus, anti-malware, host based IPS, include IoT devices
- ***Automate audit/monitoring:*** dedicated SOC, enhanced SIEM, behavioral analysis
- ***Step up IR capabilities:*** define process, train members, establish contacts, track & learn, share intelligence
- ***Threat deception:*** use technologies that deceive/divert, endpoints, applications, data, identity and infrastructure

With motivation, the right equipment, the right training and timely execution ***YOU*** can stop the threat.

OCR Permanent Audit Program

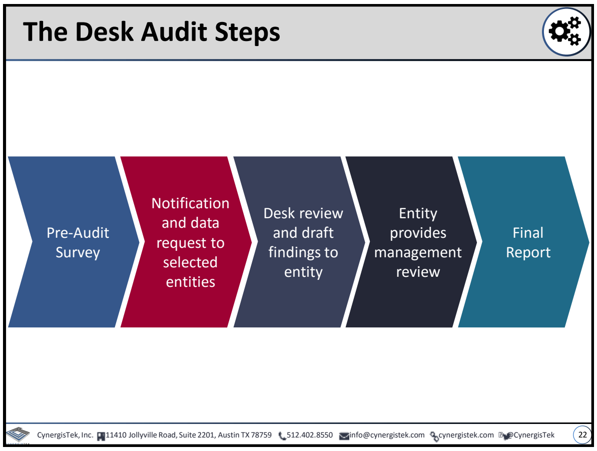
Today: OCR's Permanent Audit Program

- 14,000 covered entities catalogued about the services they provide, their size and who to contact for possible HIPAA audit
- 167 covered entities selected for desk audit
  - CEs queried on OCR compliance with Security Rule or Privacy/Breach Rules
  - All CEs to provide business associate names and contact information http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html
- Fall 2016: 40-50 business associates selected for desk audit
- Early 2017: Small number of onsite, comprehensive audits
- 2017: Will OCR use HIPAA $$ for larger audit program?



Desk Audit Expectations

- Data request will specify content and other electronic document submission requirements
- 10 business days to respond
- Only the documentation submitted on time is reviewed
- All documentation must be current as of the date of the request
- Auditors will not be able to contact the entity for clarifications or ask for additional information
  - Critical that documentation accurately reflects the program
- Submission of extraneous information increases difficulty for auditor in finding/assessing required items
- Failure to submit responses leads to compliance review



The Desk Audit Steps

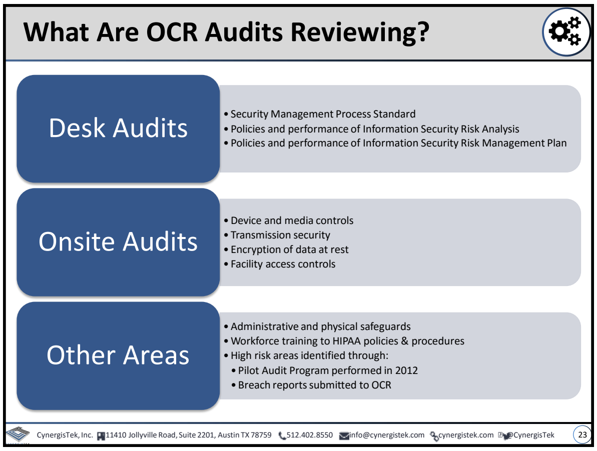
Pre-Audit Survey

Notification and data request to selected entities

Desk review and draft findings to entity

Entity provides management review

Final Report



What Are OCR Audits Reviewing?

Desk Audits

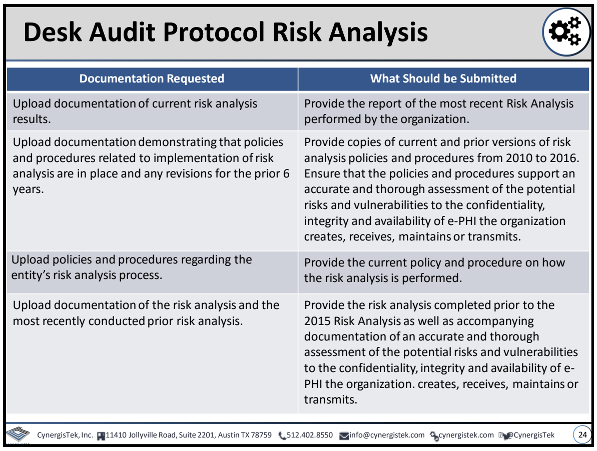
- Security Management Process Standard
- Policies and performance of Information Security Risk Analysis
- Policies and performance of Information Security Risk Management Plan

Onsite Audits

- Device and media controls
- Transmission security
- Encryption of data at rest
- Facility access controls

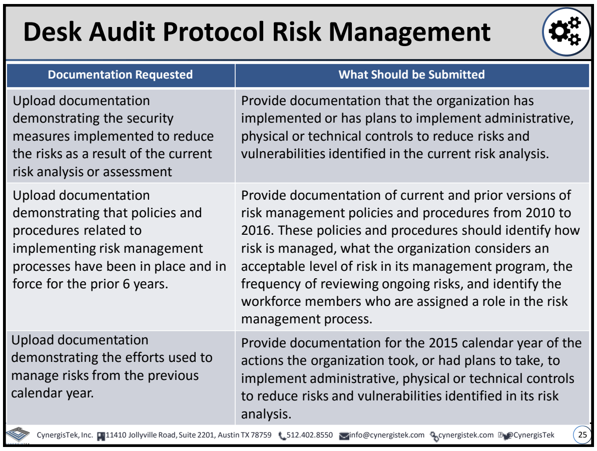
Other Areas

- Administrative and physical safeguards
- Workforce training to HIPAA policies & procedures
- High risk areas identified through:
  - Pilot Audit Program performed in 2012
  - Breach reports submitted to OCR



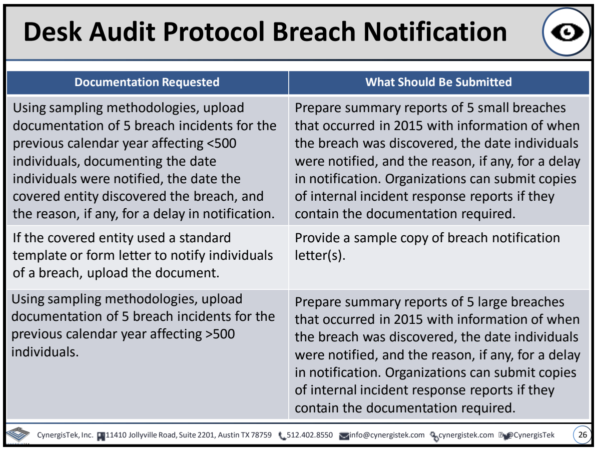
Desk Audit Protocol Risk Analysis

Documentation Requested	What Should be Submitted
Upload documentation of current risk analysis results.	Provide the report of the most recent Risk Analysis performed by the organization.
Upload documentation demonstrating that policies and procedures related to implementation of risk analysis are in place and any revisions for the prior 6 years.	Provide copies of current and prior versions of risk analysis policies and procedures from 2010 to 2016. Ensure that the policies and procedures support an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI the organization creates, receives, maintains or transmits.
Upload policies and procedures regarding the entity's risk analysis process.	Provide the current policy and procedure on how the risk analysis is performed.
Upload documentation of the risk analysis and the most recently conducted prior risk analysis.	Provide the risk analysis completed prior to the 2015 Risk Analysis as well as accompanying documentation of an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI the organization. creates, receives, maintains or transmits.



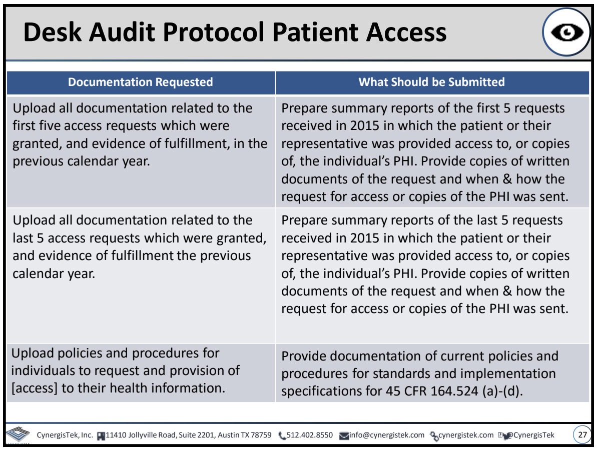
Desk Audit Protocol Risk Management

Documentation Requested	What Should be Submitted
Upload documentation demonstrating the security measures implemented to reduce the risks as a result of the current risk analysis or assessment	Provide documentation that the organization has implemented or has plans to implement administrative, physical or technical controls to reduce risks and vulnerabilities identified in the current risk analysis.
Upload documentation demonstrating that policies and procedures related to implementing risk management processes have been in place and in force for the prior 6 years.	Provide documentation of current and prior versions of risk management policies and procedures from 2010 to 2016. These policies and procedures should identify how risk is managed, what the organization considers an acceptable level of risk in its management program, the frequency of reviewing ongoing risks, and identify the workforce members who are assigned a role in the risk management process.
Upload documentation demonstrating the efforts used to manage risks from the previous calendar year.	Provide documentation for the 2015 calendar year of the actions the organization took, or had plans to take, to implement administrative, physical or technical controls to reduce risks and vulnerabilities identified in its risk analysis.



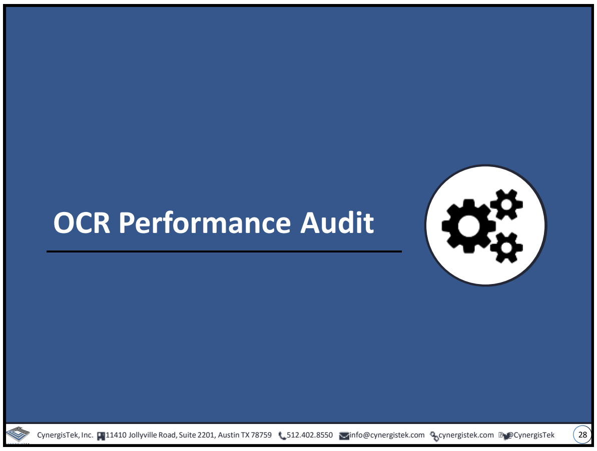
Desk Audit Protocol Breach Notification

Documentation Requested	What Should Be Submitted
Using sampling methodologies, upload documentation of 5 breach incidents for the previous calendar year affecting <500 individuals, documenting the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification.	Prepare summary reports of 5 small breaches that occurred in 2015 with information of when the breach was discovered, the date individuals were notified, and the reason, if any, for a delay in notification. Organizations can submit copies of internal incident response reports if they contain the documentation required.
If the covered entity used a standard template or form letter to notify individuals of a breach, upload the document.	Provide a sample copy of breach notification letter(s).
Using sampling methodologies, upload documentation of 5 breach incidents for the previous calendar year affecting >500 individuals.	Prepare summary reports of 5 large breaches that occurred in 2015 with information of when the breach was discovered, the date individuals were notified, and the reason, if any, for a delay in notification. Organizations can submit copies of internal incident response reports if they contain the documentation required.



Desk Audit Protocol Patient Access

Documentation Requested	What Should be Submitted
Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year.	Prepare summary reports of the first 5 requests received in 2015 in which the patient or their representative was provided access to, or copies of, the individual's PHI. Provide copies of written documents of the request and when & how the request for access or copies of the PHI was sent.
Upload all documentation related to the last 5 access requests which were granted, and evidence of fulfillment the previous calendar year.	Prepare summary reports of the last 5 requests received in 2015 in which the patient or their representative was provided access to, or copies of, the individual's PHI. Provide copies of written documents of the request and when & how the request for access or copies of the PHI was sent.
Upload policies and procedures for individuals to request and provision of [access] to their health information.	Provide documentation of current policies and procedures for standards and implementation specifications for 45 CFR 164.524 (a)-(d).

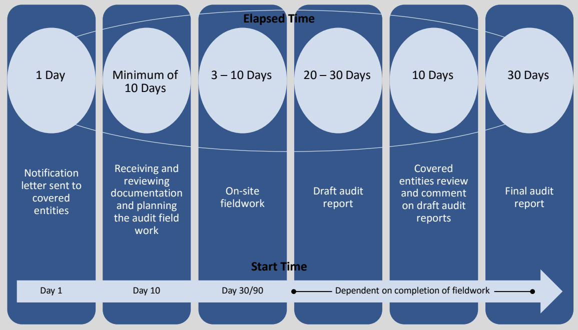


OCR Performance Audit

On-site Audits are Performance Audits

- Conducted in accordance with Generally Accepted Government Audit Standards (GAGAS)
- Provides findings, observations, or conclusions from evaluation of evidence against established criteria
- Objective assessment of variety of attributes
  - Program effectiveness, economy, and efficiency
  - Internal controls
  - Compliance

Audit Process



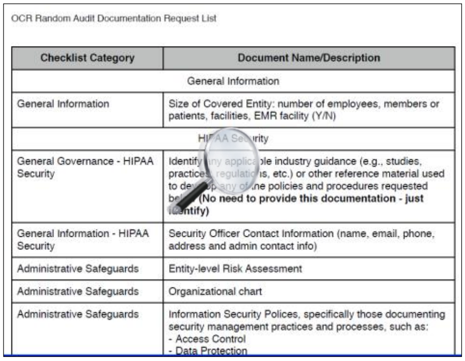
Elapsed Time

1 Day	Minimum of 10 Days	3 – 10 Days	20 – 30 Days	10 Days	30 Days
Notification letter sent to covered entities	Receiving and reviewing documentation and planning the audit field work	On-site fieldwork	Draft audit report	Covered entities review and comment on draft audit reports	Final audit report

Start Time

Day 1 — Day 10 — Day 30/90 — Dependent on completion of fieldwork

Documentation Request



OCR Random Audit Documentation Request List

Checklist Category	Document Name/Description
General Information	
General Information	Size of Covered Entity: number of employees, members or patients, facilities, EMR facility (Y/N)
HIPAA Security	
General Governance - HIPAA Security	Identify any applicable industry guidance (e.g., studies, practices, regulations, etc.) or other reference material used to develop any of the policies and procedures requested below **(No need to provide this documentation - just identify)**
General Information - HIPAA Security	Security Officer Contact Information (name, email, phone, address and admin contact info)
Administrative Safeguards	Entity-level Risk Assessment
Administrative Safeguards	Organizational chart
Administrative Safeguards	Information Security Polices, specifically those documenting security management practices and processes, such as: - Access Control - Data Protection

Provider/Health Plan Sample Audit Protocol

Breach Notification

- Assessment for breach
- Notification to individuals
- Notification to Secretary
- Notification to media

Privacy

- Notice of Privacy Practices
- Request Restrictions
- Right to Access
- Administrative Requirements
- Amendment
- Uses & Disclosures
- Accounting of Disclosures

Security

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Business Associate: Sample Audit Protocol

Breach Notification

- Assessment for breach
- Notification to Covered Entity

Privacy

- Uses & Disclosures
- Accounting of Disclosures

Security

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Prepare for OCR Audit

- Requirements for listing business associates
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html
- OCR's 2016 Audit Protocol
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html

Use OCR Desk Audit Protocol As Guide

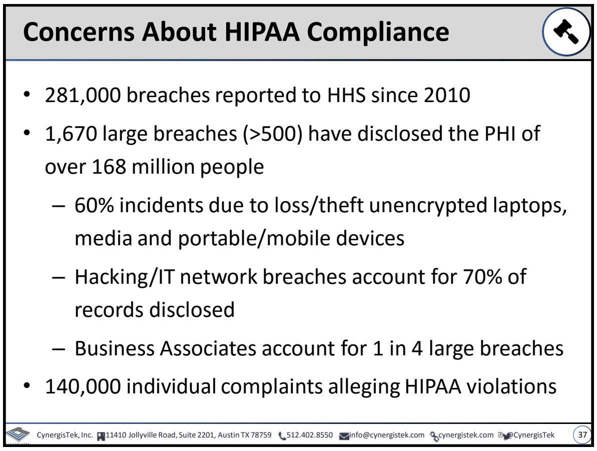
- Desk Audit Protocol & Document Request List

  http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

- OCR Desk Audit Introduction Webinar

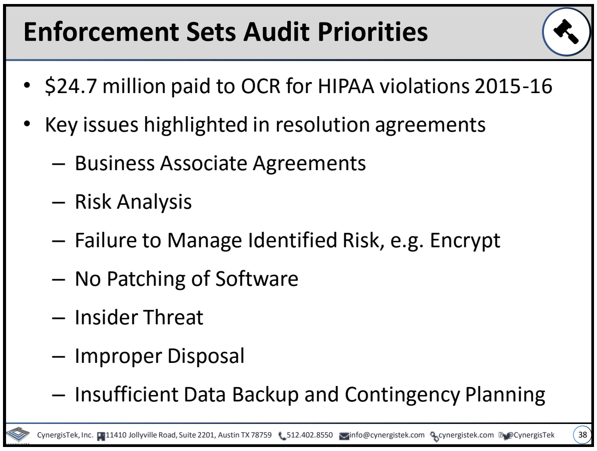
  http://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf

Current Enforcement Update



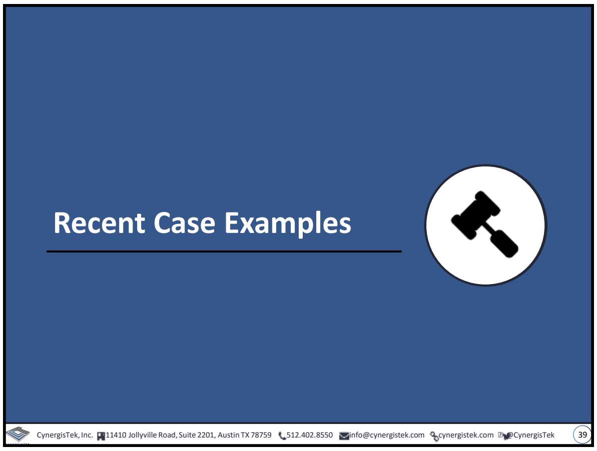
Concerns About HIPAA Compliance

- 281,000 breaches reported to HHS since 2010
- 1,670 large breaches (>500) have disclosed the PHI of over 168 million people
  - 60% incidents due to loss/theft unencrypted laptops, media and portable/mobile devices
  - Hacking/IT network breaches account for 70% of records disclosed
  - Business Associates account for 1 in 4 large breaches
- 140,000 individual complaints alleging HIPAA violations

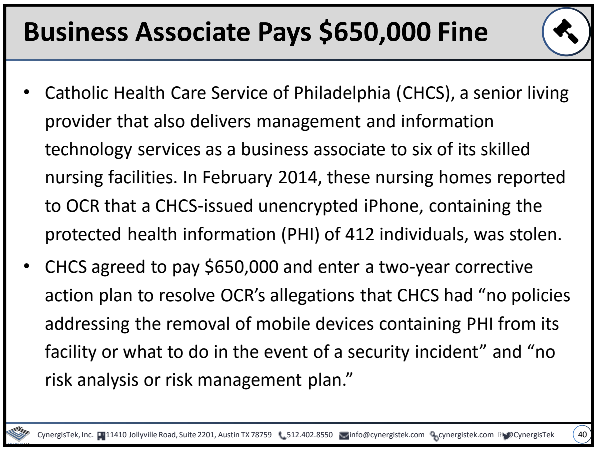


Enforcement Sets Audit Priorities

- $24.7 million paid to OCR for HIPAA violations 2015-16
- Key issues highlighted in resolution agreements
  - Business Associate Agreements
  - Risk Analysis
  - Failure to Manage Identified Risk, e.g. Encrypt
  - No Patching of Software
  - Insider Threat
  - Improper Disposal
  - Insufficient Data Backup and Contingency Planning

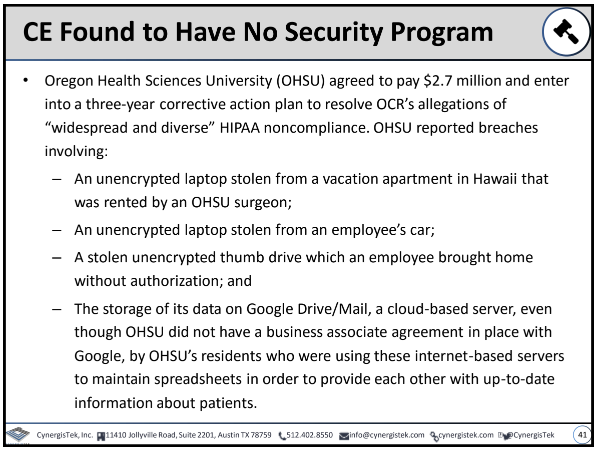


Recent Case Examples



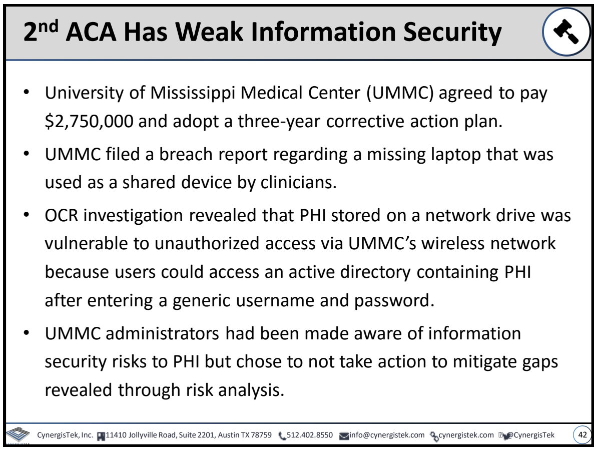
Business Associate Pays $650,000 Fine

- Catholic Health Care Service of Philadelphia (CHCS), a senior living provider that also delivers management and information technology services as a business associate to six of its skilled nursing facilities. In February 2014, these nursing homes reported to OCR that a CHCS-issued unencrypted iPhone, containing the protected health information (PHI) of 412 individuals, was stolen.
- CHCS agreed to pay $650,000 and enter a two-year corrective action plan to resolve OCR's allegations that CHCS had "no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident" and "no risk analysis or risk management plan."



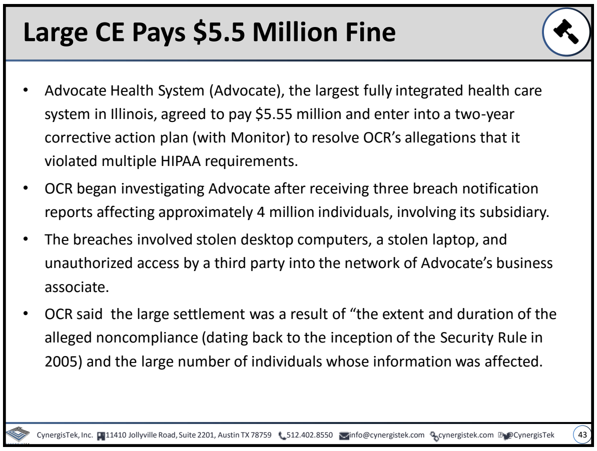
CE Found to Have No Security Program

- Oregon Health Sciences University (OHSU) agreed to pay $2.7 million and enter into a three-year corrective action plan to resolve OCR's allegations of "widespread and diverse" HIPAA noncompliance. OHSU reported breaches involving:
  - An unencrypted laptop stolen from a vacation apartment in Hawaii that was rented by an OHSU surgeon;
  - An unencrypted laptop stolen from an employee's car;
  - A stolen unencrypted thumb drive which an employee brought home without authorization; and
  - The storage of its data on Google Drive/Mail, a cloud-based server, even though OHSU did not have a business associate agreement in place with Google, by OHSU's residents who were using these internet-based servers to maintain spreadsheets in order to provide each other with up-to-date information about patients.



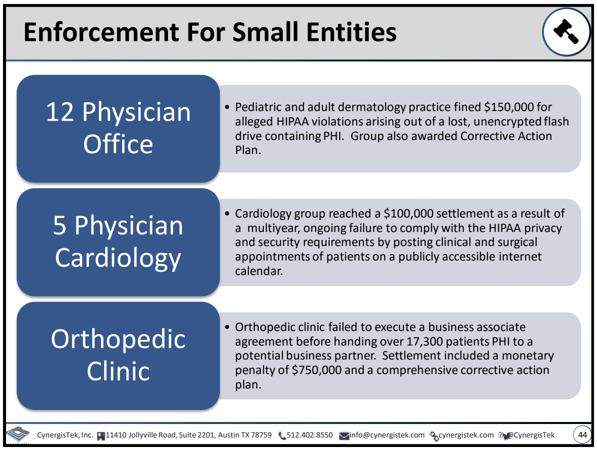
2nd ACA Has Weak Information Security

- University of Mississippi Medical Center (UMMC) agreed to pay $2,750,000 and adopt a three-year corrective action plan.
- UMMC filed a breach report regarding a missing laptop that was used as a shared device by clinicians.
- OCR investigation revealed that PHI stored on a network drive was vulnerable to unauthorized access via UMMC's wireless network because users could access an active directory containing PHI after entering a generic username and password.
- UMMC administrators had been made aware of information security risks to PHI but chose to not take action to mitigate gaps revealed through risk analysis.



Large CE Pays $5.5 Million Fine

- Advocate Health System (Advocate), the largest fully integrated health care system in Illinois, agreed to pay $5.55 million and enter into a two-year corrective action plan (with Monitor) to resolve OCR's allegations that it violated multiple HIPAA requirements.
- OCR began investigating Advocate after receiving three breach notification reports affecting approximately 4 million individuals, involving its subsidiary.
- The breaches involved stolen desktop computers, a stolen laptop, and unauthorized access by a third party into the network of Advocate's business associate.
- OCR said the large settlement was a result of "the extent and duration of the alleged noncompliance (dating back to the inception of the Security Rule in 2005) and the large number of individuals whose information was affected.



Enforcement For Small Entities

12 Physician Office

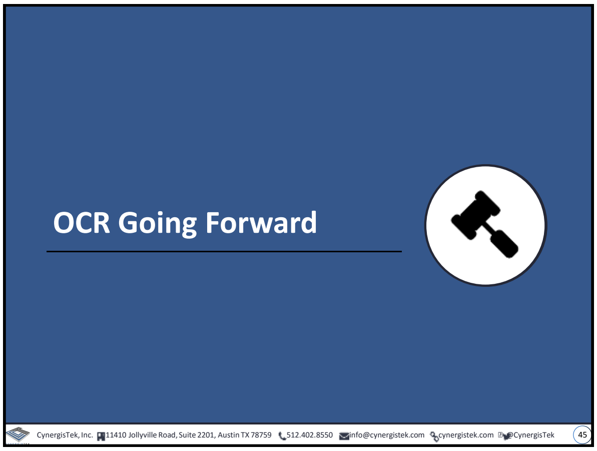
- Pediatric and adult dermatology practice fined $150,000 for alleged HIPAA violations arising out of a lost, unencrypted flash drive containing PHI. Group also awarded Corrective Action Plan.

5 Physician Cardiology

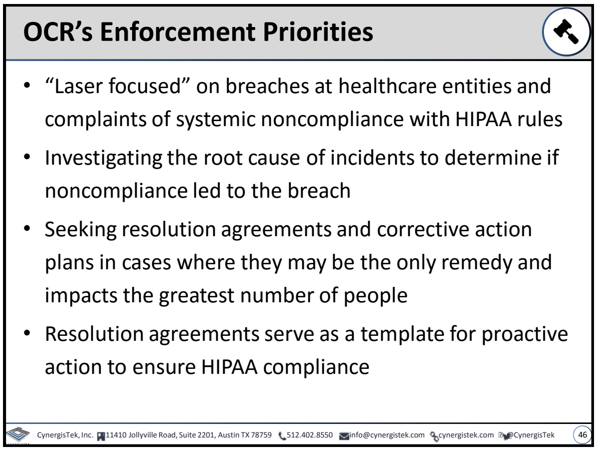
- Cardiology group reached a $100,000 settlement as a result of a multiyear, ongoing failure to comply with the HIPAA privacy and security requirements by posting clinical and surgical appointments of patients on a publicly accessible internet calendar.

Orthopedic Clinic

- Orthopedic clinic failed to execute a business associate agreement before handing over 17,300 patients PHI to a potential business partner. Settlement included a monetary penalty of $750,000 and a comprehensive corrective action plan.

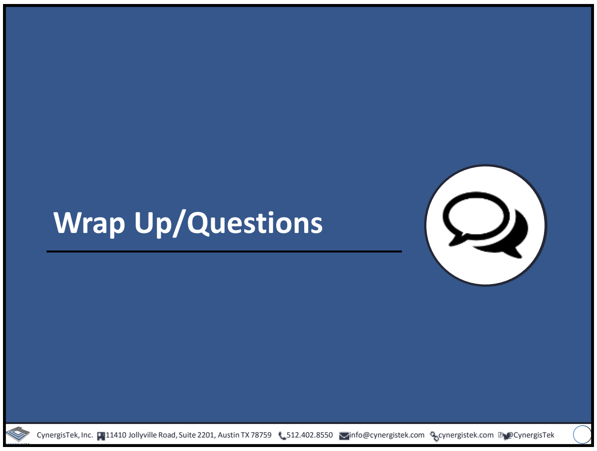


OCR Going Forward

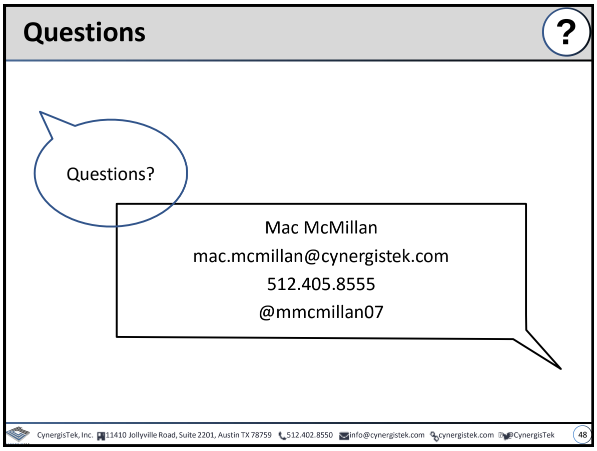


OCR's Enforcement Priorities

- "Laser focused" on breaches at healthcare entities and complaints of systemic noncompliance with HIPAA rules
- Investigating the root cause of incidents to determine if noncompliance led to the breach
- Seeking resolution agreements and corrective action plans in cases where they may be the only remedy and impacts the greatest number of people
- Resolution agreements serve as a template for proactive action to ensure HIPAA compliance



Wrap Up/Questions



Questions

Questions?

Mac McMillan
mac.mcmillan@cynergistek.com
512.405.8555
@mmcmillan07