



Medical records and default passwords

A healthcare hacker's perspective

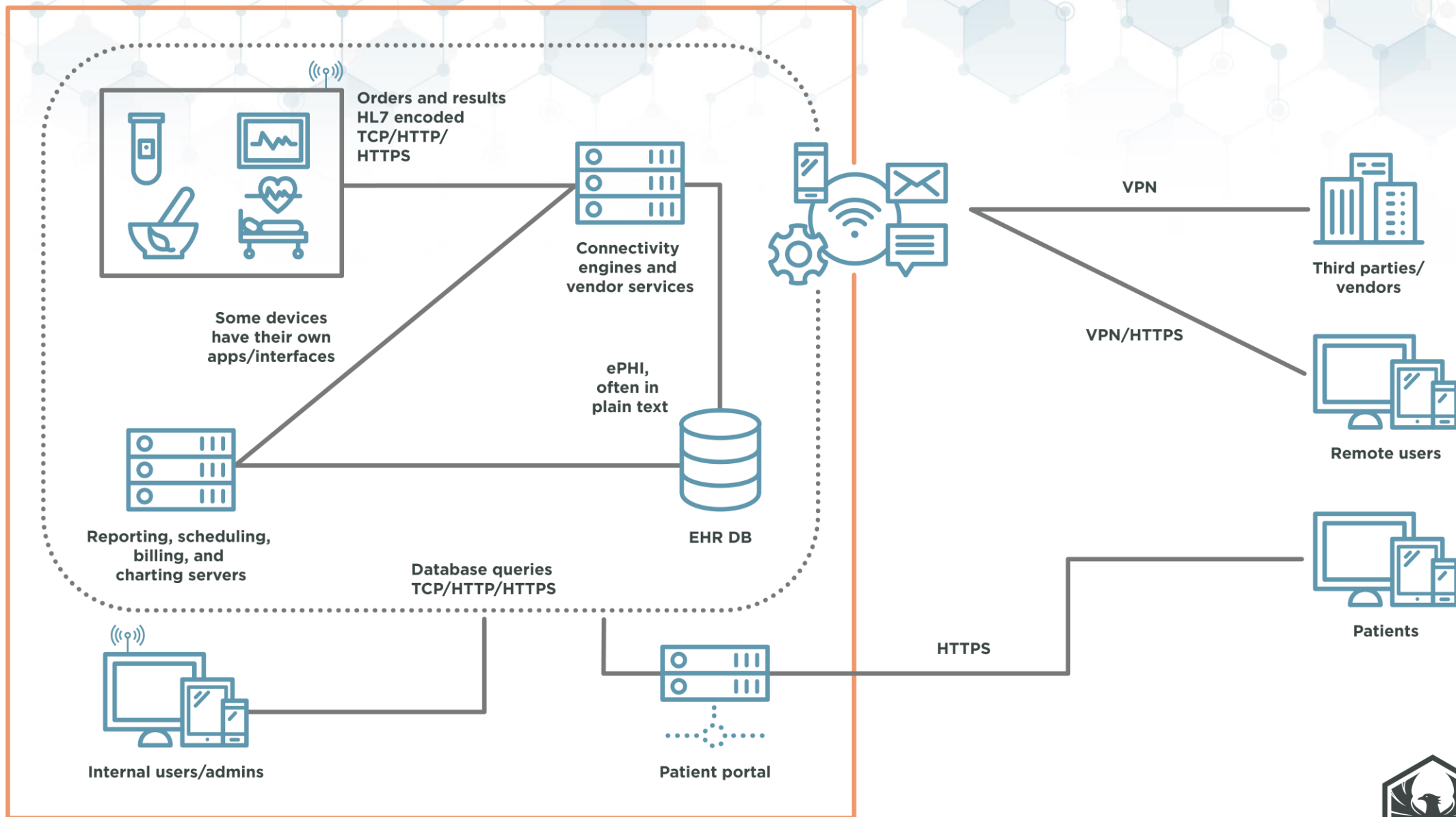
Qasim "Q" Ijaz



\$ 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>
- <https://twitter.com/coalfirelabs>

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

**Gimme the
goods, man!**



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

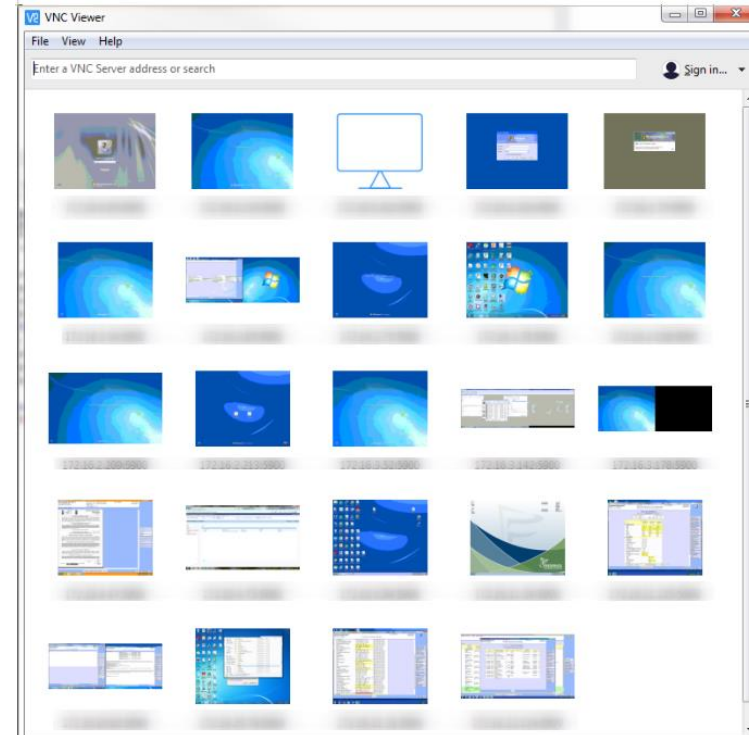
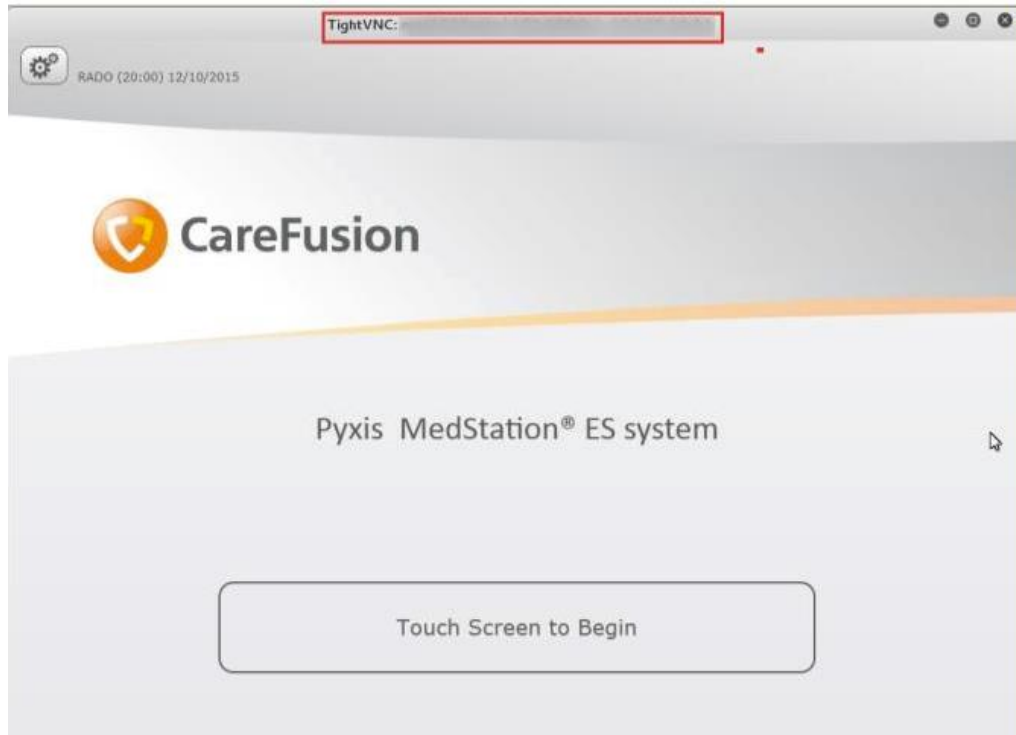
Because nobody would read the manual (or Google)

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

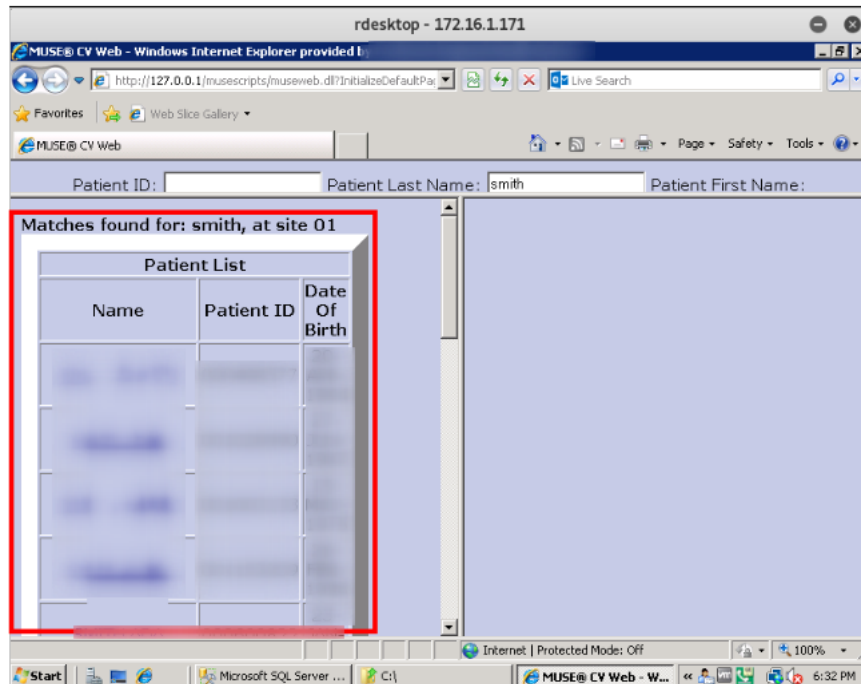


Unauthenticated VNC



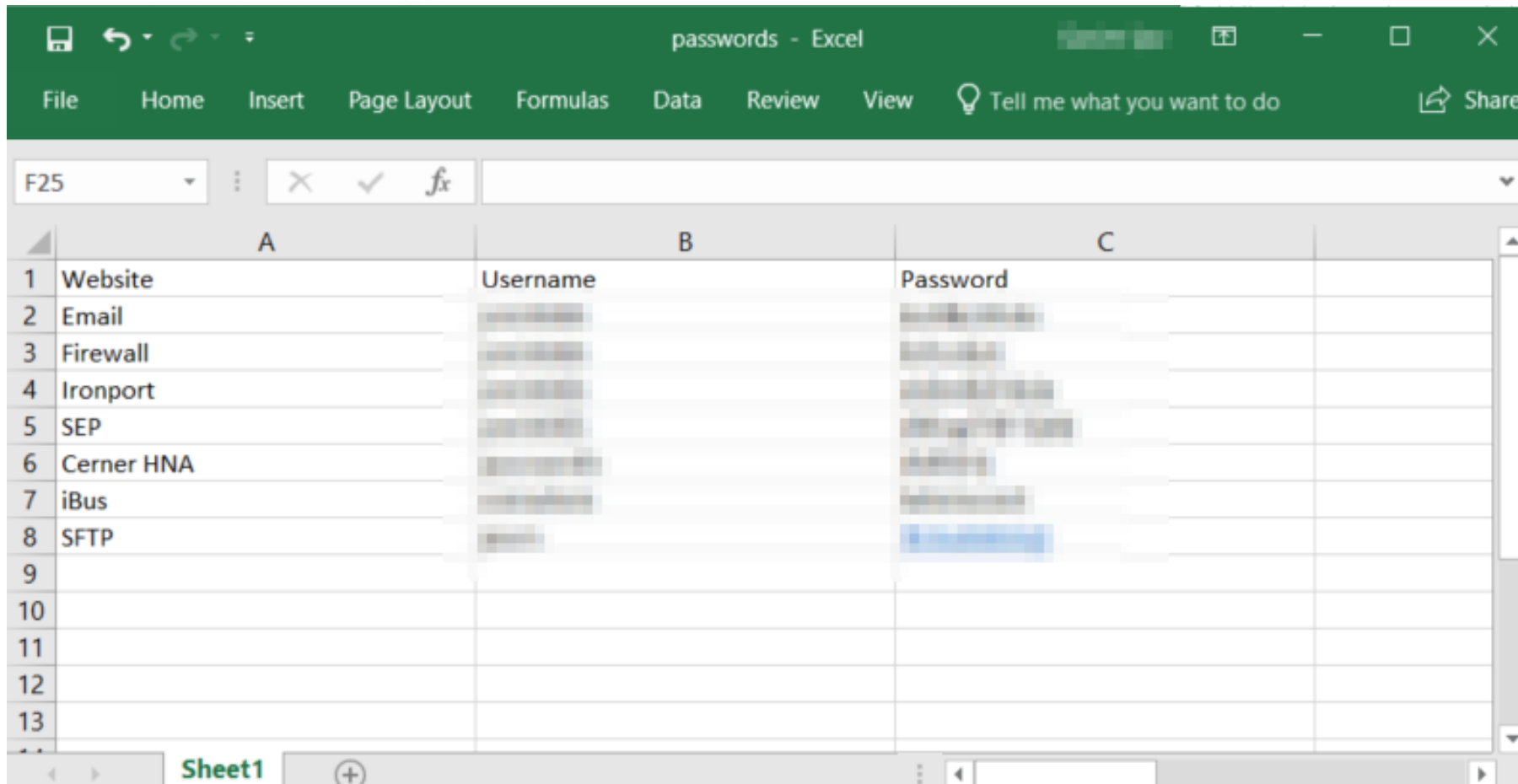
Unauthenticated access to ePHI

```
|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
```



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

Who needs a password manager anyway?



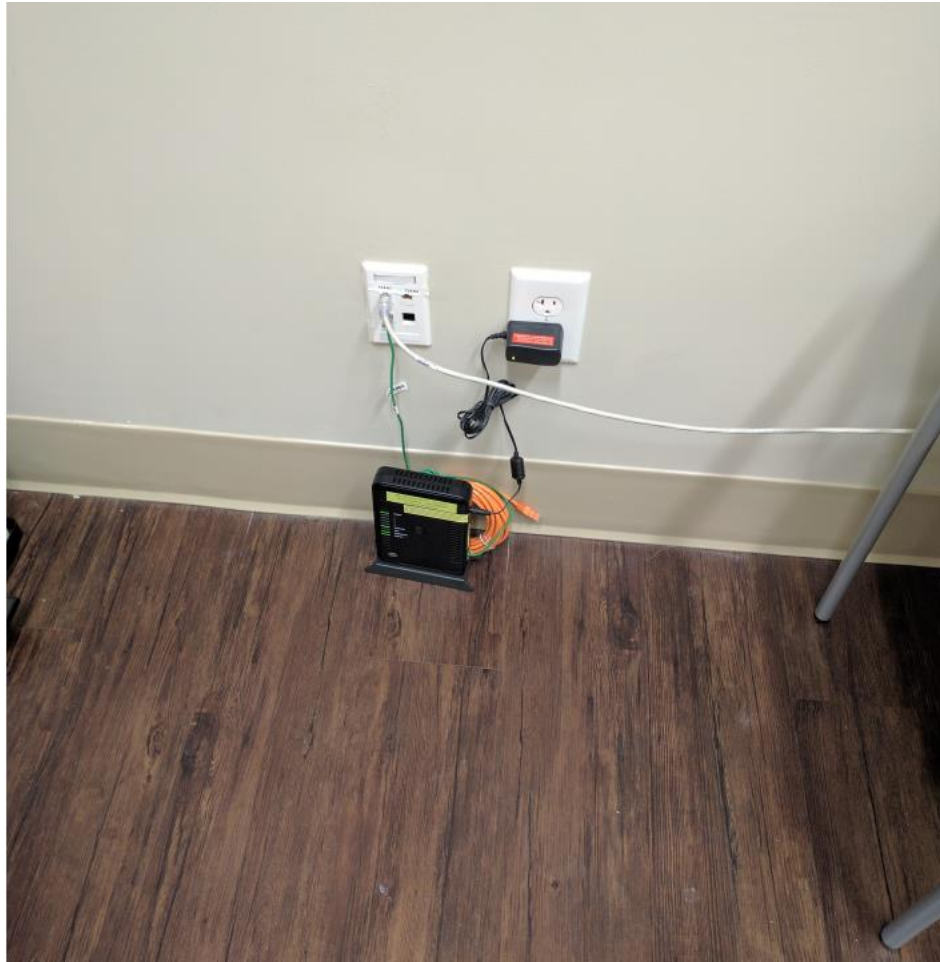
The screenshot shows an Excel spreadsheet with three columns: Website, Username, and Password. The data is as follows:

	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



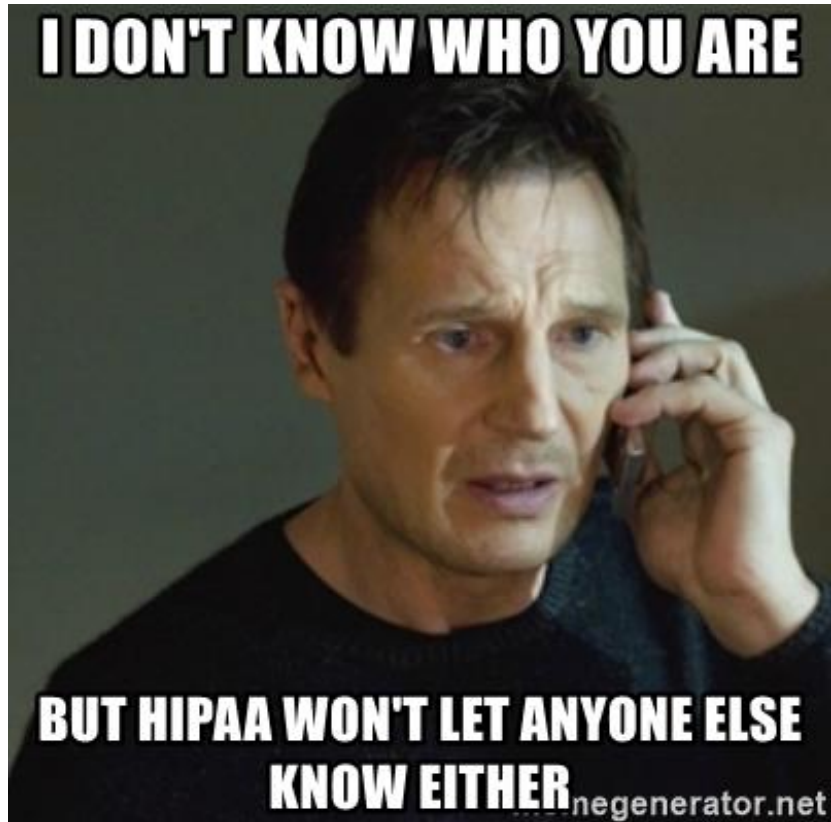
OCR Breach Portal

Name of Covered Entity ▾	State ▾	Covered Entity Type ▾	Individuals Affected ▾	Breach Submission Date ▾	Type of Breach	Location of Breached Information
Magellan Healthcare	MD	Business Associate	55637	09/17/2019	Hacking/IT Incident	Email
National Imaging Associates	MD	Business Associate	589	09/17/2019	Hacking/IT Incident	Email
Bates Technical College	WA	Healthcare Provider	2112	09/13/2019	Hacking/IT Incident	Network Server
June E. Nylen Cancer Center	IA	Healthcare Provider	927	09/11/2019	Unauthorized Access/Disclosure	Email
Berry Family Services	TX	Healthcare Provider	1751	09/08/2019	Hacking/IT Incident	Network Server
Premier Family Medical	UT	Healthcare Provider	320000	09/07/2019	Hacking/IT Incident	Network Server
Prisma - Midlands	SC	Healthcare Provider	2770	09/06/2019	Theft	Paper/Films
Shore Specialty Consultants Pulmonology Group	NJ	Healthcare Provider	9700	09/06/2019	Hacking/IT Incident	Desktop Computer, Network Server
Simmons Family Chiropractic	GA	Healthcare Provider	2000	09/06/2019	Theft	Laptop, Other Portable Electronic Device
Health Care Service Corporation	IL	Health Plan	998	09/06/2019	Unauthorized Access/Disclosure	Paper/Films
Rural Health Access Corporation dba Coalfield Health Center	WV	Healthcare Provider	874	09/06/2019	Unauthorized Access/Disclosure	Email
East Central Indiana School Trust	IN	Health Plan	3259	09/03/2019	Hacking/IT Incident	Email
Fraser	MN	Healthcare Provider	2890	08/30/2019	Hacking/IT Incident	Email
Fedcap Rehabilitation Services, Inc.	NY	Healthcare Provider	2158	08/29/2019	Hacking/IT Incident	Email

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 go in effect 12/31/2019
- **Specific requirements around technical security (e.g. password length,**
- **data integrity, DNSSEC, and differentiation between vulnerability scanning**
- **and pen testing)**

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



Where the Crown Jewels at?



COAL FIRE
LABS

Crown Jewels

- **ePHI**
 - Databases with names relevant to EMR/EHR
 - Look for EMR/EHR servers and navigate to them over HTTP/HTTPS
 - Webcam shots from devices inside patient rooms (caution)
- **ePHI/PHI (Physical pen tests)**
 - Look for printers, fax machines, copiers
 - Unlocked secure bins?
 - Check NICU/ICU/ER for publicly visible EMR/EHR screens

We're Hiring

- **Consultant, Penetration Tester**
 - Alpharetta, GA
 - Denver & Westminster, CO
 - Far-away state of Washington
 - Dallas, TX
- **Senior Consultant, Penetration Tester**
 - Alpharetta, GA
 - Denver & Westminster, CO
 - Far-away state of Washington
 - Dallas, TX
 - Remote



<https://www.coalfire.com/Careers>



Thank you!

Questions?

Oh and we're hiring 😊

<https://www.coalfire.com/Careers>

<https://github.com/hashtaginfosec/contalks>

