



# Hacking Healthcare

A healthcare hacker's perspective

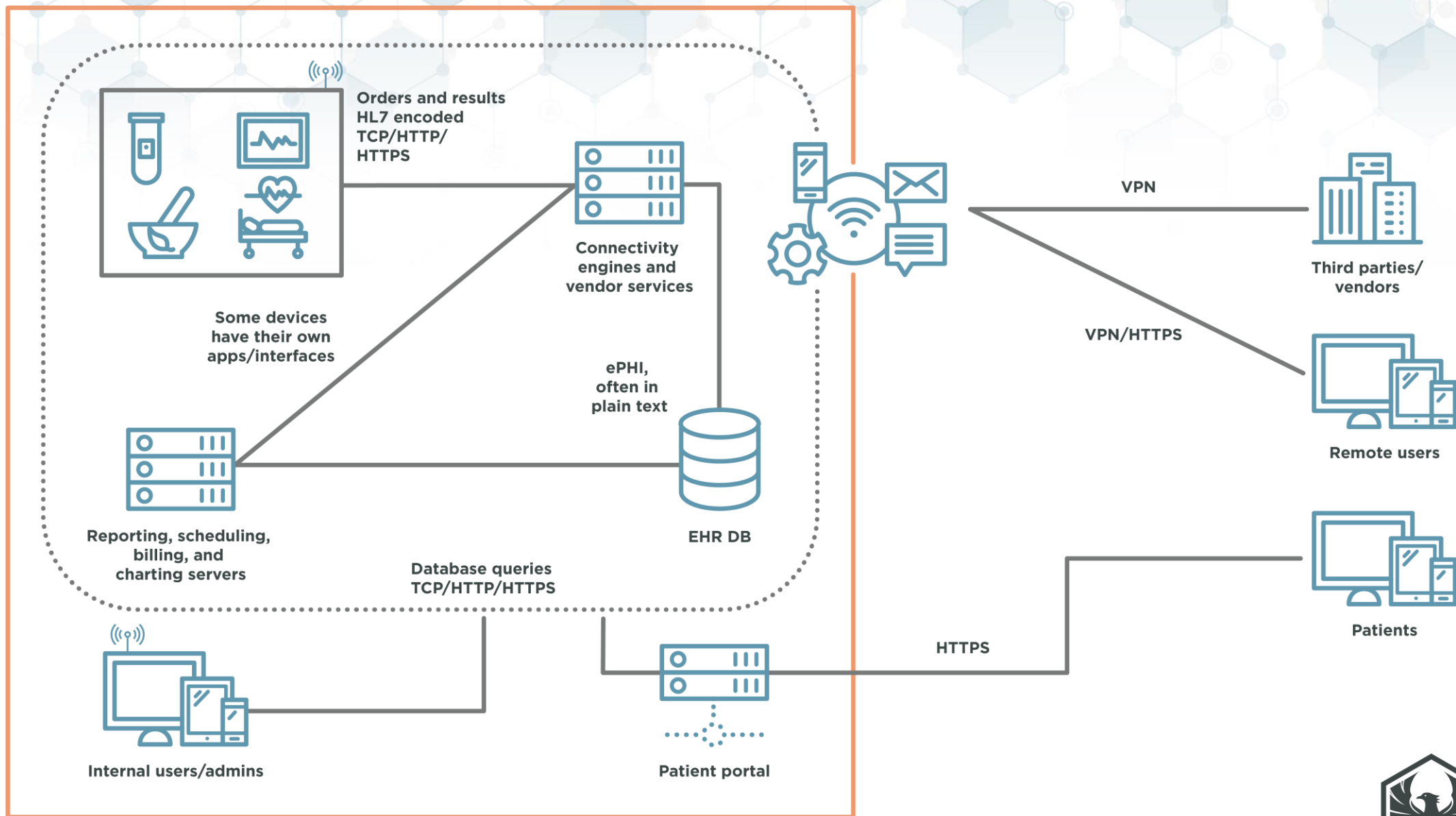
Qasim "Q" Ijaz



# \$ whoami

- Qasim / “Q”
- Director, Penetration Testing at Coalfire LABS
- Largely focused on healthcare clients
  - HIPAA and HITRUST assessor in past life
- 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

Sheets

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

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

Meetings

Meeting	Date	Time
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

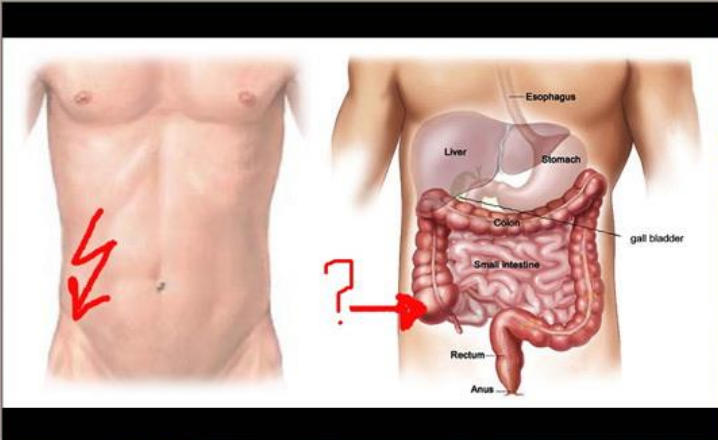
Draw ☒

Mark ☐

Color ☐

Pen ☐

8



Documents manager

Previous page Next page

# 10-Minute Domain Admin

Obvious Disclaimer: “It depends”



# My Methodology : Internal Network

- **cme smb <subnet>**
  - Try default AD accounts
- **MSF auxiliary/scanner/vnc/vnc\_none\_auth**
  - Radiology/PACs devices often use VNC and are AD connected
- **cme mssql or auxiliary/scanner/mssql/mssql\_login with defaults**
  - Broad force. Don't lock out EMR databases 😊
- **Look for creds / ePHI in user shares**
  - Use creds to access EMR/EHR
  - Try both SMB and NFS shares

# Default Credentials

- **museadmin:Muse!Admin**
- **museBkgnd:Muse!Bkgnd**
- **These are Active Directory Accounts 😊**

<https://www.slideshare.net/Shakacon/medical-devices-passwords-to-pwnage-by-scott-erven>





# My Methodology : Internal Network

- EyeWitness or PeepingTom to find unauthenticated WebApps with ePHI
- Quantify amount of ePHI you had access to
  - `select count(*) from database.table`
- **Usually Responder isn't needed but if you choose to run it, be careful not to take down the EMR!**



# My Methodology : Privesc

**Look for clinical application binaries with bad permissions or overly descriptive config files 😊**





# My Methodology : Phishing





# Sorry, just had to





# My Methodology: External

- **Medical defaults on OWA, Citrix, and VPN**
  - Don't forget to break out of Citrix 😊
- **Weak passwords + TheHarvester + External Portals = <3**
- **site:[client domain] intitle:'Patient Portal'**
  - Beware of third party hosted patient portals
- **Quantify amount of ePHI you had access to**



# Common Vulnerabilities



COAL FIRE  
LABS

# HL7: MITM'ers heaven

HL7: Set of international standards for transfer of clinical and administrative data among software applications used by various healthcare providers

```
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
```



See

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

# Healthcare defaults

Because nobody would read the manual (or Google)

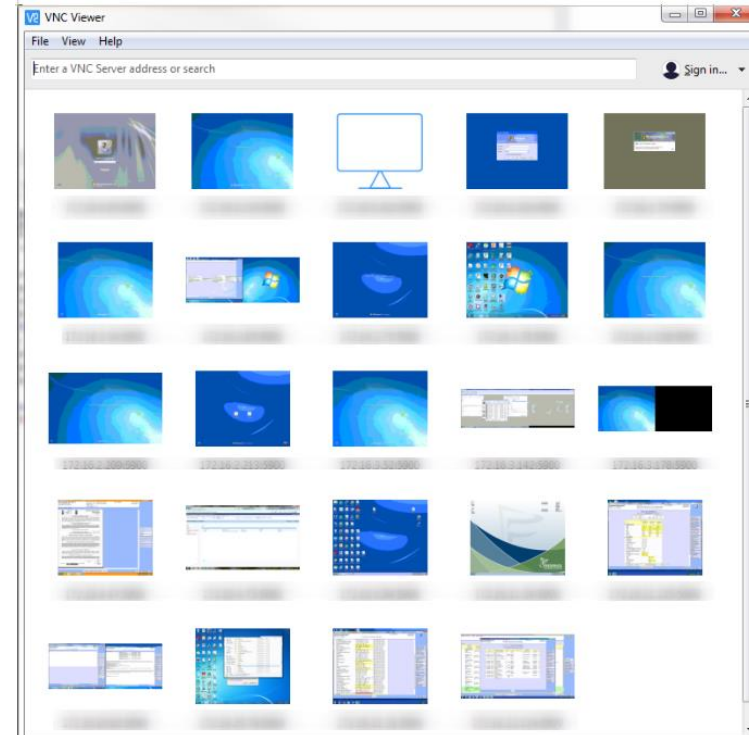
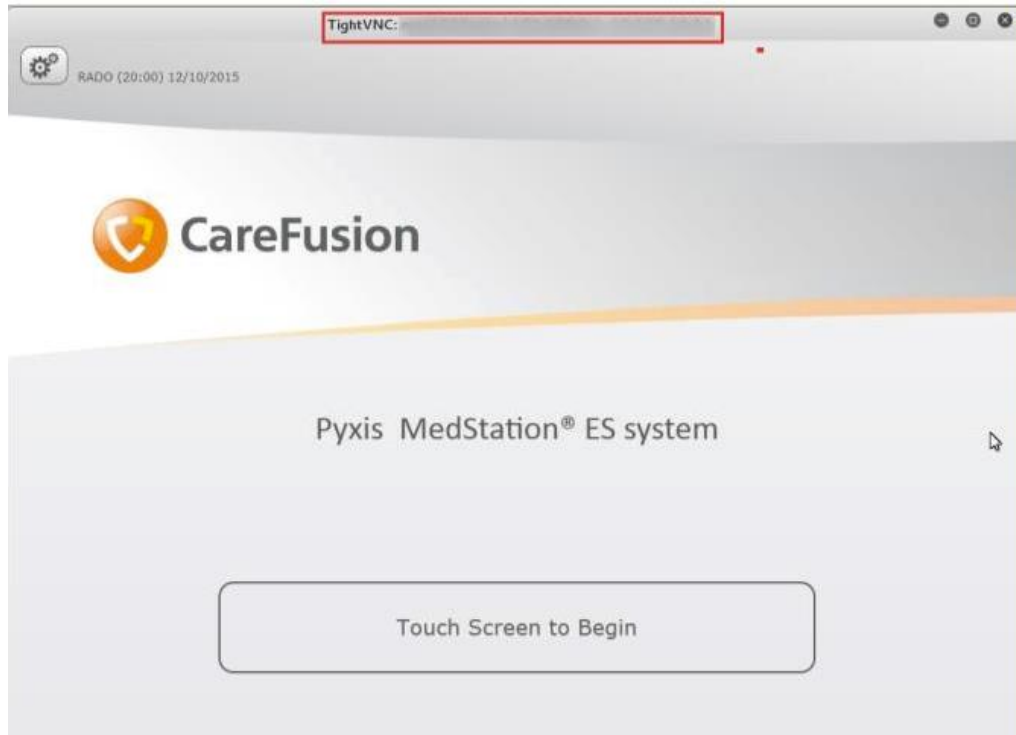
```
root@Kali:~/coalfire# crackmapexec 10.17.0.30 -u MuseAdmin -p [REDACTED]
CME 10.17.0.30:445 Muse [*] Windows 6.1 Build 7601 (name:Muse) (domain:[REDACTED])
CME 10.17.0.30:445 Muse [+] Muse\MuseAdmin [REDACTED] (Pwn3d!)
```

- If it's a hospital, start with the following AD accounts:
  - museadmin:Muse!Admin
  - museBkgnd:Muse!Bkgnd
- [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



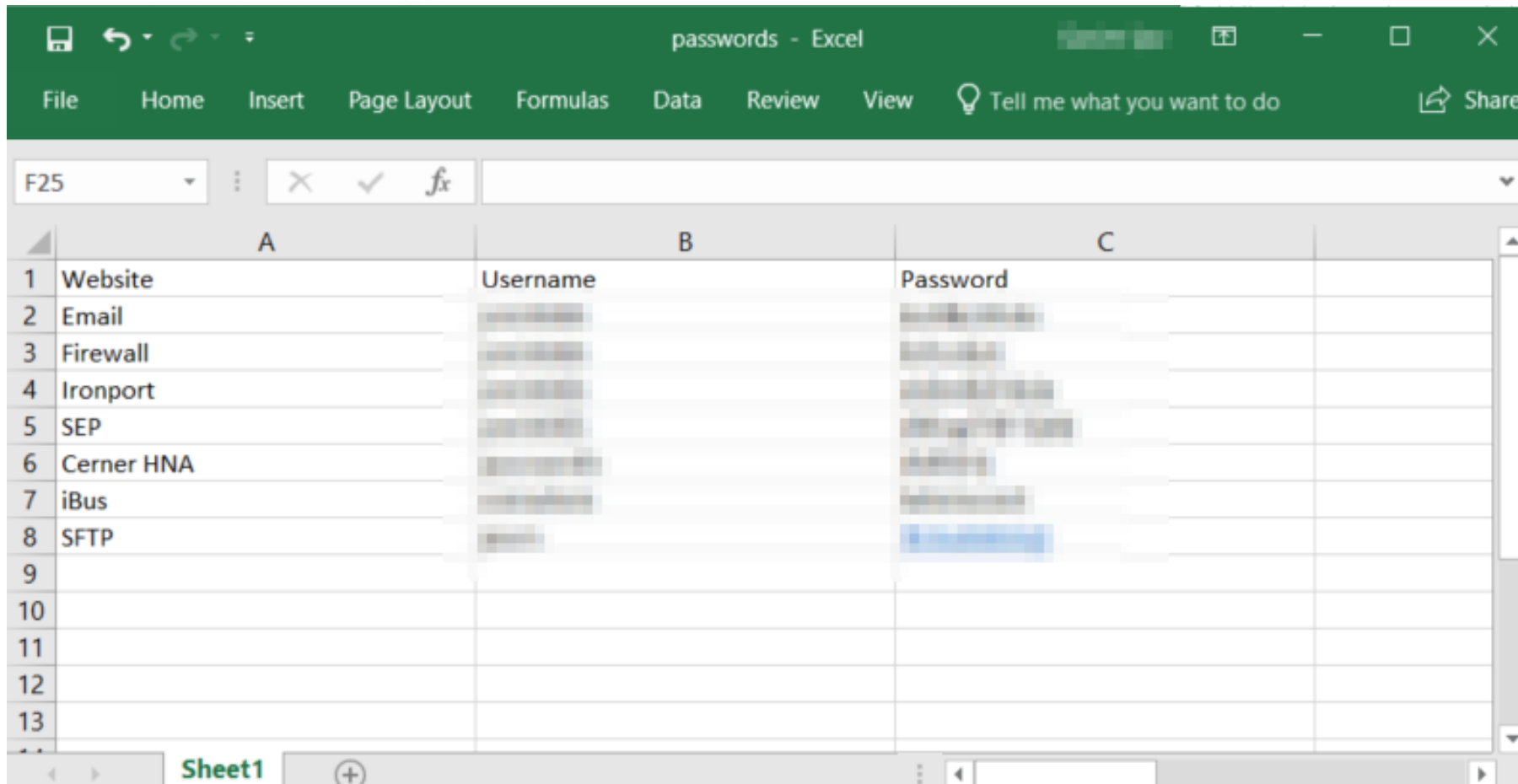
# Unauthenticated access to ePHI

```
|root@██████████ patient]# zcat patient.*.gz| wc -l  
13797281142  
[2019-04-22|11:23:25|EDT ██████████%eth0 172.23.69.206|  
|root@██████████ 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 IVXZE	NEW-00) 8		4.33	.68	.00	5.01	.00	5.01
	2	GUAIFENEX-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 three columns: Website, Username, and Password. The data is as follows:

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

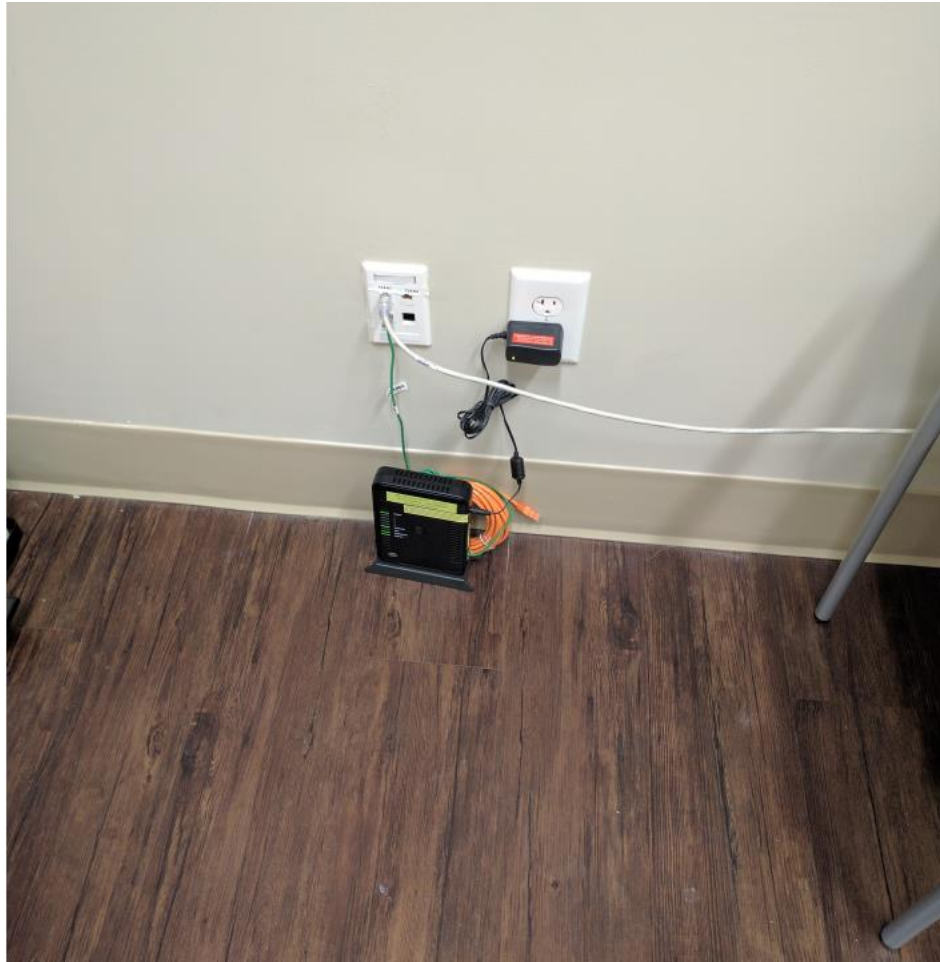


# Physical Goodies





# Physical Goodies



# OCR Breach Portal

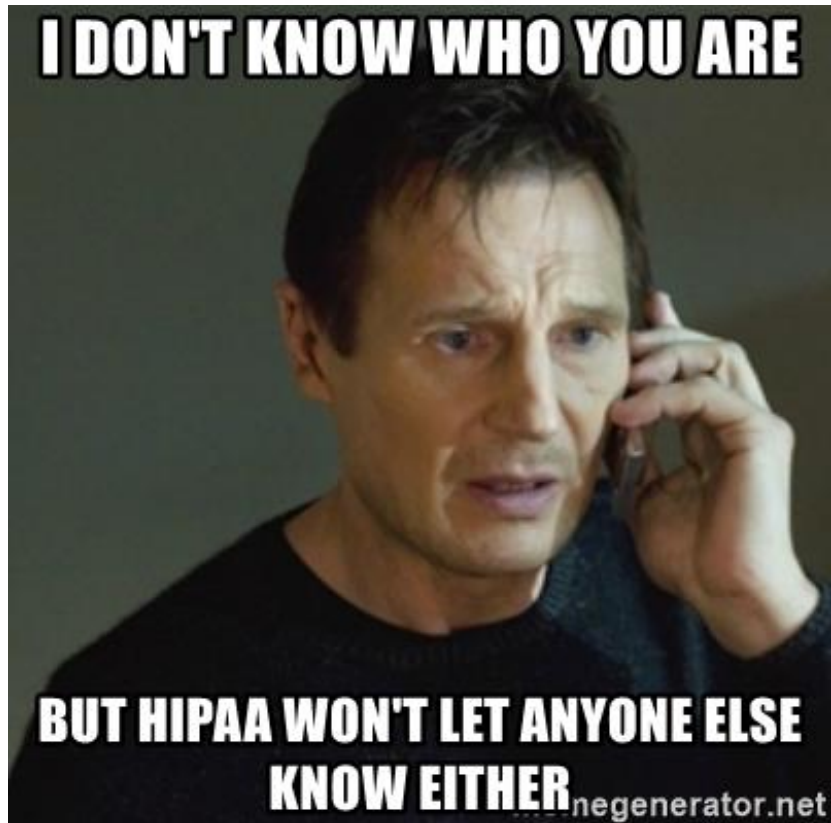
Because numbers don't lie

Name of Covered Entity ⇅	State ⇅	Covered Entity Type ⇅	Individuals Affected ⇅	Breach Submission Date ⇅	Type of Breach	Location of Breached Information
VibrantCare Rehabilitation, Inc.	CA	Healthcare Provider	1655	02/08/2020	Hacking/IT Incident	Email
Kaiser Health Plan, Southern California	CA	Health Plan	500	02/06/2020	Unauthorized Access/Disclosure	Paper/Films
Lake County Behavioral Health Services	CA	Healthcare Provider	1178	01/31/2020	Theft	Paper/Films
Solara Medical Supplies, LLC	CA	Healthcare Provider	1531	01/17/2020	Unauthorized Access/Disclosure	Paper/Films
PIH Health	CA	Healthcare Provider	199548	01/10/2020	Hacking/IT Incident	Email
San Francisco Department of Public Health - Zuckerberg SF General Hospital	CA	Healthcare Provider	1174	12/16/2019	Improper Disposal	Paper/Films
Western Health Advantage	CA	Health Plan	869	12/13/2019	Unauthorized Access/Disclosure	Network Server
Family Care Medical Specialists Group, Inc.	CA	Healthcare Provider	2490	12/08/2019	Unauthorized Access/Disclosure	Paper/Films
Adventist Health Simi Valley	CA	Healthcare Provider	62000	12/06/2019	Hacking/IT Incident	Email
Sunshine Behavioral Health Group, LLC	CA	Business Associate	3500	12/02/2019	Unauthorized Access/Disclosure	Other
San Francisco VA Health Care System	CA	Healthcare Provider	735	11/29/2019	Theft	Other, Paper/Films
La Clinica de La Raza, Inc.	CA	Healthcare Provider	2477	11/22/2019	Theft	Other Portable Electronic Device
Solara Medical Supplies, LLC	CA	Healthcare Provider	114007	11/13/2019	Hacking/IT Incident	Email
SALIH M MAYALIDAG DENTAL CORP	CA	Healthcare Provider	6000	11/12/2019	Hacking/IT Incident	Network Server
Kaiser Foundation Health Plan (Kaiser Permanente)	CA	Health Plan	515	11/07/2019	Unauthorized Access/Disclosure	Paper/Films
The Guidance Center	CA	Healthcare Provider	1189	10/28/2019	Hacking/IT Incident	Email
Central Valley Regional Center	CA	Business Associate	15975	10/11/2019	Hacking/IT Incident	Email

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

**What do we do now?**

# What 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)))

HIPPA-

Allowing healthcare workers everywhere avoid conversations with annoying family members.

somee cards  
user card



COAL FIRE  
LABS

# 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 (15%), procedure (20%), implementation (40%), measurement (10%), and management (15%)**
  - Changes to weights went into effect 12/31/2019
- **Specific requirements around technical security (e.g. password length, data integrity, DNSSEC, and differentiation between vulnerability scanning and pen testing)**
- **Pain in the rear to implement and assess**



# FHIR (pronounced “fire”)

- 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



# Thank you!

Questions?

@hashtaginfosec (twitter and github)  
qasim.ijaz@coalfire.com

