KeepItSafe

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

HOW TO SAFEGUARD YOUR ePHI IN THE CLOUD

PRESENTERS

PATRICK ROUGEAU
Compliance Officer

KeepItSafe

MARC HASKELSON
President & CEO

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

KeepItSafe

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

AGENDA

Horror Story —
The $750,000 HIPAA Mistake

Recent HIPAA Trends —
and What They Mean for Your Business

What Does HIPAA Require?

How Does My Current Protection Level Measure Up to These Requirements?

How Do I Bridge the Gap?

The $750,000 HIPAA Mistake

University of Washington 2013 Breach

- ✓ *School of Medicine employee accidentally downloads **malware***
- ✓ *Health rec ords of 90,000 patients are **breached***
- ✓ *OCR investigates, discovers other **HIPAA Security Rule violations***
- ✓ *UW forced to pay **$750,000 in fines***

***Source:** Healthcare IT News*

Recent HIPAA Trends — and What They Mean for You

The 5 Leading HIPAA Violations

5. *Third-Party Disclosure*

4. *Improper Disposal*

3. *Employee Dishonesty*

2. *Hacking*

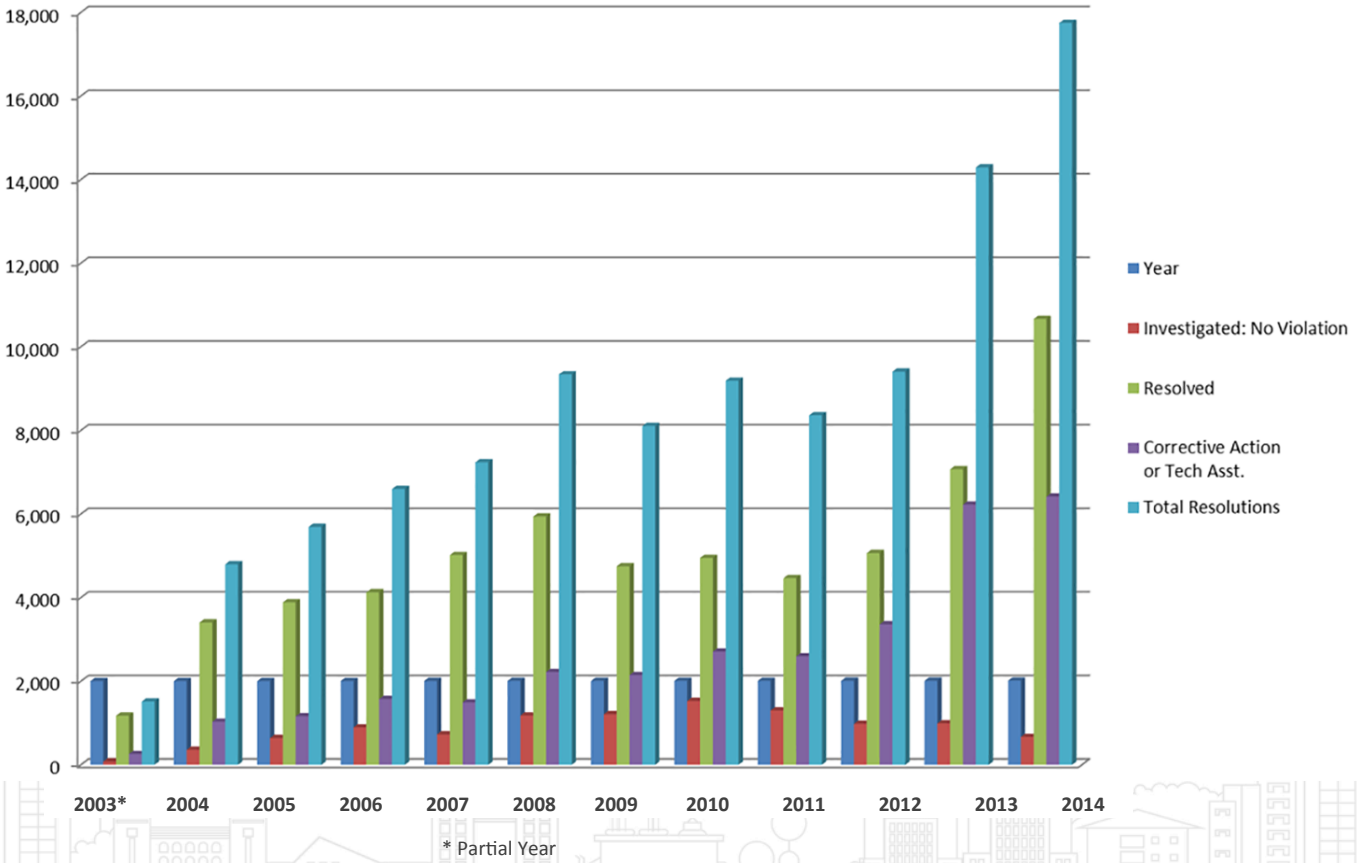
...

1. *Lost or Stolen Devices*

Source: *NueMD*

Recent HIPAA Trends — and What They Mean for You

Enforcement is on the Rise



* Partial Year

Source: *HHS.gov*

Recent HIPAA Trends — and What They Mean for You

2015: Biggest Year Ever for ePHI Breaches (and "Security Rule" Violations)

Top 10 Healthcare Data Breaches 2015

Organization	Records Breached	Type of Breach
Anthem	78,800,000	Hacking / IT Incident
PREMERA BLUE CROSS	11,000,000	Hacking / IT Incident
Excellus	10,000,000	Hacking / IT Incident
UCLA Health	4,500,000	Hacking / IT Incident
mie	3,900,000	Hacking / IT Incident
CareFirst	1,100,000	Hacking / IT Incident
DMAS	697,586	Hacking / IT Incident
Georgia Department of Community Health	557,779	Hacking / IT Incident
BEACON HEALTH SYSTEM	306,789	Hacking / IT Incident
DJO GLOBAL	160,000	Laptop Theft
2015 Total	111,022,154	(almost 35% U.S. population)

All potential violations of the HIPAA Security Rule

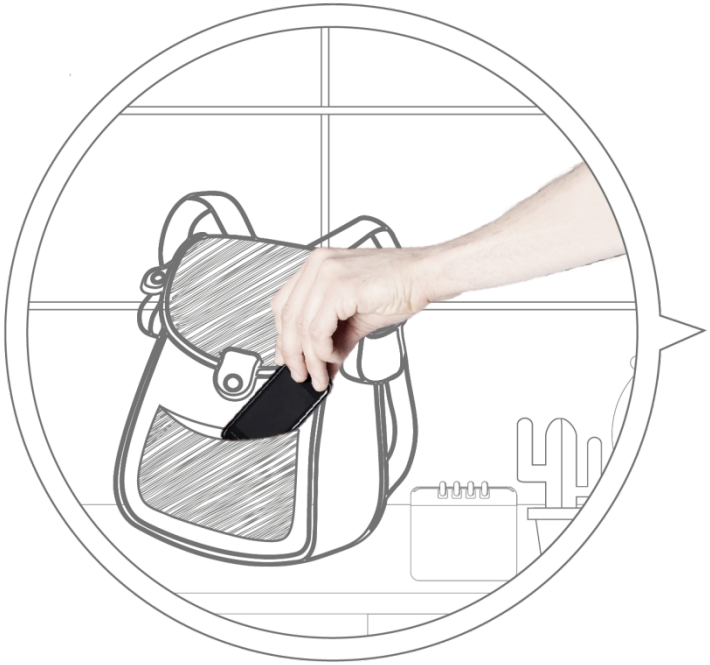
Source: *Forbes*

KeepItSafe

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Is Your ePHI in Violation… Here?

What if your physician accesses PHI on a device outside your firewall — and the data is hacked?



81%

of medical doctors use mobile devices to access ePHI such as patient records.

40%

of HIPAA violations involve lost or stolen mobile devices.

Source: *American Bar Association*

What Does HIPAA Actually Require?

Technical Safeguards

- ✓ *Have I established and implemented procedures to create and maintain retrievable exact copies of ePHI?*
- ✓ *Have I established procedures to restore ANY loss of ePHI stored electronically?*
- ✓ *Have I implemented a mechanism to encrypt ePHI?*

What Does HIPAA Actually Require?

Physical Safeguards

- ✓ *Is my data securely stored in an offsite location?*
- ✓ *Have I implemented policies and procedures to restrict access to ePHI*
- ✓ *Have I limited physical access to electronic information systems at the facilities my ePHI is being housed?*
- ✓ *Have I implemented procedures to securely terminate ePHI – both electronic and physical*

What Does HIPAA Actually Require?

Administrative Safeguards

- ✓ *Have I conducted a risk analysis to expose potential security violations*
- ✓ *Have I established procedures to enable business continuity in the event of an emergency?*
- ✓ *Have I implemented procedures for periodic testing and revision of my continuity plan?*

How Does My Current Protection Level Measure Up?

Define the Scope of Your Audit

What are security parameters?

- *Where is my ePHI data located?*
- *Who has access to it?*
- *Can I track potential IT incidents?*
- *Are my employees trained?*
- *Have I undertaken a risk analysis?*
-
-

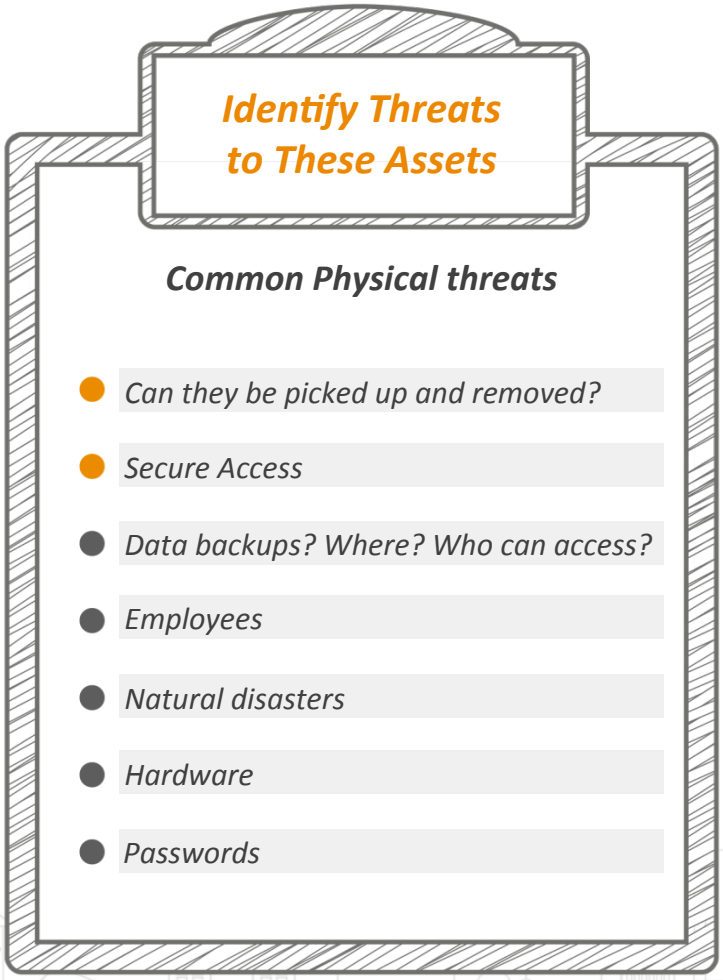
How Does My Current Protection Level Measure Up?

Define the Scope of Your Audit

What assets store or access ePHI?

- *Desktops and laptops*
- *Servers*
- *External hard drives*
- *Cloud applications (like Office 365)*
- *Company phones*
- *Emails*
- *Business associates*

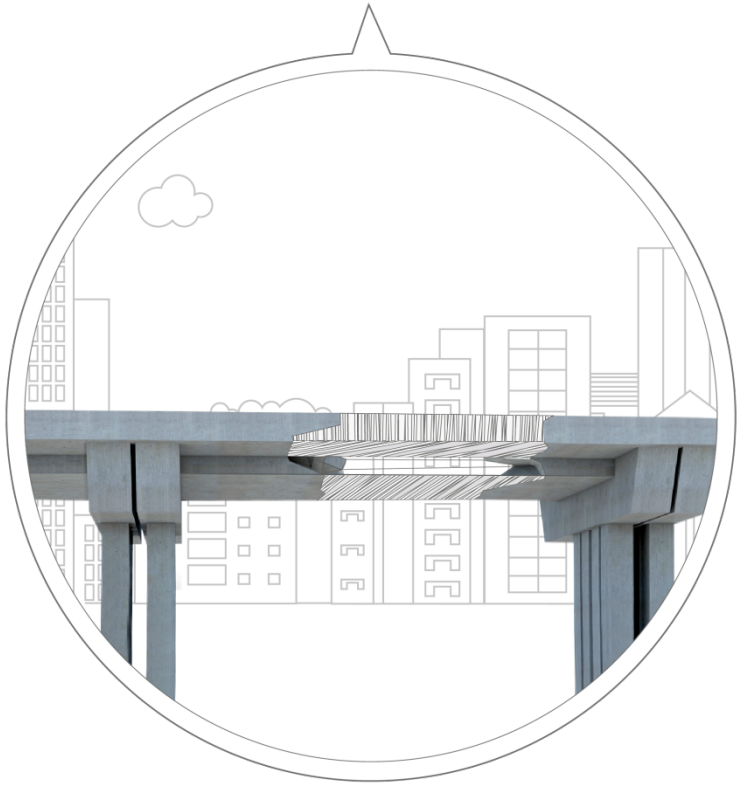
How Does My Current Protection Level Measure Up?



How Does My Current Protection Level Measure Up?

Bridging the Gap

From your current protection level…

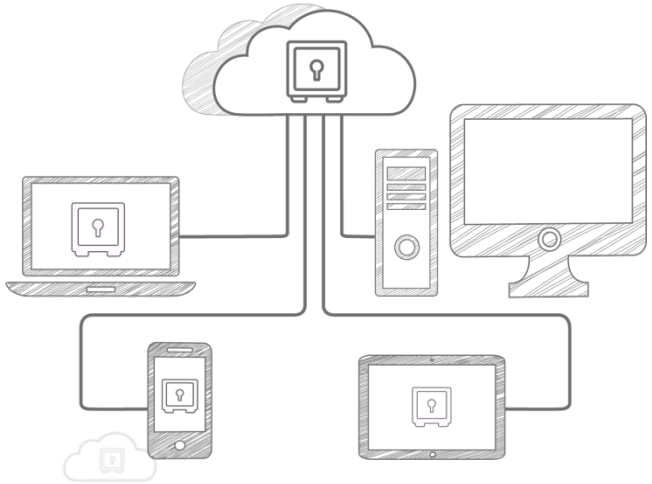


to HIPAA compliance.

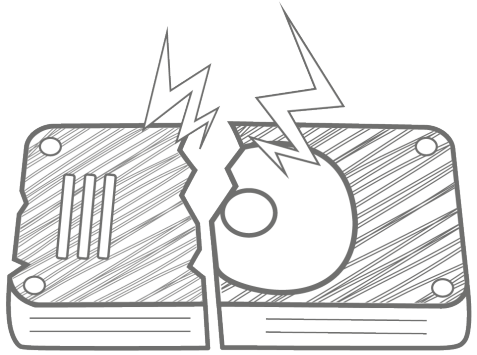
1. Develop Contingency Operations

Develop Contingency Operations

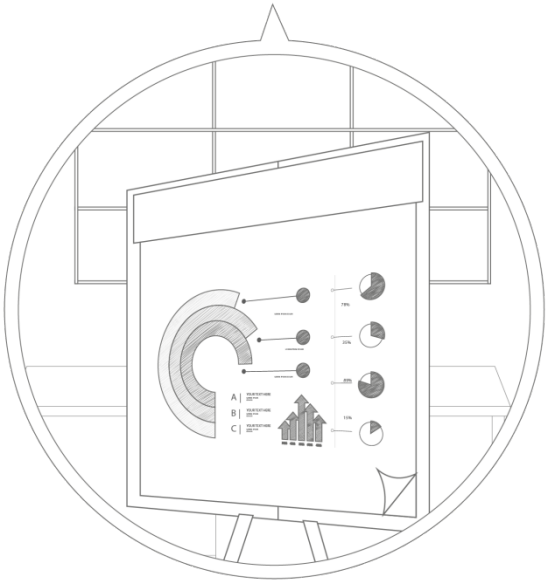
Cloud Backup



Tapes & Disks



2. Develop a Business Continuity Plan



3. Encrypt Your Data

Both in flight and at rest.

HIPAA Security Rule:
45 CFR § 164.304

NIST encryption standards for ePHI in motion…

NIST encryption standards for ePHI at rest…

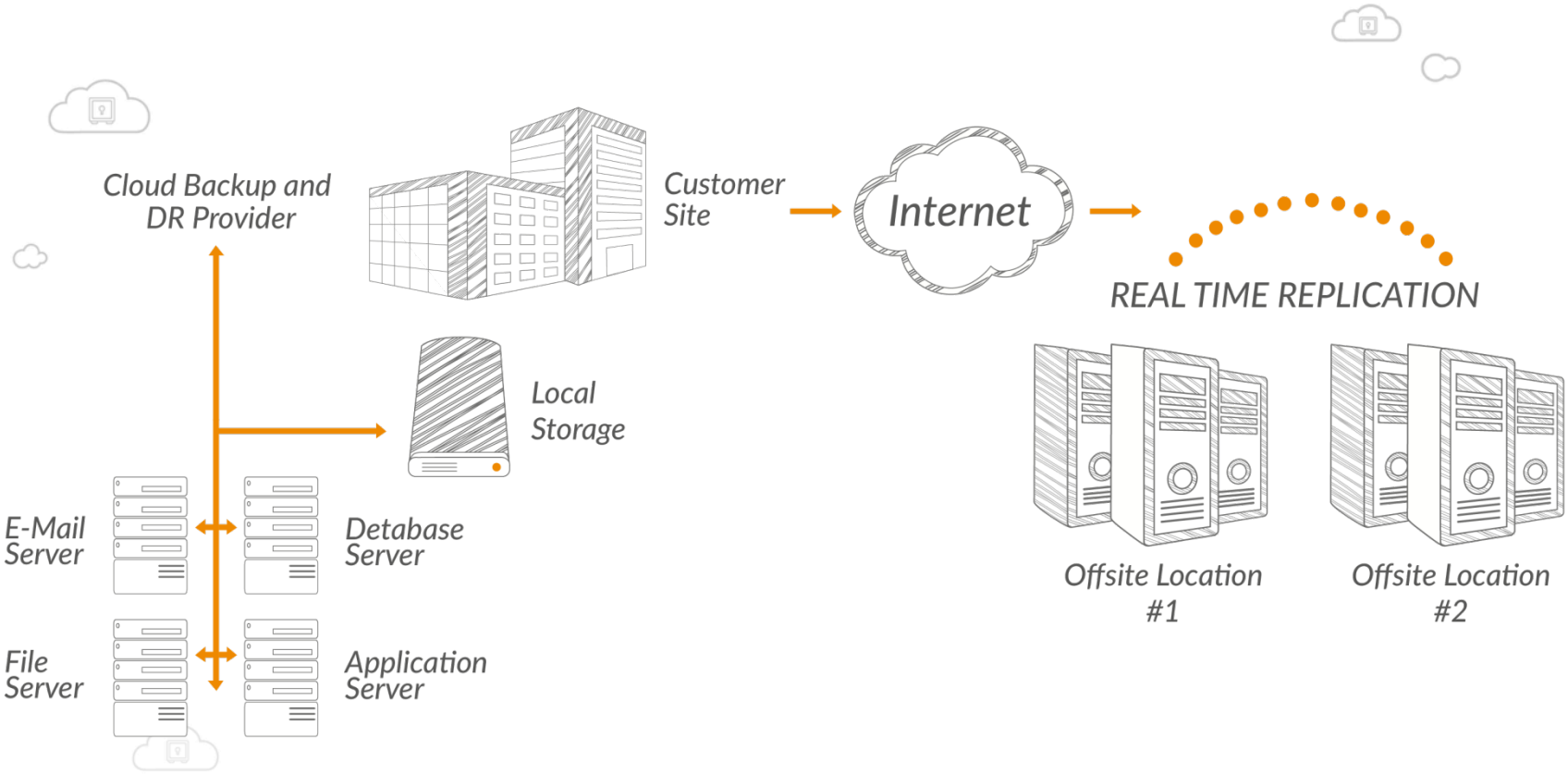
"… requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."

TLS encryption

AES 256-bit encryption

Source: *National Institute of Science and Technology*

4. Use Vendors With Dependable Infrastructure



- ✓ Facility Security Plan
- ✓ Secure Data Centers
- ✓ Access Control

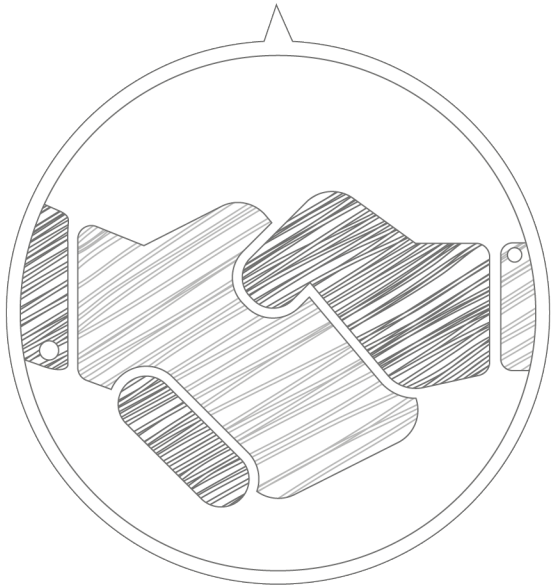
Source: National Institute of Science and Technology

5. Ensure You're Properly Disposing of ePHI

Security implications & HIPAA-compliance implications

6. Identify the Right Business Associates

Not just any BA — but the right one.



30%

of ePHI breaches are the fault of a Business Associate.

Source: *Ponemon Institute, Third Annual Benchmark Study on Patient Privacy & Data Security*

KeepItSafe

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Don’t Take on the ePHI Risk Alone…

Trust the Experts

Technical Safeguards

ISO-27001 Certification
256-AES Encryption
Endpoint Encryption

Physical Safeguards

Redundant tier-4 data centers
Secured in the cloud
24/7 live support

Administrative Safeguards

Business Associate Agreements
Fully Managed and Monitored
Policies and Procedures Dedicated to ePHI


?
Q
&
&
A
!

KeepItSafe

Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Compliance Questions?
For more information, contact:

Securing Your ePHI in the cloud

PATRICK ROUGEAU

646-747-0556
patrick.rougeau@keepitsafe.com

Achieve HIPAA Compliance Today!

MARC HASKELSON

855-854-4722 ext 507
marc@compliancygroup.com