



# Medical records and default passwords

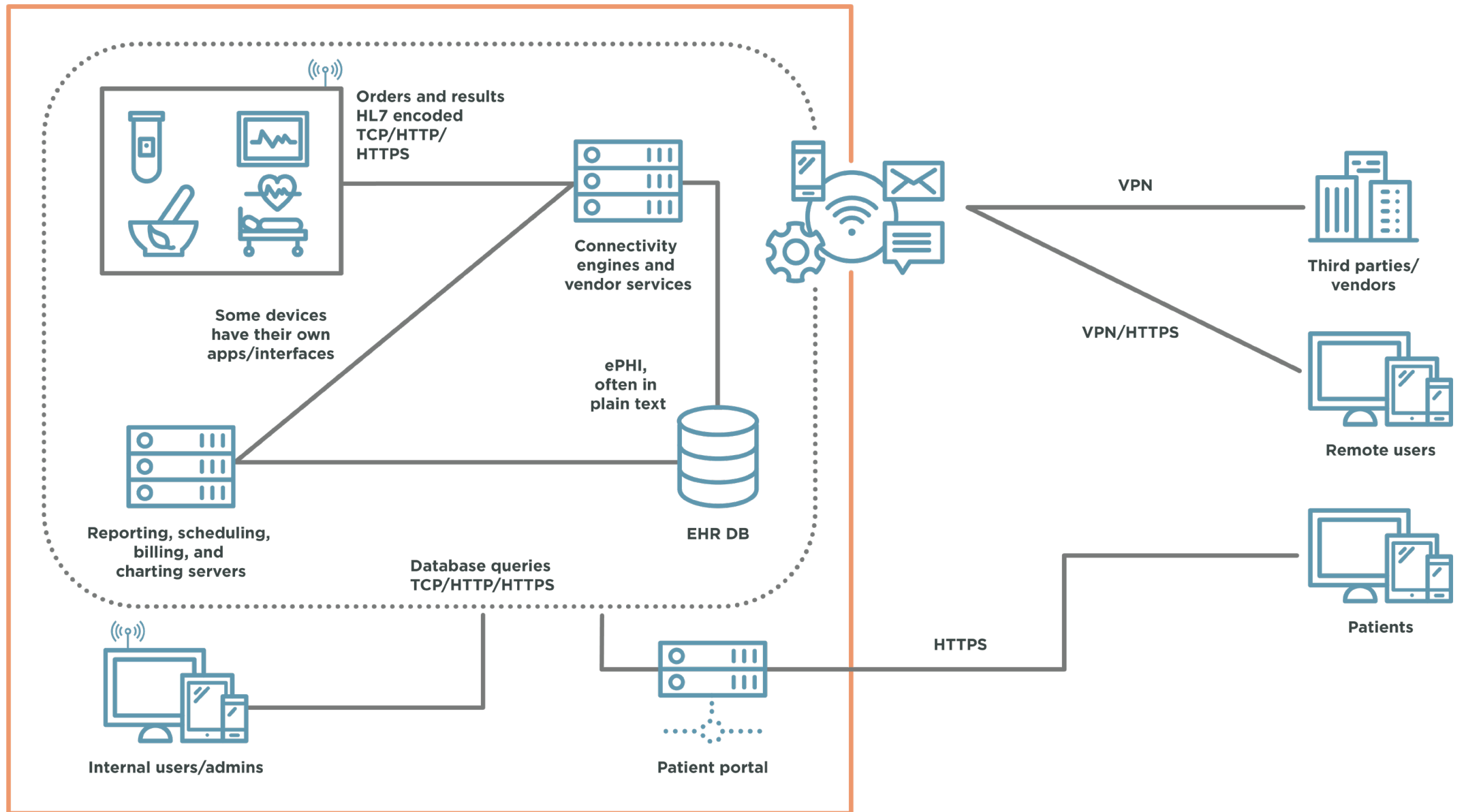
A healthcare hacker's perspective

*Qasim "Q" Ijaz*

# \$ whoami

- Qasim / “Q”
- Director of penetration testing at Coalfire Labs
- “Adaptive penetration testing” instructor at BlackHat U.S. and Europe
- Hundreds of penetration tests, largely focused on healthcare clients
  - As well as tens of HIPAA and HITRUST assessments
- Systems Engineer at an EHR company in my previous life
- <https://twitter.com/hashtaginfosec>

# Healthcare IT overview



# Electronic medical record (EMR)

Handy patients enterprise edition

File Edit View Help

David (8 month and 10 day John (2 years and 3 month)

Mother: Teacher  
Father: Financial advisor  
Parents: Married

Last: Anderson P  
First: David Boy  
Birth: 5 January 2009  
Age: 8 month and 10 days Patient nb: 3

Appointments

Forms

- Meeting (Doctor)
- Full status (Doctor)
- Assistant
- Billing
- Reports
- Statistics

SOAP Sum. T  
R-V T, P, PC  
Admission Agenda

Sheets

- O: Neurologic
- O: Vascular
- O: Cardiac
- O: Respiratory
- O: Abdomen
- Exams
- Radiology
- Summary
- Patient documents
- Letter

Meetings

2 month checkup	5 Mar 09	2m.0d
1 month checkup	5 Feb 09	1m.0d
Respiration problem	22 Jan 09	17d
10 days checkup	13 Jan 09	8d
Control for return at home	9 Jan 09	4d
Birth	5 Jan 09	0d

Diagnosis

General  
My Diagnosis  
Social

New documents

- Abdomen palpat - 15 Sep 2009
- Cardiac auscul - 15 Sep 2009

To do

Send checkup

Assist: 1 Doc: 0

Notes

Father ask many questions, add 10 minutes to consultation

Current doctor: Dr Herman

Menu 1 Menu 2 Menu 3 Search

## Digestive

Thursday, 22 Jan 2009

Digestive inspection

Normal

Digestive auscultation

Normal abdomen noises

Digestive palpation

Little pain on the right lower area

Liver

No hepatomegaly.

Rectal

Page 1/1

Draw ☒  
Mark ☐  
Color   
Pen   
8

Documents manager

Previous page Next page



# HL7: MITM's heaven

Wireshark · Packet 4 · HL7-ADT.pcap

```
TCP payload (477 bytes)
▼ Health Level Seven, Type: Admit Discharge Transfer, Event: Admit/visit notification
  ▼ MSH (Message Header)
    field 1: MSH
    field 2: ^~\&
    field 3: SENDING_APPLICATION
    field 4: SENDING_FACILITY
    field 5: RECEIVING_APPLICATION
    field 6: RECEIVING_FACILITY
    field 7: 20110613083617
    field 9: ADT^A01
    field 10: 934576120110613083617
    field 11: P
    field 12: 2.3
  ▼ EVN (Event Type)
    field 1: EVN
    field 2: A01
    field 3: 20110613083617
  ▼ PID (Patient Identification)
    field 1: PID
    field 2: 1
    field 4: 135769
    field 6: MOUSE^MICKEY^
    field 8: 19281118
    field 9: M
    field 12: 123 Main St.^Lake Buena Vista^FL ^32830
    field 14: (407)939-5555^^^ohtoodles@notdisney.com
    field 19: 1719
```

Patient name

DOB

Address

Phone and email

See

<https://www.linuxincluded.com/hl7-medical-fundamental-flaw/>



# Healthcare defaults

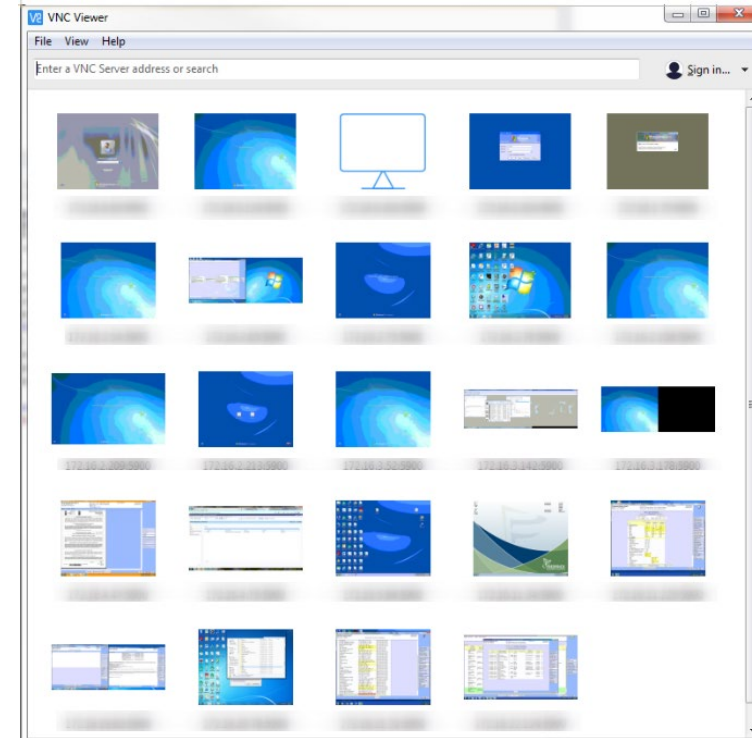
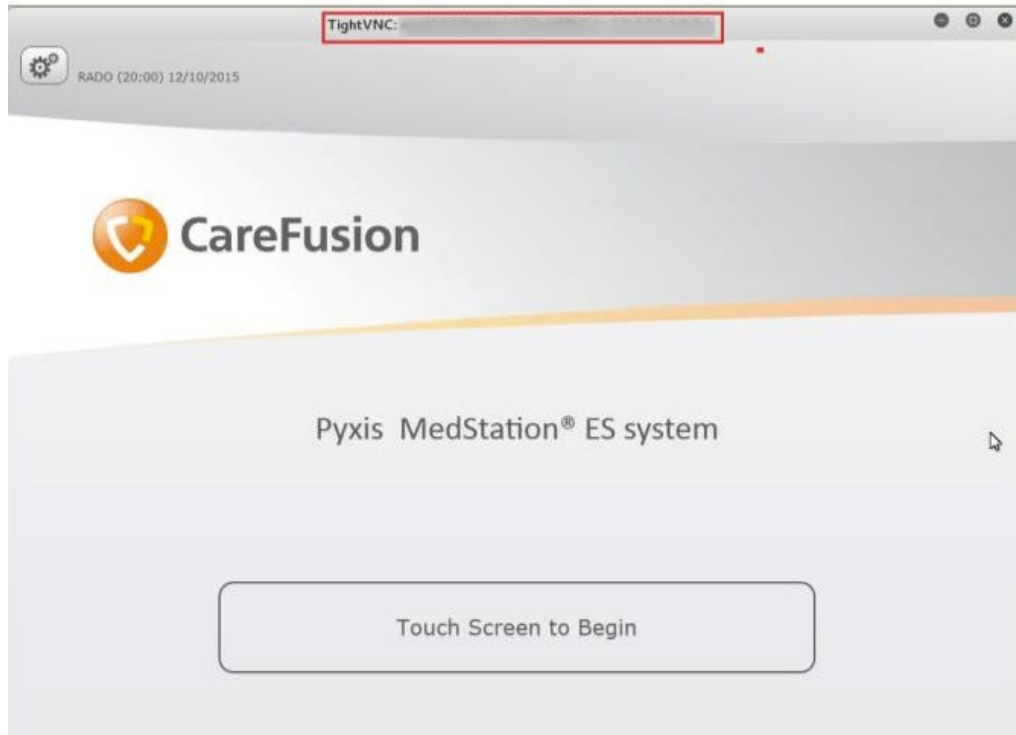
Because nobody would read the manual (or Google)

```
root@Kali:~/coalfire# crackmapexec 10.17.0.30 -u MuseAdmin -p [REDACTED]
CME 10.17.0.30:445 Muse [*] Windows 6.1 Build 7601 (name:Muse) (
CME 10.17.0.30:445 Muse [+] Muse\MuseAdmin [REDACTED] (Pwn3d!)
```

- If it's a hospital, start with the following AD accounts:
  - Museadmin
  - museBkgnd
- Often, vendors are responsible for configuration
  - And they leave defaults as is
- [https://www.cvedetails.com/vulnerability-list/vendor\\_id-15545/year-2015/Gehealthcare.html](https://www.cvedetails.com/vulnerability-list/vendor_id-15545/year-2015/Gehealthcare.html)
- Other defaults: <https://www.slideshare.net/Shakacon/medical-devices-passwords-to-pwnage-by-scott-erven>



# Unauthenticated VNC



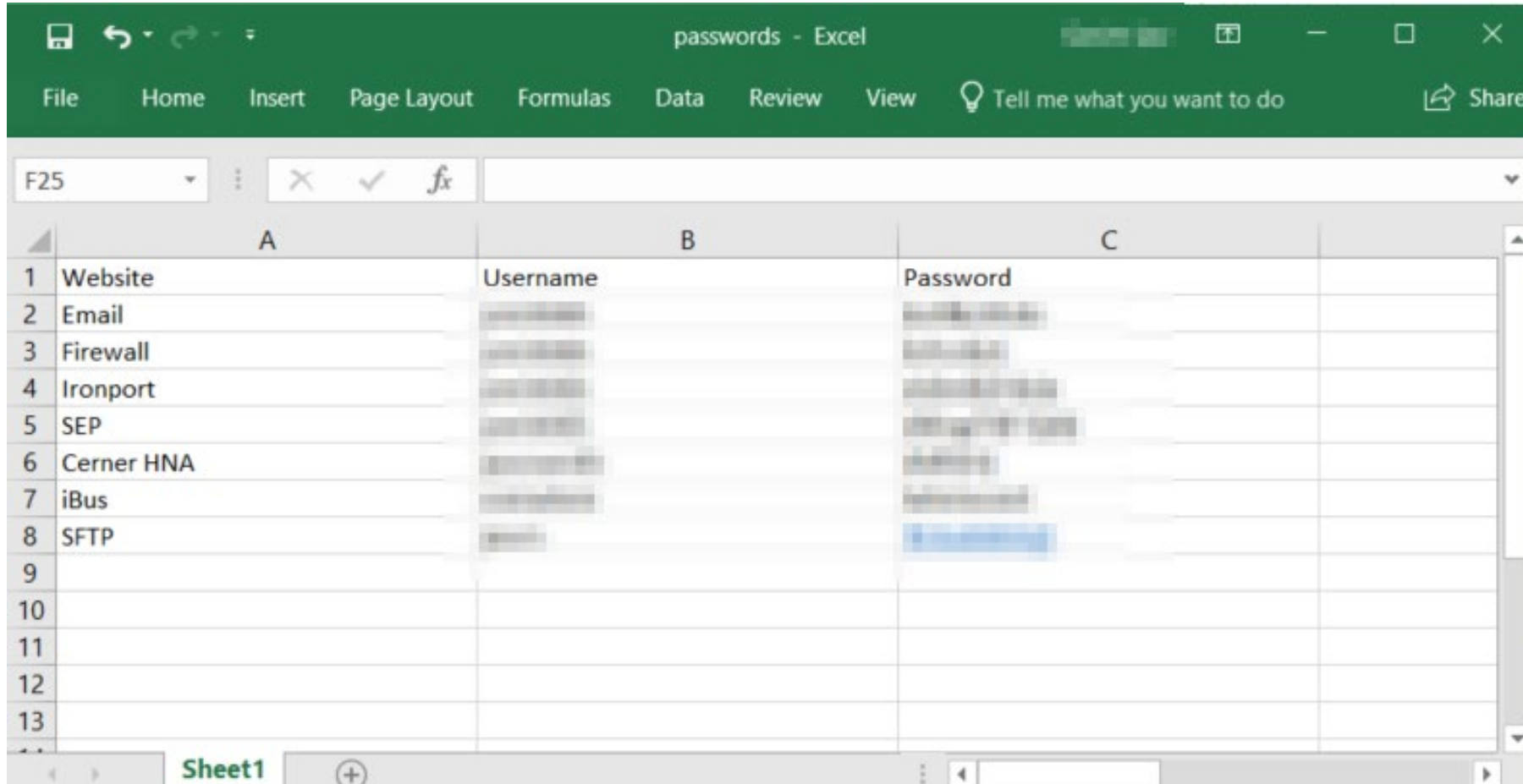
# Unauthenticated access to ePHI

```
|root@[REDACTED] patient]# zcat patient.*.gz| wc -l
13797281142
[2019-04-22|11:23:25|EDT [REDACTED] %eth0 172.23.69.206|
|root@[REDACTED] patient]# ls patient.*.gz| wc -l
8186
```

[illegible]

PATIENT NAME POLICY NBR BTH DTE IN CARE OF	SEX R/C TYPE	DRUG NAME NDC NBR ST CODE MANUF	RX NBR RX DATE QTY D/S PRIOR AUTH	DOCTOR DR NO D-TYPE	COST	FEE	TAX	TOTAL	CO-PAY	BALANCE
	1	FOLGARD RX 2.2MG 00245-0016-11 UPSH	NEW-00) 30		21.83	.00	.00	21.83	7.50	14.33
	1	ALTACE 5MG CAPSULE 61570-0112-01 HMR	NEW-00) 30		72.35	.00	.00	72.35	18.09	54.26
	1	AMOXICILLIN 250MG 00093-3107-05 TEVA	NEW-00) 25		3.68	.00	.00	3.68	3.68	.00
	2	ALBUTEROL ORAL INH 00172-4390-18 IVXE	NEW-00) 8		4.33	.68	.00	5.01	.00	5.01
	2	GUAFENEX-DM E.R. 58177-0213-04 ETHEX	NEW-00) 30		4.12	.66	.00	4.78	.00	4.78
	1	SPIRIVA 18MCG ORAL 00597-0075-37 PFIZE	NEW-00) 15		92.56	9.51	.00	102.07	.00	102.07

# Who needs a password manager anyway?



The screenshot shows an Excel spreadsheet with the following data:

	A	B	C
1	Website	Username	Password
2	Email	[Redacted]	[Redacted]
3	Firewall	[Redacted]	[Redacted]
4	Ironport	[Redacted]	[Redacted]
5	SEP	[Redacted]	[Redacted]
6	Cerner HNA	[Redacted]	[Redacted]
7	iBus	[Redacted]	[Redacted]
8	SFTP	[Redacted]	[Redacted]
9			
10			
11			
12			
13			

# OCR breach portal

Because numbers don't lie

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	American Medical Response, Inc.	TX	Healthcare Provider	4300	05/06/2019	Hacking/IT Incident	Email
	Inspira Behavioral Care, Corp		Healthcare Provider	4246	05/02/2019	Theft	Desktop Computer
	The Southeastern Council on Alcoholism and Drug Dependence	CT	Healthcare Provider	25148	05/01/2019	Hacking/IT Incident	Network Server
	AA OBGYN PLLC	TX	Healthcare Provider	930	04/30/2019	Unauthorized Access/Disclosure	Other
	Partners In Care	OR	Healthcare Provider	3048	04/26/2019	Hacking/IT Incident	Email
	Medical Oncology Hematology Consultants, PA	DE	Healthcare Provider	8591	04/26/2019	Hacking/IT Incident	Email
	Health Care Service Corporation	IL	Health Plan	676	04/24/2019	Unauthorized Access/Disclosure	Other Portable Electronic Device
	Doctors Management Services, Inc.	MA	Business Associate	206695	04/22/2019	Hacking/IT Incident	Network Server
	LISA ROSE DURSO, M.D. PLLC	NY	Healthcare Provider	537	04/22/2019	Hacking/IT Incident	Network Server
	Area Agency on Aging and Disabilities of Southwest Washington	WA	Health Plan	7000	04/22/2019	Unauthorized Access/Disclosure	Email
	EmCare, Inc.	FL	Healthcare Provider	31236	04/20/2019	Hacking/IT Incident	Email
	Bodybuilding.com LLC, operated by Vitalize, LLC ("Vitalize, LLC")	ID	Health Plan	3193	04/19/2019	Unauthorized Access/Disclosure	Network Server
	Blue Cross of Idaho Health Service, Inc.	ID	Health Plan	6045	04/19/2019	Unauthorized Access/Disclosure	Other
	Partners For Quality, Inc.	PA	Healthcare Provider	3673	04/19/2019	Hacking/IT Incident	Email
	KIM P. KORNEGAY, DMD	AL	Healthcare Provider	27000	04/19/2019	Theft	Desktop Computer, Electronic Medical Record, Paper/Films

[https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

**WHAT DO WE**

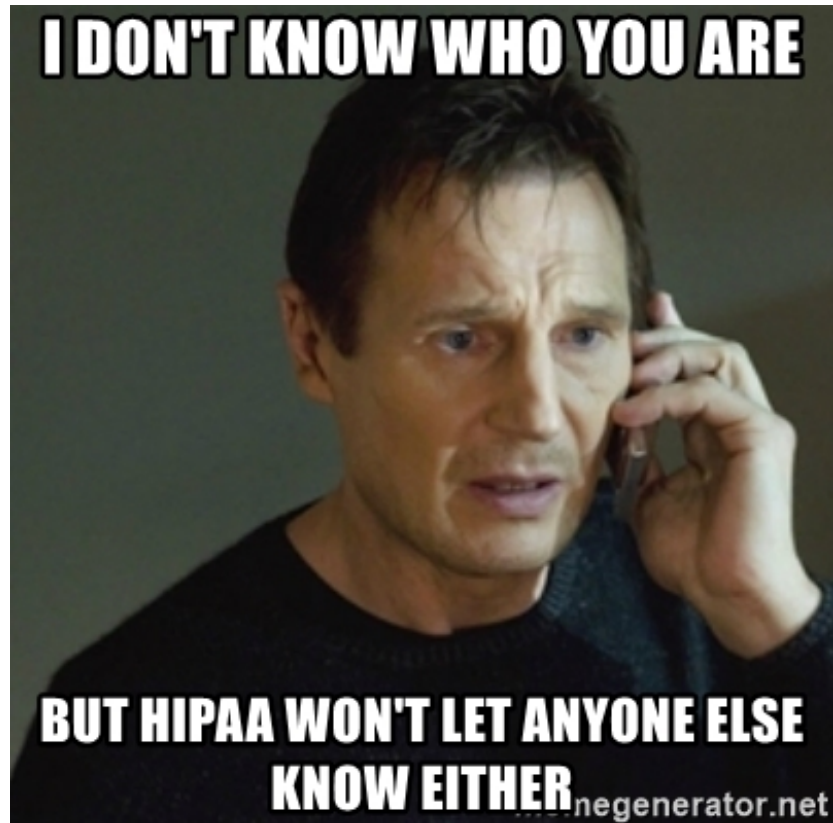


**DO NOW?**

memegenerator.net



# There's HIPAA



# Health Insurance Portability and Accountability Act

- **HIPAA Security Rule requires implementation of safeguards:**
  - Organizational policies and procedures
  - Administrative safeguards (e.g., access management and evaluation of safeguards)
  - Physical safeguards such as physical access controls
  - Technical implementation (e.g., encryption and authentication)
  - Risk analysis and management of risk
- **Conduct penetration testing, if reasonable and appropriate**  
(Evaluation (§ 164.308(a)(8)))



# HITRUST framework

Because HIPAA certified isn't a thing

- **Based on ISO 27002 and incorporates other relevant information security assessment frameworks, such as NIST RMF, HIPAA, FedRAMP, and PCI DSS**
- **Three levels of requirements**
- **Requirements for policy (25%), procedure (25%), implementation (25%), measurement (15%), and management (10%)**
- **Specific requirements around technical security (e.g. password length, data integrity, DNSSEC, and differentiation between vulnerability scanning and pen testing)**

# FHIR (pronounced “fire”)

- Replaces HL7
- Supports RESTful APIs
- Has OAuth, JSON, and HTTP capabilities
- Supports the use of W3C and JSON digital signatures

```
<Patient xmlns="http://hl7.org/fhir">
  <id value="glossy"/>
  <meta>
    <lastUpdated value="2014-11-13T11:41:00+11:00"/>
  </meta>
  <text>
    <status value="generated"/>
    <div xmlns="http://www.w3.org/1999/xhtml">
      <p>Henry Levin the 7th</p>
      <p>MRN: 123456. Male, 24-Sept 1932</p>
    </div>
  </text>
  <extension url="http://example.org/StructureDefinition/trials">
    <valueCode value="renal"/>
  </extension>
  <identifier>
    <use value="usual"/>
    <type>
      <coding>
        <system value="http://hl7.org/fhir/v2/0203"/>
        <code value="MR"/>
      </coding>
    </type>
    <system value="http://www.goodhealth.org/identifiers/mrn"/>
    <value value="123456"/>
  </identifier>
  <active value="true"/>
  <name>
    <family value="Levin"/>
    <given value="Henry"/>
    <suffix value="The 7th"/>
  </name>
  <gender value="male"/>
  <birthDate value="1932-09-24"/>
  <careProvider>
    <reference value="Organization/2"/>
    <display value="Good Health Clinic"/>
  </careProvider>
</Patient>
```

Resource identity  
and metadata

Human readable  
summary

Extension with  
URL to definition

Standard data:

- MRM
- Name
- Gender
- Birth date
- Provider

# Information security best practices

Because compliance is a minimum

- **Change them default passwords**
- **Follow NIST guidance on passwords**
- **Vendor risk management**
- **Continuous vulnerability management and patching**
- **Internal red and blue teams complemented by third-party testers**
- **Move security function out of risk/compliance**
- **Test all web apps in accordance with OWASP Top 10**
- **Perform physical penetration tests and phishing exercises**

**Go beyond compliance and aim for defense in depth**

# Thank you!

@hashtaginfosec

qasim.ijaz@coalfire.com



# H DON'T BE A HIPAAcite