practice fusion™
Free, web-based Electronic Health Records

# Risk and Opportunities in EMR Technology


Shanit Gupta

Director of Information Security


EMR In-Depth Seminar – Session 2

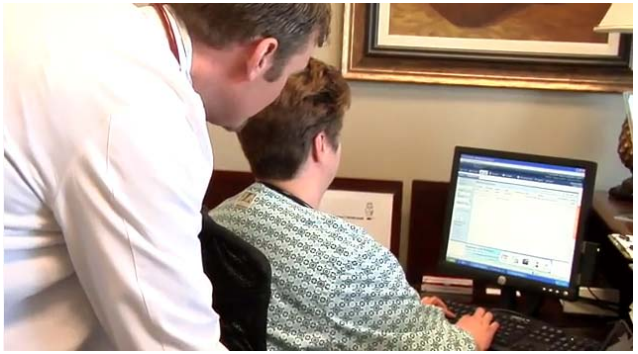
# The Changing Healthcare Landscape

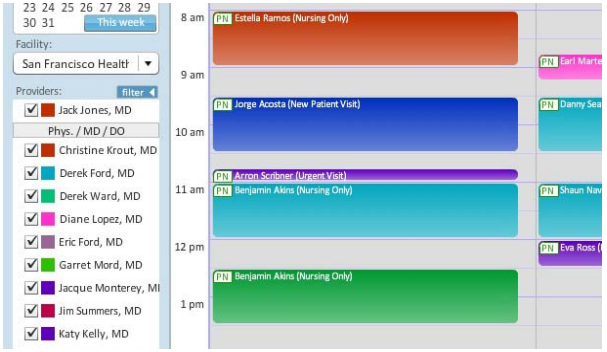
- The U.S. spends 17.4% of GDP on healthcare, more than twice the average for developed countries
- 80% of US doctors are still using paper health records
- 195,000 annual deaths from preventable medical errors
  - *7,000 of those deaths are tied to illegible handwriting alone*

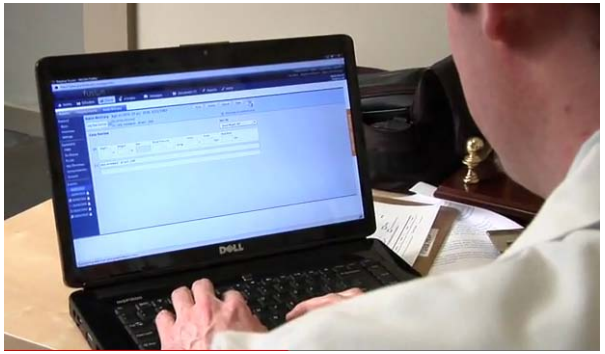
# Fundamental Goal: Save Lives

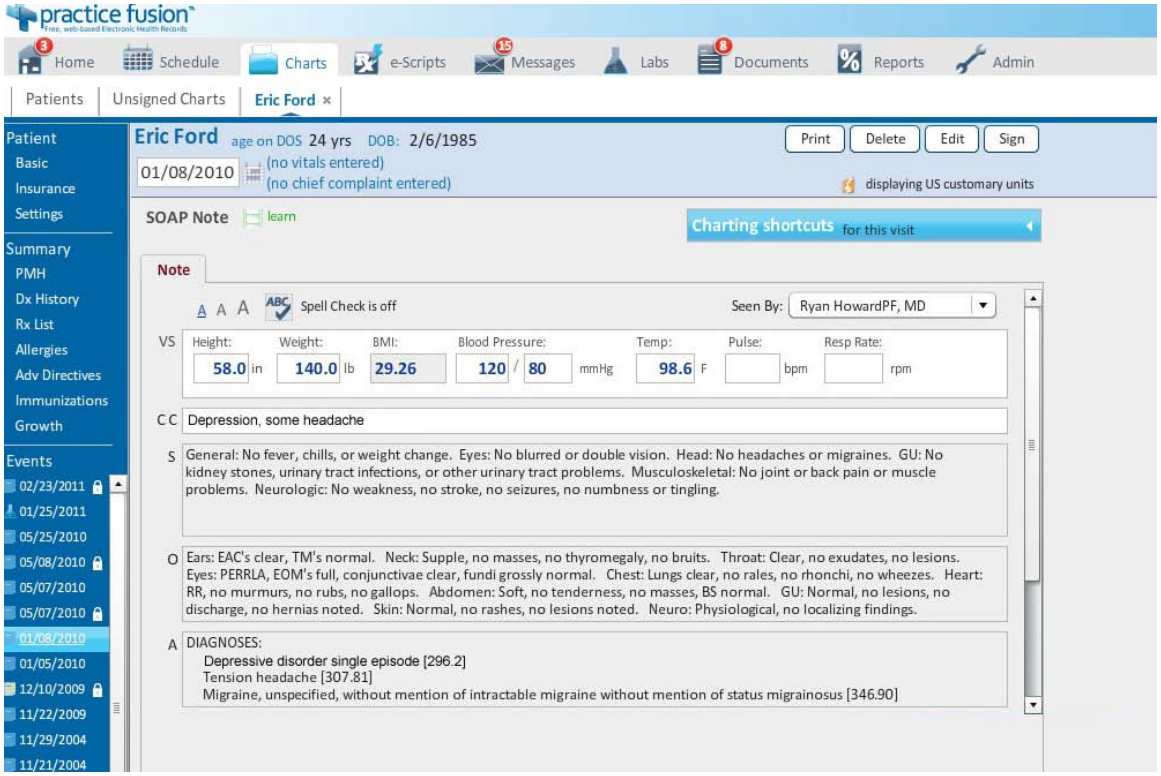
***"…just wanted to let you know PF saved a patient's life.*** *I admitted through the emergency room a patient seen by one of my partners and needed to start a blood thinner.* ***Had I not had her electronic info on Practice Fusion and seen that she had a history of a clotting disorder, I likely would have killed her.*** *It was not found anywhere else."*

# What Is EHR?




23 24 25 26 27 28 29
30 31
This week
Facility:
San Francisco Health
Providers:
filter
Jack Jones, MD
Phys. / MD / DO
Christine Krout, MD
Derek Ford, MD
Derek Ward, MD
Diane Lopez, MD
Eric Ford, MD
Garret Mord, MD
Jacque Monterey, MI
Jim Summers, MD
Katy Kelly, MD
8 am
9 am
10 am
11 am
12 pm
1 pm
Estella Ramos (Nursing Only)
Jorge Acosta (New Patient Visit)
Arron Scribner (Urgent Visit)
Benjamin Akins (Nursing Only)
Benjamin Akins (Nursing Only)




practice fusion
Home
Schedule
Charts
e-Scripts
Messages
Labs
Documents
Reports
Admin
Patients
Unsigned Charts
Eric Ford
Patient
Basic
Insurance
Settings
Summary
PMH
Dx History
Rx List
Allergies
Adv Directives
Immunizations
Growth
Events
02/23/2011
01/25/2011
05/25/2010
05/08/2010
05/07/2010
05/07/2010
01/08/2010
01/05/2010
12/10/2009
11/22/2009
11/29/2004
11/21/2004
Eric Ford age on DOS 24 yrs DOB: 2/6/1985
01/08/2010
(no vitals entered)
(no chief complaint entered)
Print
Delete
Edit
Sign
displaying US customary units
SOAP Note
learn
Charting shortcuts for this visit
Note
Spell Check is off
Seen By: Ryan HowardPF, MD
VS
Height: 58.0 in
Weight: 140.0 lb
BMI: 29.26
Blood Pressure: 120 / 80 mmHg
Temp: 98.6 F
Pulse: bpm
Resp Rate: rpm
CC Depression, some headache
S General: No fever, chills, or weight change. Eyes: No blurred or double vision. Head: No headaches or migraines. GU: No kidney stones, urinary tract infections, or other urinary tract problems. Musculoskeletal: No joint or back pain or muscle problems. Neurologic: No weakness, no stroke, no seizures, no numbness or tingling.
O Ears: EAC's clear, TM's normal. Neck: Supple, no masses, no thyromegaly, no bruits. Throat: Clear, no exudates, no lesions. Eyes: PERRLA, EOM's full, conjunctivae clear, fundi grossly normal. Chest: Lungs clear, no rales, no rhonchi, no wheezes. Heart: RR, no murmurs, no rubs, no gallops. Abdomen: Soft, no tenderness, no masses, BS normal. GU: Normal, no lesions, no discharge, no hernias noted. Skin: Normal, no rashes, no lesions noted. Neuro: Physiological, no localizing findings.
A DIAGNOSES:
Depressive disorder single episode [296.2]
Tension headache [307.81]
Migraine, unspecified, without mention of intractable migraine without mention of status migrainosus [346.90]

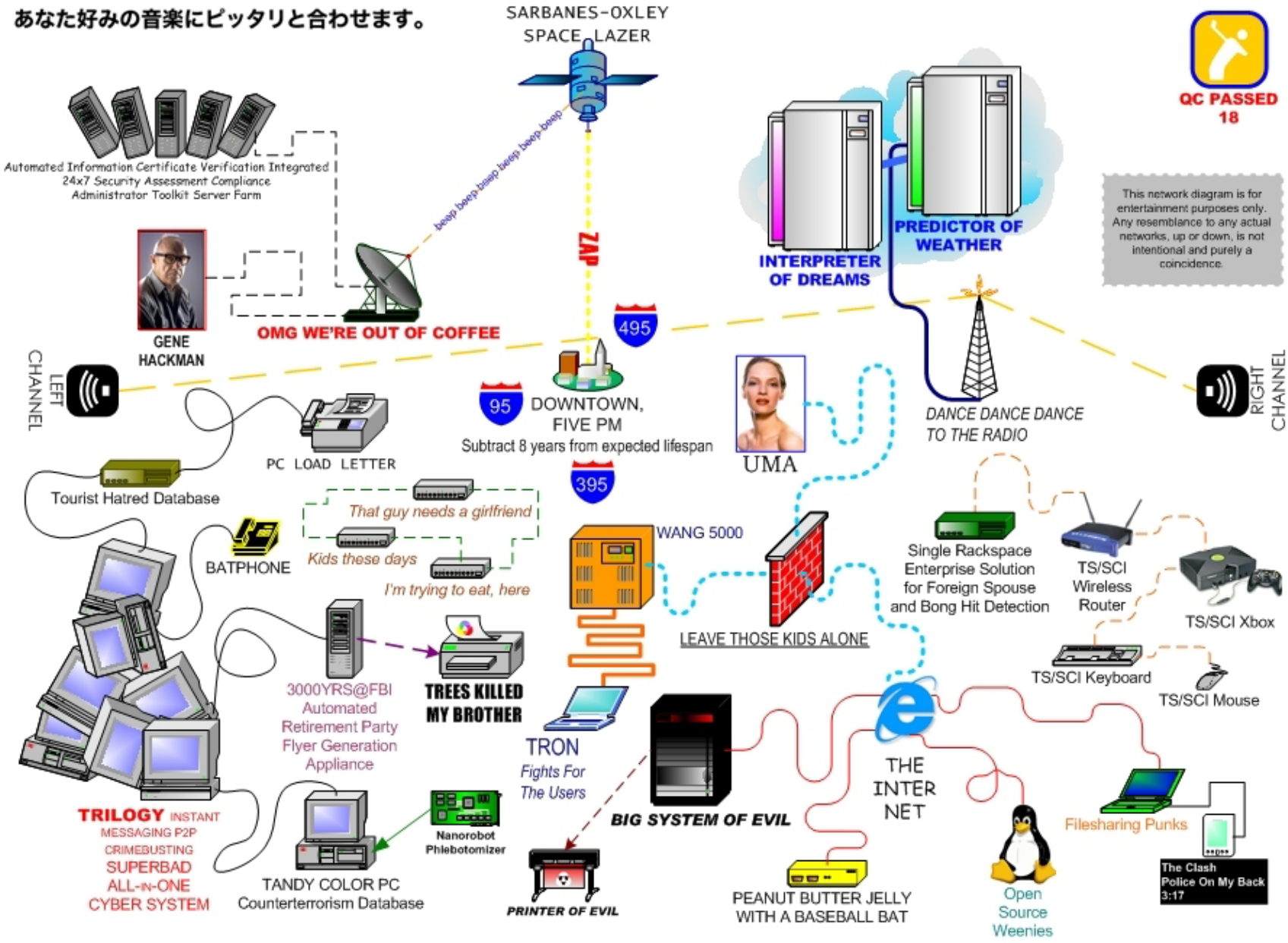
# Key Requirements



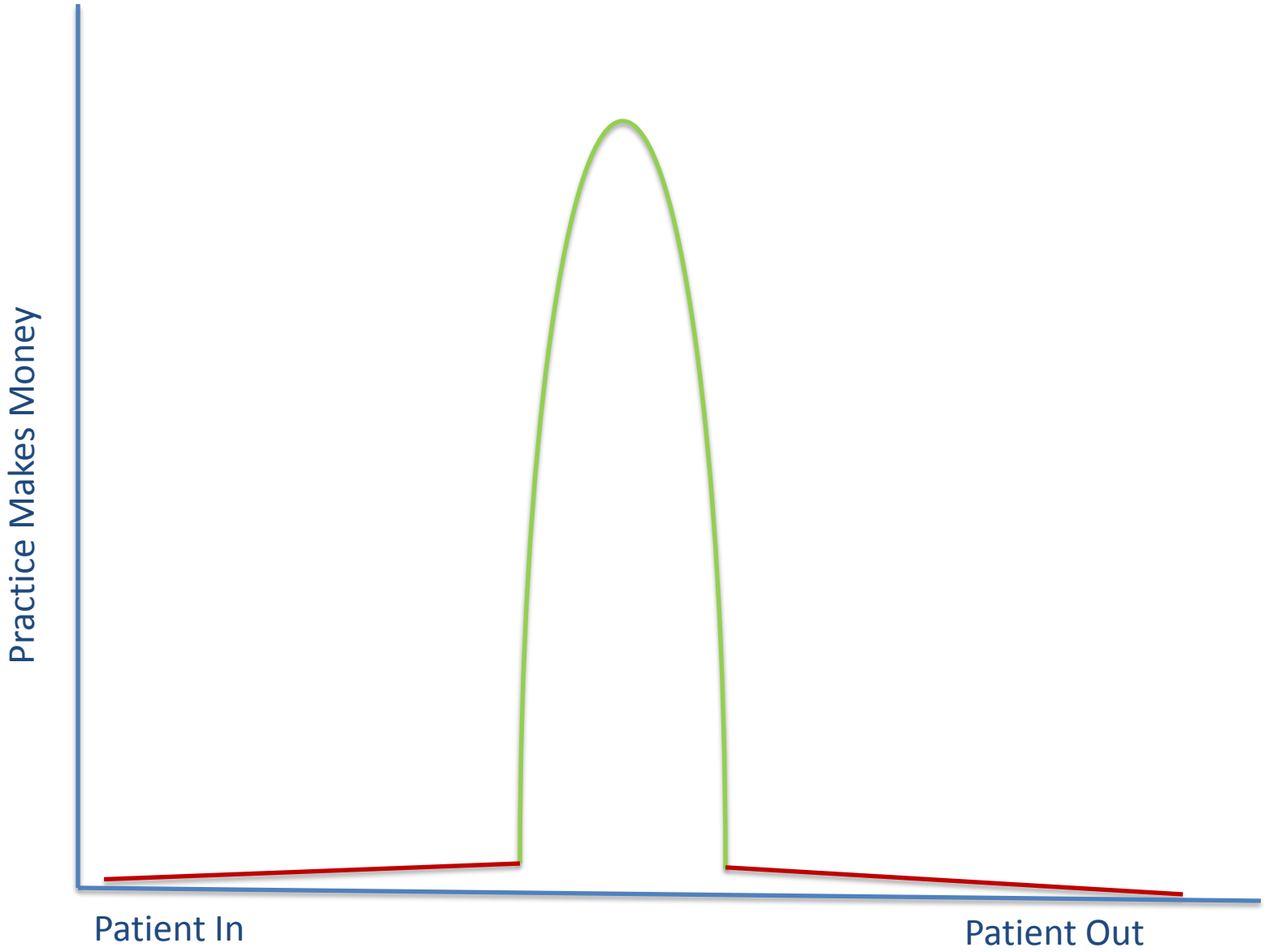

# Security is Fundamental Requirement




# Traditional EHR


あなた好みの音楽にピッタリと合わせます。
SARBANES-OXLEY
SPACE LAZER
QC PASSED
18
Automated Information Certificate Verification Integrated
24x7 Security Assessment Compliance
Administrator Toolkit Server Farm
beep beep beep beep beep beep
ZAP
INTERPRETER
OF DREAMS
PREDICTOR OF
WEATHER
This network diagram is for entertainment purposes only. Any resemblance to any actual networks, up or down, is not intentional and purely a coincidence.
GENE
HACKMAN
OMG WE'RE OUT OF COFFEE
495
95
DOWNTOWN,
FIVE PM
Subtract 8 years from expected lifespan
395
UMA
DANCE DANCE DANCE
TO THE RADIO
LEFT
CHANNEL
RIGHT
CHANNEL
PC LOAD LETTER
Tourist Hatred Database
That guy needs a girlfriend
Kids these days
I'm trying to eat, here
BATPHONE
WANG 5000
LEAVE THOSE KIDS ALONE
Single Rackspace
Enterprise Solution
for Foreign Spouse
and Bong Hit Detection
TS/SCI
Wireless
Router
TS/SCI Xbox
TS/SCI Keyboard
TS/SCI Mouse
3000YRS@FBI
Automated
Retirement Party
Flyer Generation
Appliance
TREES KILLED
MY BROTHER
TRON
Fights For
The Users
BIG SYSTEM OF EVIL
THE
INTER
NET
TRILOGY INSTANT
MESSAGING P2P
CRIMEBUSTING
SUPERBAD
ALL-IN-ONE
CYBER SYSTEM
Nanorobot
Phlebotomizer
TANDY COLOR PC
Counterterrorism Database
PRINTER OF EVIL
PEANUT BUTTER JELLY
WITH A BASEBALL BAT
Open
Source
Weenies
Filesharing Punks
The Clash
Police On My Back
3:17


iPad
4:15 PM
Summary
60%
Report that new technology has made life at their practice easier
26%
Have a computer that is less than one year old
73%
38%
2011
2012
Doctors who are using a computer 3+ years old
Electronic Medical Records (EMR)
Search
Small Medical Practice
2-9 practioners
Overall career satisfaction
2012
2011
89% of doctors say they are satisfied or extremely satisfied
The most positive trend for doctors was advancements in medicine.
Top negative pressures
Insurance and reimbursement 69%
Patient compliance issues 64%
Practice administration 48%
What do doctors know about Meaningful Use?
4% expert
53% advanced
43% novice
Advancements in medicine
Increased patient compliance
Improvement in workforce
Positive trends affecting doctors
45% of doctors say they are doing better compared to last year
50%
40%
30%
20%
10%
Doing better
No change
Doing worse
We asked doctors how they are doing


Practice Makes Money
Patient In
Patient Out

# Rethink EHR


I SPENT MORE OF MY CHILDHOOD PLAYING VIDEO GAMES THAN I SPENT DRAWING OR WRITING OR ET CETERA.

FACT: GAMES = FUN.


DIABLO III
BLIZZARD ENTERTAINMENT

# Goal 1: We want it ~~Now~~ Yesterday

# Goal 2: Open Anywhere for Anyone

# Makes Security Interesting

# Where Do We Start?

# EHR Security 101

HIPAA

HITECH ACT

INFORMATION

# HIPAA in a Slide

- Holistic Attempt at Security
  - Administrative
  - Physical
  - Technical
- Documentation
  - Policies, Procedures, Standards
- Consistency
  - Follow the documentation
- Subject to Interpretation

# HIPAA – Beyond Security Best Practices

- Training
- Information Security Officer
- Periodic Risk Assessments and Audits
- Identify PHI and Define Boundaries
- Data Retention Requirements

# HITECH in a Slide

- Combination of Incentives and Penalties
- Enforcement of HIPAA
  - Mandatory Penalties up to $1.5 million
  - HHS required to conduct periodic audits
- Notification of Breach
  - Breach of > 500 patients will result in public disclosure
- Right to PHI
  - Personal
  - Delegated Authority
- Business Associates
  - Subject to HIPAA Security Rule
  - Subject to civil and criminal penalties

# How can I Qualify for HITECH Incentives?

1) Adopt a Certified EHR

2) Check Eligibility and Register

3) Meaningfully Use your EHR

4) Apply for HITECH Incentives

- **Core Requirement 15: Conduct Privacy and Risk Audit**

# What's with the Cloud?


# Yes – We are in the Cloud

- We use private + public cloud
- ain't perfect
- ain't broken
- Cloud FUD
- Cloud does not provide or break HIPAA compliance
  - They provide the tools
- Cloud Security is getting better

# Physical Security

- Armed Guards
- Surveillance Systems
- Access Card/Biometric Authentication
- 24/7/365 Monitoring
- Redundant Utilities
- Man Traps
- Concrete Structures
- Fire Detection and Flood Protection
- List goes on..

# Top 5 Breaches

| Covered Entity | Individuals Affected | Year | Type |
|---|---|---|---|
| TRICARE Management Activity (TMA) | 4,901,432 | 2011 | Backup Tapes |
| HeaHealth Net, Inc. | 1,900,000 | 2011 | Lost Drives |
| New York City Health & Hospitals Corporation's North Bronx Healthcare Network | 1,700,000 | 2010 | Lost Drives |
| AvMed, Inc. | 1,220,000 | 2009 | Lost Laptop |
| The Nemours Foundation | 1,055,489 | 2011 | Lost Backup Tapes |

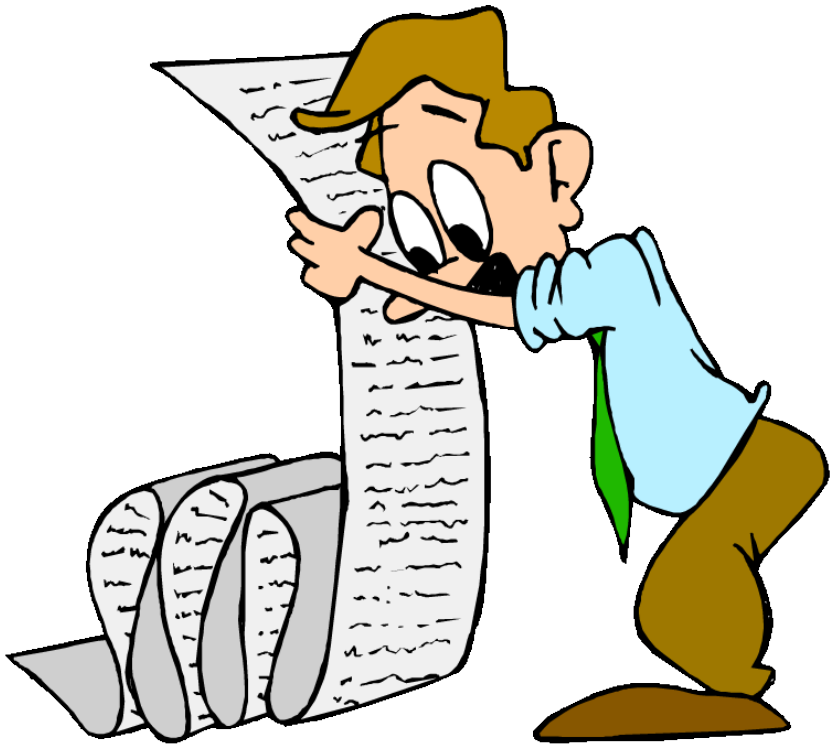
* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html


PROBLEM
SOLVED

# Yes – We do have the Standard Challenges

# We do have the Standard Solutions

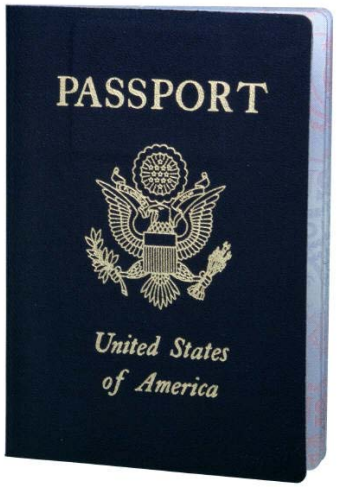
- Background Checks ✓
- Isolation of PHI ✓
- Segregation of Roles ✓
- Malware Detection ✓
- Strong Cryptography ✓
- Firewalls, IPS, VPN ✓
- List goes on..




Select Level
1
2
1

# Identify to Proceed

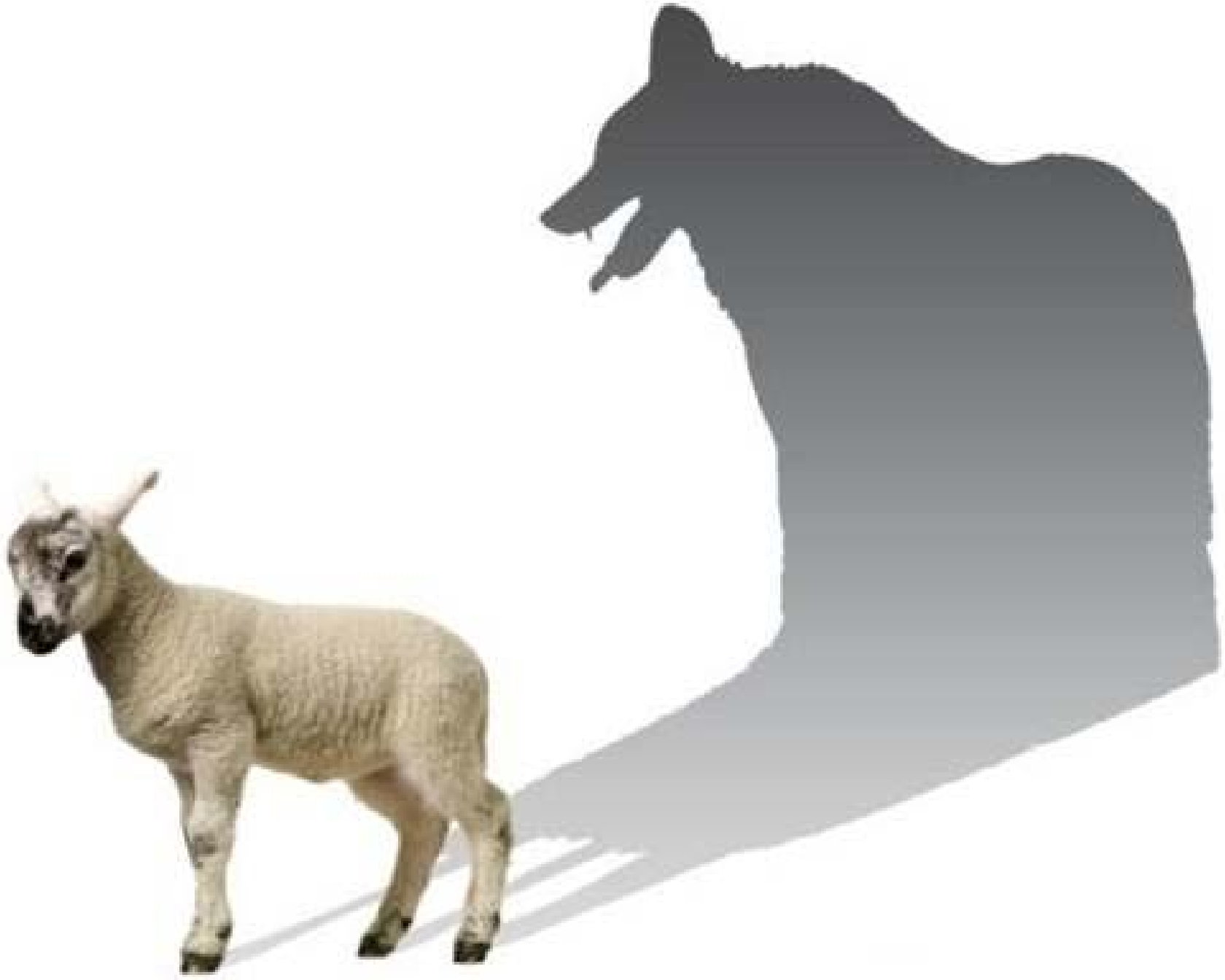

Rx




National
Provider
Identifier

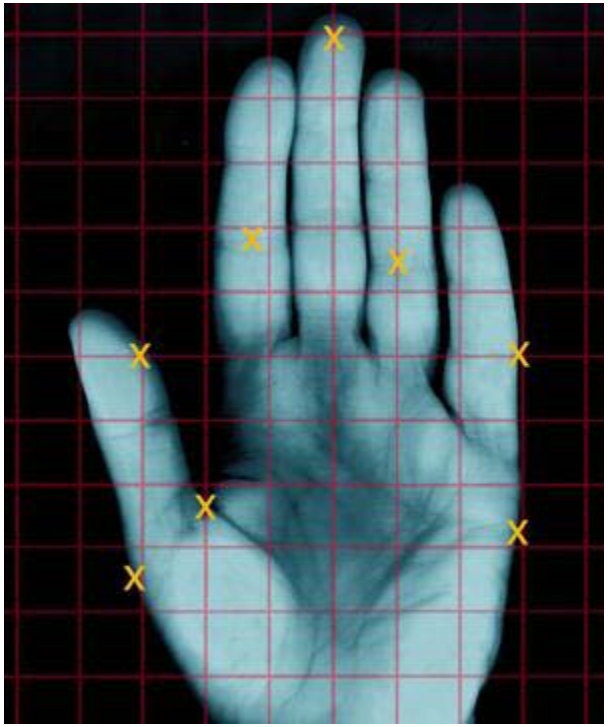
1245294826

Signature



# Authentication and Identification

- Successful Authentication
  - Practice Identifier
  - Username
  - Password
- Password Hashing
  - SHA-512
  - Random Salt
- Account Lockout
- Audit Logs



# How do you Protect Against Password Reuse?

- Beyond Username + Password
- Practice Identifier has served well

# Cryptography

- All EHR calls are encrypted (HTTPS)
  - Support for strong ciphers (128 bit and above)
  - Disable support for weak encryption
- Passwords are hashed
  - SHA-512
  - Random Salt
- Backups are encrypted
  - No physical media
- Laptops are protected using Full Disk Encryption
  - Equipment will get stolen/lost

# We Know Our Application Better

```
if (Authorize.IsUserAuthorized("Chart ", i_Session.lUserID,
Authorize.UserAccessEntity.Patient, lPatientID,))
{
      .....
}
else
{
      throw new BL_Exception(XXXX);
}
```

local & organic

# This Code Path is Used ☹

```
                    INFO  PF.BusinessLogic.Utilities.Log - !! Error in the PracticeManagement web service
!! Method:
!! WS caller address:         4.171; name:
Base Exception message: Practice Fusion Application Server Exception
BL_Exception fields:
  Error Number:     320
  Category:         Authorization
  Display Message:  User does not have rights to execute this call
  Internal Message: Web Service call failed
  Severity:         4
  Message Type:     OperationFailure
  Description:
!! ExceptionMessage: Practice Fusion Application Server Exception
2012-08-03                  INFO  PF.BusinessLogic.Utilities.Log - Call Elapsed Time = 0.0936 s
2012-08-03                   INFO  PF.BusinessLogic.Utilities.Log - BL_VitalsStandard.                called: PracticeID=       PatientID=
```

# Security is ~~My~~ Everyone's Responsibility

# Starbucks Workforce

- Workers cannot be confined any longer
- BYOD
- IT as Business Enabler

# Think Beyond Boundaries

- **Goal : Any where anytime protection**
  - **Device Verification**
  - **User Verification**
  - **Web Traffic Filtering**
  - **Device Encryption**

# Reduce Risk

# Isolate PHI and Business

- Employees provides EMR
- EMR uses PHI
- Employees do NOT need access to PHI

# Social Engineering

- Problem: Humans are nice
- Strong verification processes
  - Physical
  - Support
  - Application
- Awareness about Social Engine
  - Enforcement of the process is the
- Never Reveal Passwords

# Clinical Research

- **Safe Harbor Rules**
  - De-Identify PHI
  - 18 Identifiers (Name, Address, Dates, SSN ..)
- **We go above and beyond the safe harbor rules**
  - Remove records for individuals older than 80
  - Remove records for individuals with rare conditions

# Patient Access to their Records

- Holy Grail: One Patient One Record

- Several Challenges
  - Incomplete records
  - Incorrect records
  - Lack of Standards
  - Lack of Policy
- Currently: Practitioner provisions a patient account
- Meaningful Use Criteria?

# Privacy != Security

- We need clear/consistent privacy rules


- Lack of rules causing
  - Too cautious approach
  - Too risky approach
  - Silos in the industry
- Security know how exists to enforce the rules

# What Keeps Me Up

- Zero Days
  - Underground marketplace for vulnerabilities
- Targeted Attack
  - Social Engineering + Zero Days

# What will the Future Bring?

# Goal 3: Healthcare Ecosystem

- Online Referrals
- Labs
- eRx
- Billing
- Health Personalization
- Healthcare Apps

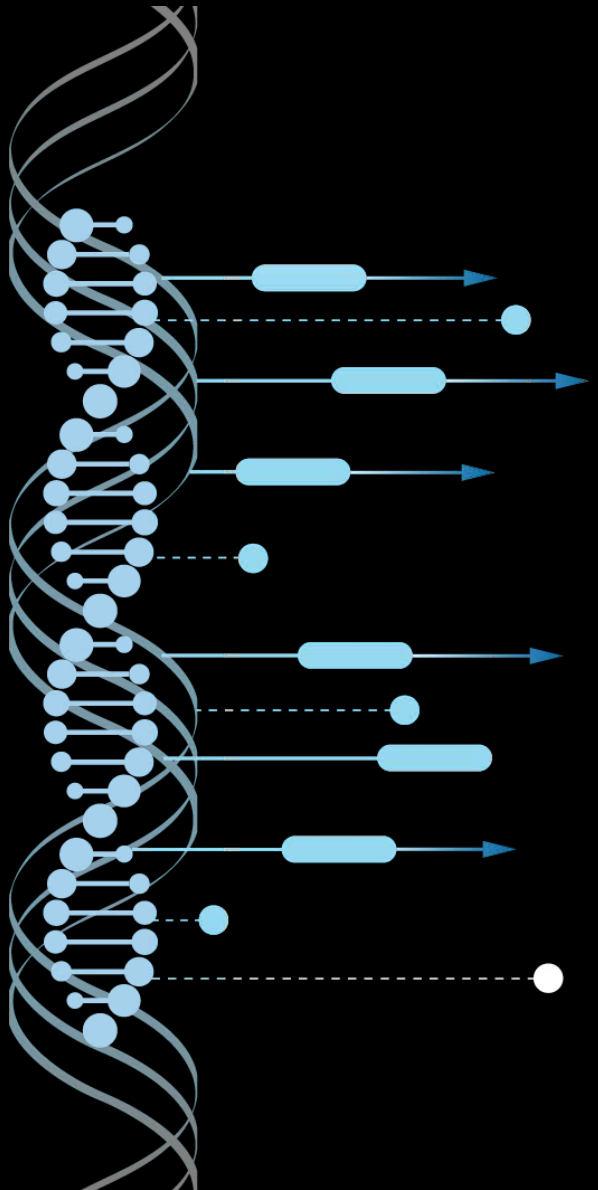
# Health Information Exchange

- A few regional success stories
- Trust/Participation is lacking
- Little integration between HIEs
- Do we want one size?

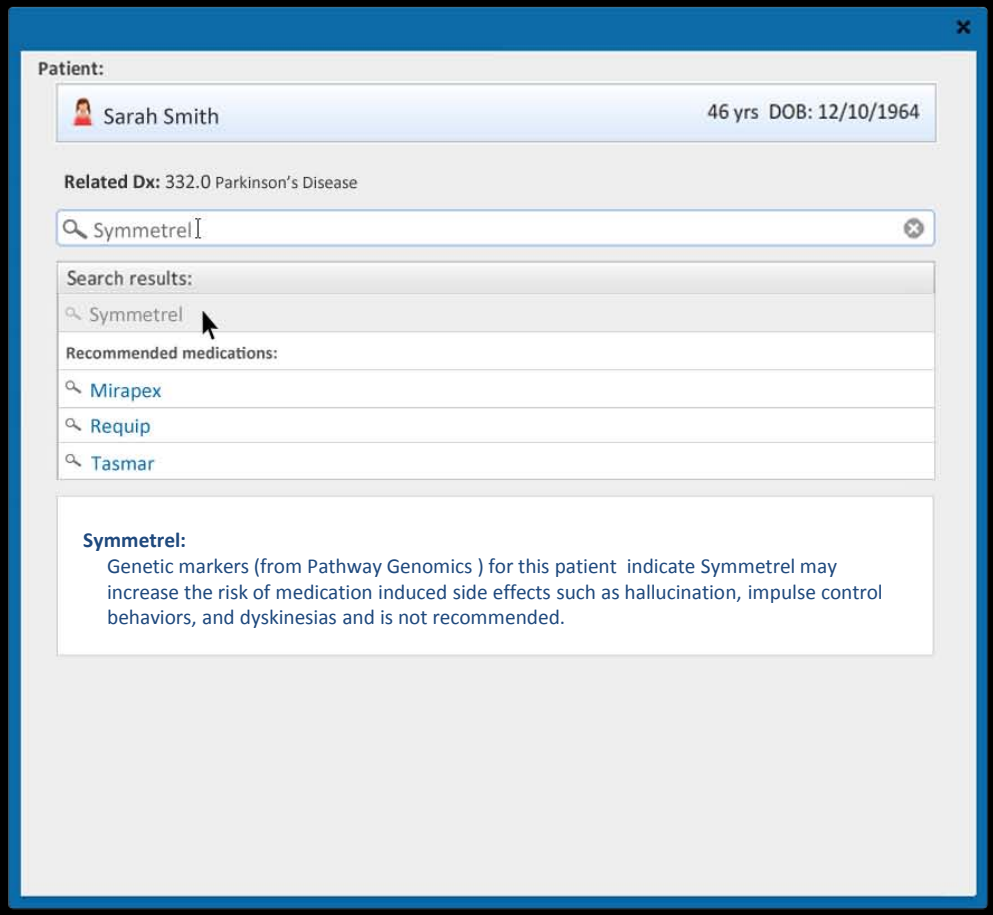
# Comprehensive Health Care

# Personalized Medicine

Pathway Genomics Genetic Information



eRx Portal




HARD
WORK
AHEAD