COALFIRE

Medical records and default passwords

A healthcare hacker's perspective

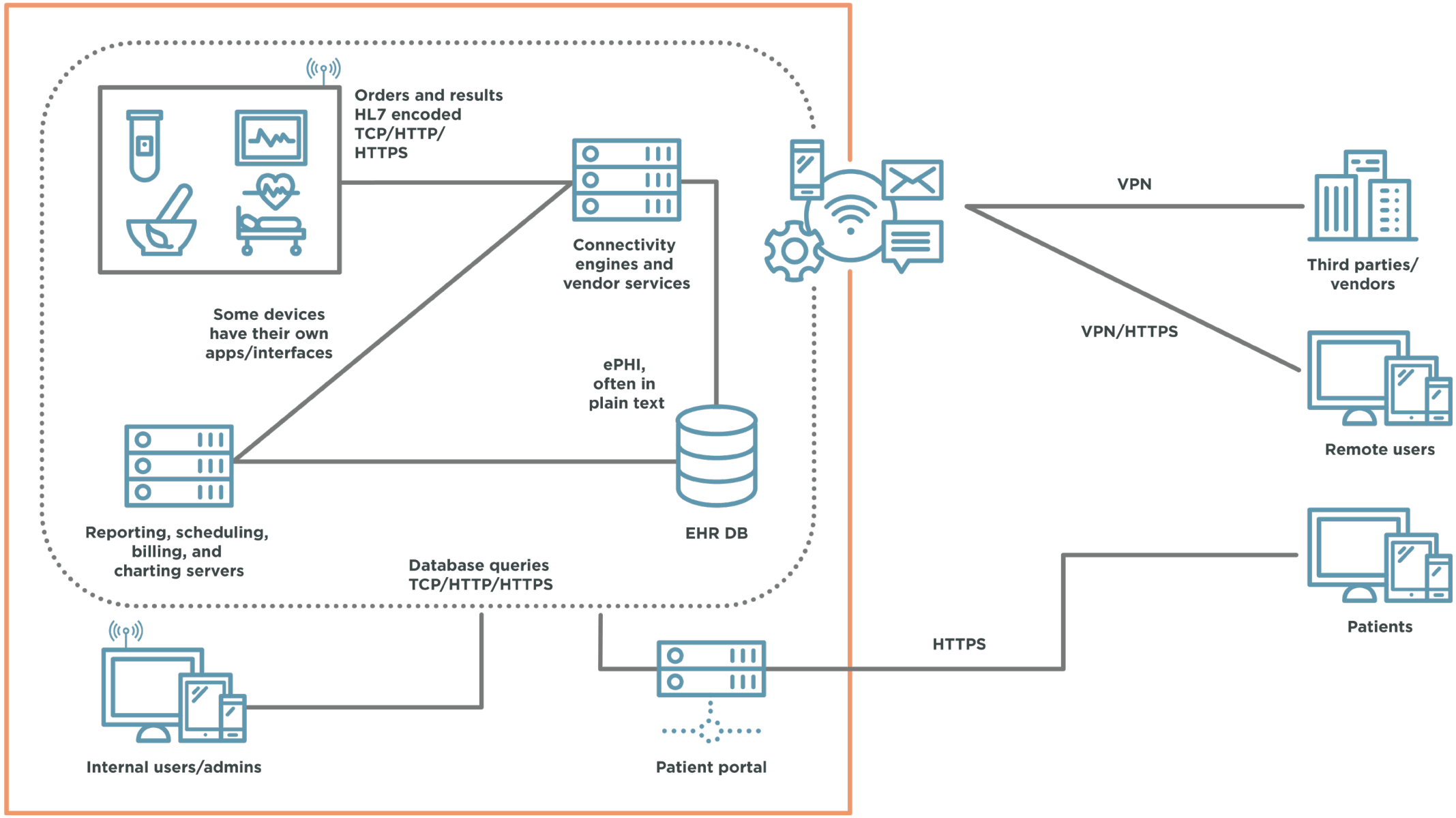
Qasim "Q" Ijaz

$ 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**

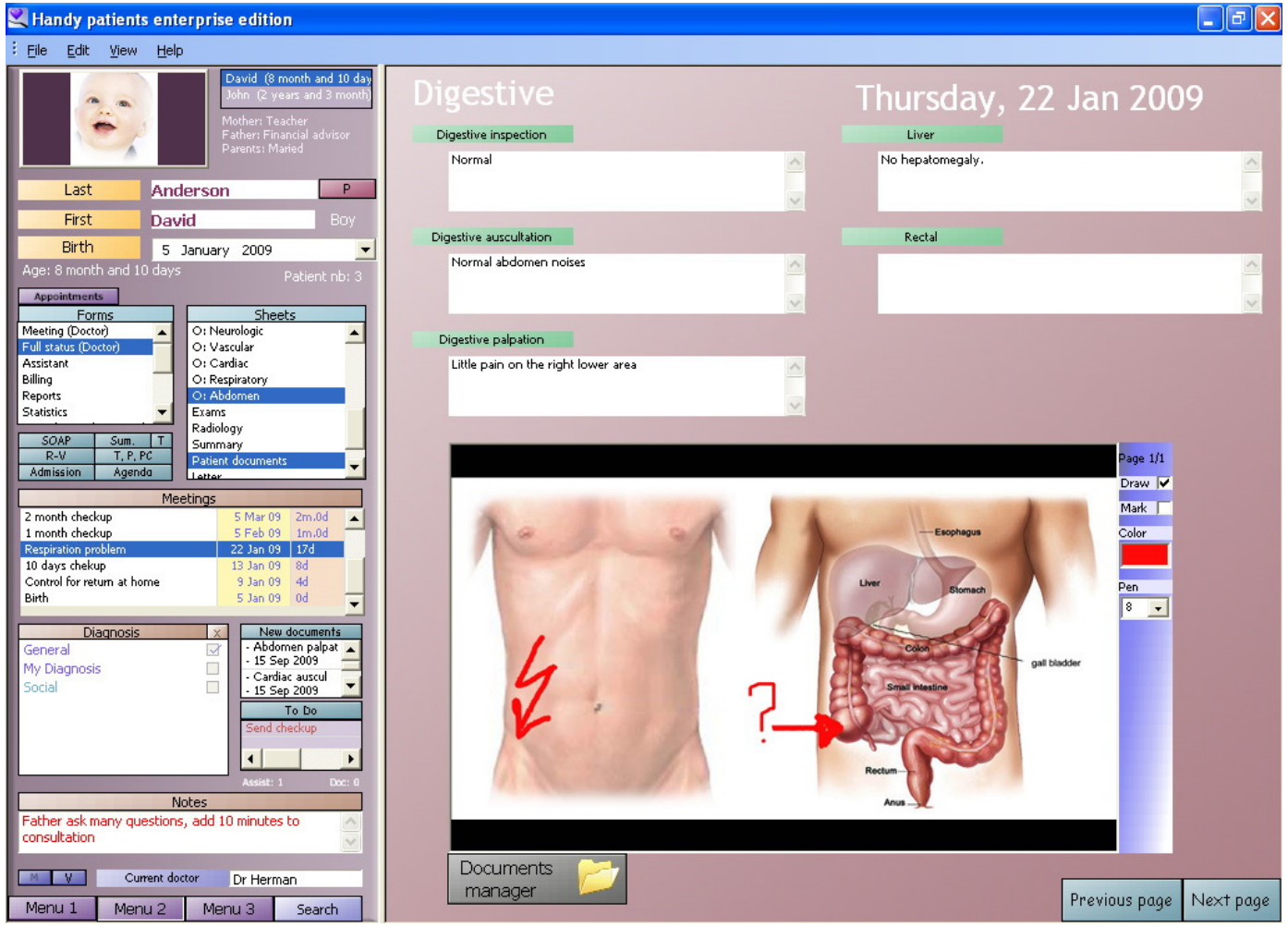
Healthcare IT overview

COALFIRE


Orders and results
HL7 encoded
TCP/HTTP/
HTTPS
Connectivity
engines and
vendor services
Some devices
have their own
apps/interfaces
ePHI,
often in
plain text
Reporting, scheduling,
billing, and
charting servers
EHR DB
Database queries
TCP/HTTP/HTTPS
Internal users/admins
Patient portal
HTTPS
VPN
VPN/HTTPS
Third parties/
vendors
Remote users
Patients

COALFIRE

Electronic medical record (EMR)



COALFIRE

COALFIRE

HL7: MITM’ers 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/

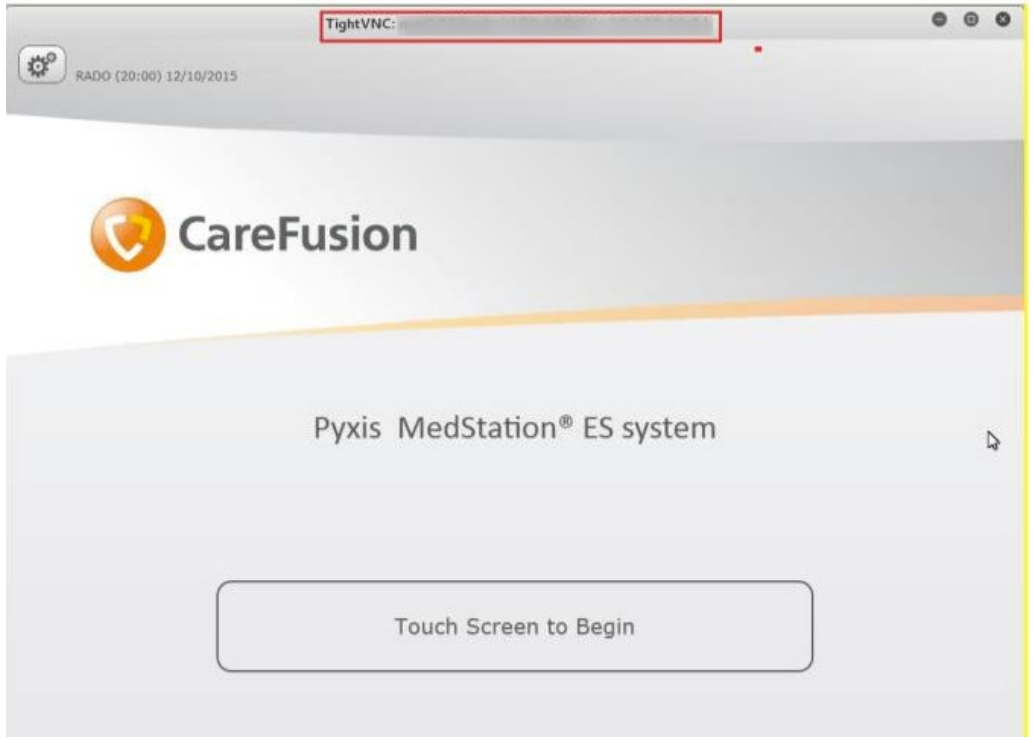
Healthcare defaults

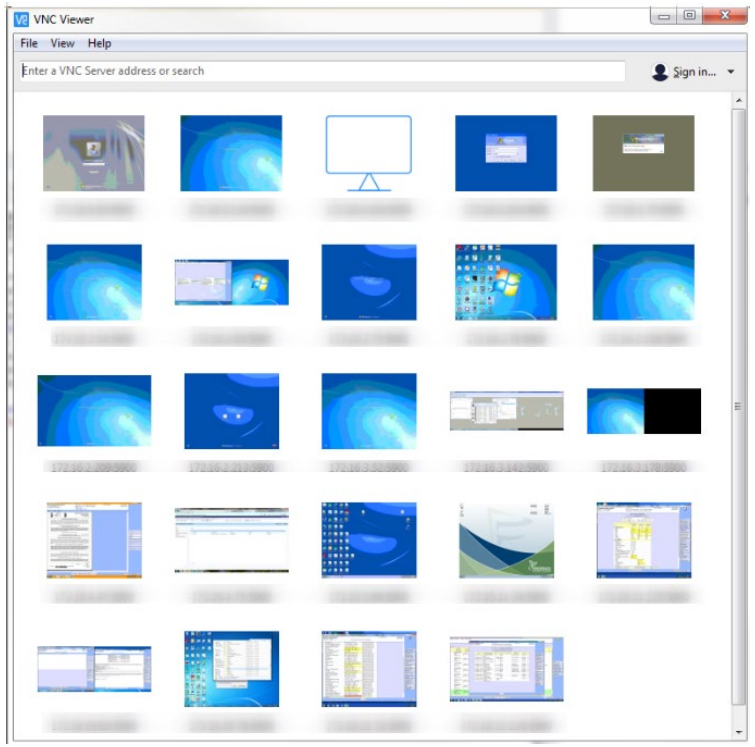
Because nobody would read the manual (or Google)

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

Unauthenticated VNC

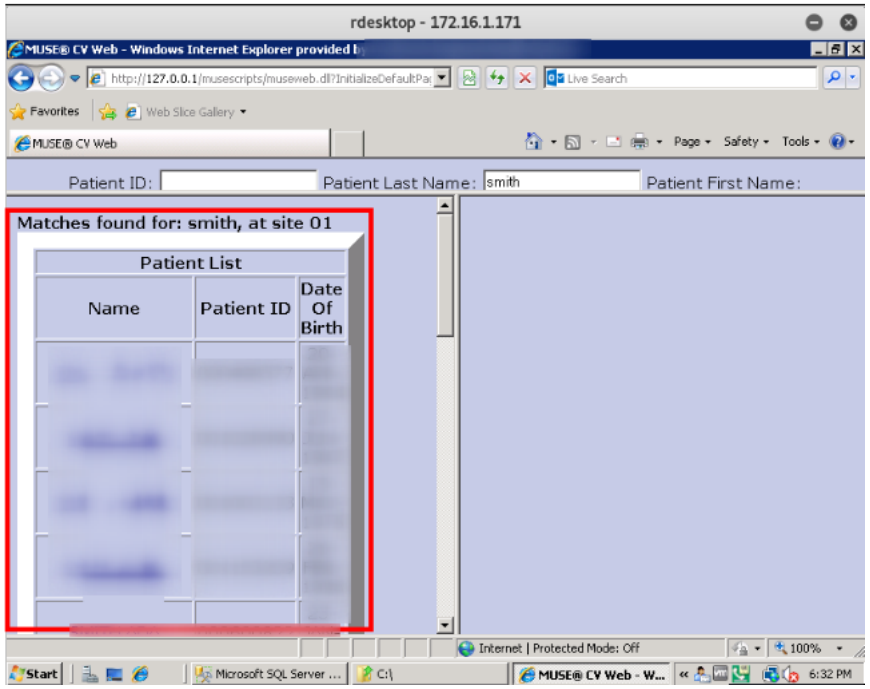


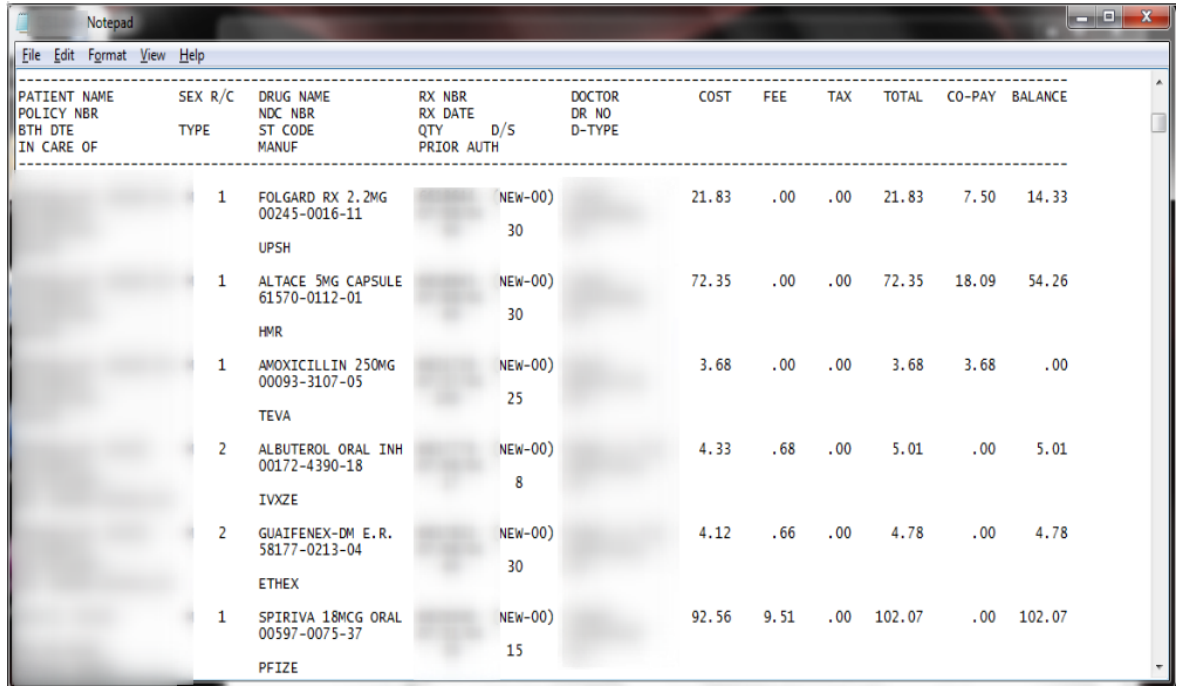


COALFIRE

Unauthenticated access to ePHI

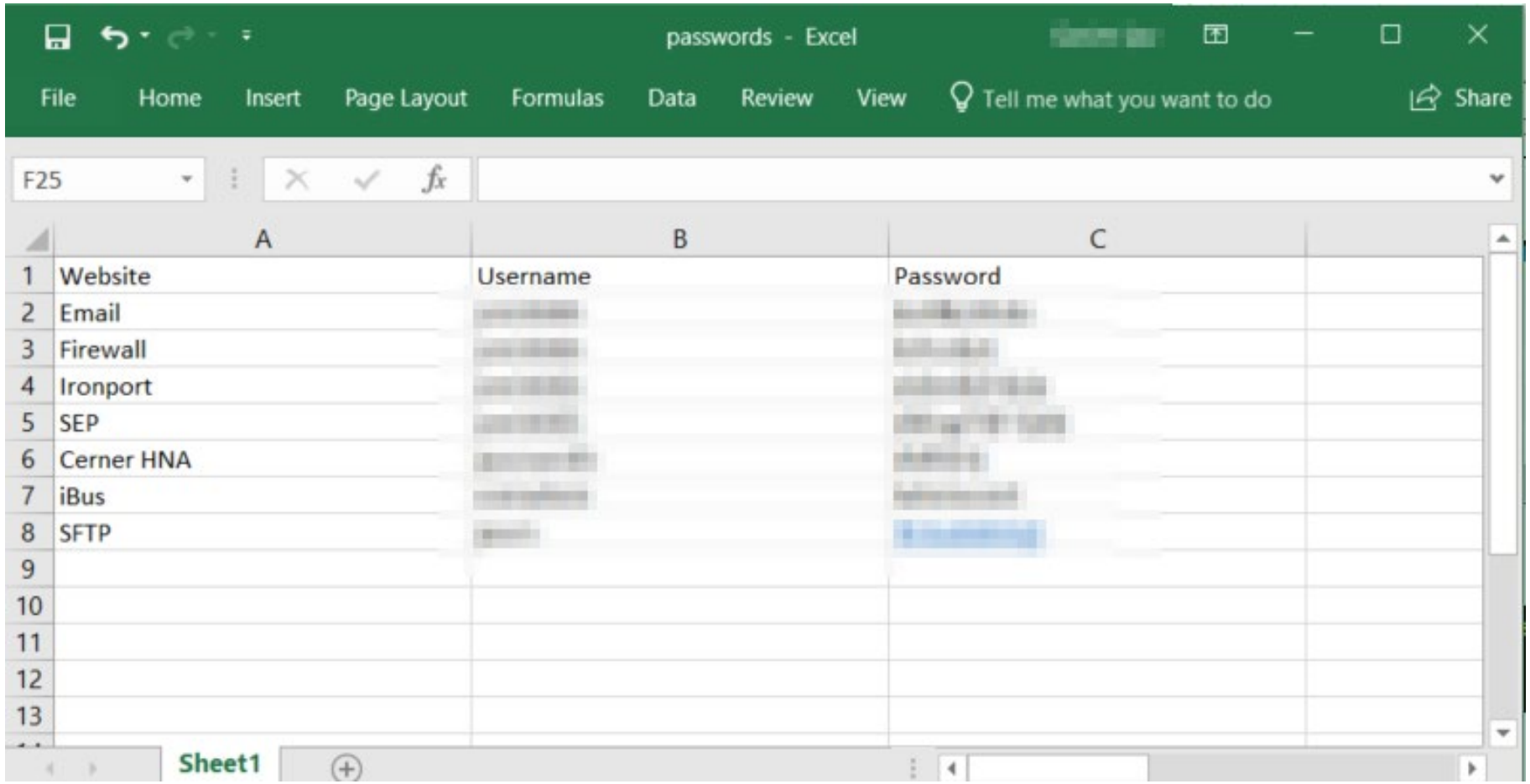
```
|root@                    patient]# zcat patient.*.*gz| wc -l
13797281142
[2019-04-22|11:23:25|EDT                    %eth0 172.23.69.206|
|root@                    patient]# ls patient.*.*gz| wc -l
8186
```





COALFIRE

Who needs a password manager anyway?



COALFIRE

OCR breach portal

Because numbers don't lie

Breach Report Results

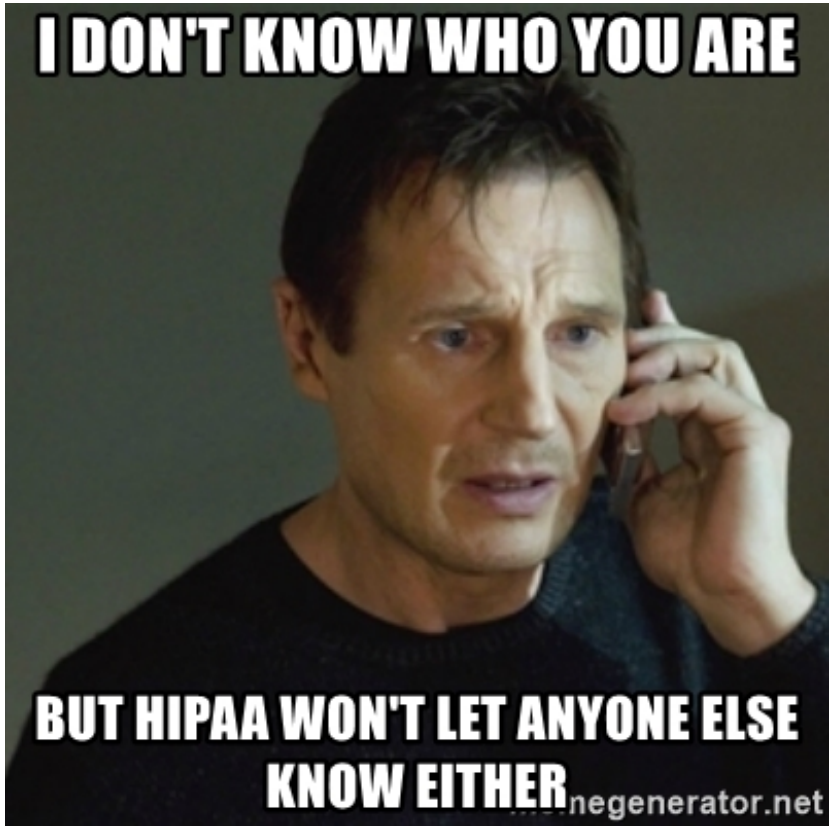
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	American Medical Response, Inc.	TX	Healthcare Provider	4300	05/06/2019	Hacking/IT Incident	Email
	Inspira Behavioral Care, Corp		Healthcare Provider	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

CALFIRE

COALFIRE

There’s HIPAA



COALFIRE

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

COALFIRE