

Biolnformatics and Security Technology in São Paulo and the US

NINA ALLI

H2HC - SÃO PAULO, BRASIL

Medical Ecosystem

SPOT THE PATIENT?



Why is MedTech InfoSec so fucking hard?



“HOPE” ISN’T A SECURITY STRATEGY



HOW DID WE GET TO THIS POINT: QUICK BACKGROUND

Technologic Pillars of Care

DEVICES

IMPLANTABLES

PATIENT MONITORS

LIFE SUPPORT SYSTEMS

SURGICAL TOOLS

IMAGING MACHINES

INFRASTRUCTURE

ELECTRONIC MEDICAL RECORDS

LABORATORY ORDERS

TELEMEDICINE

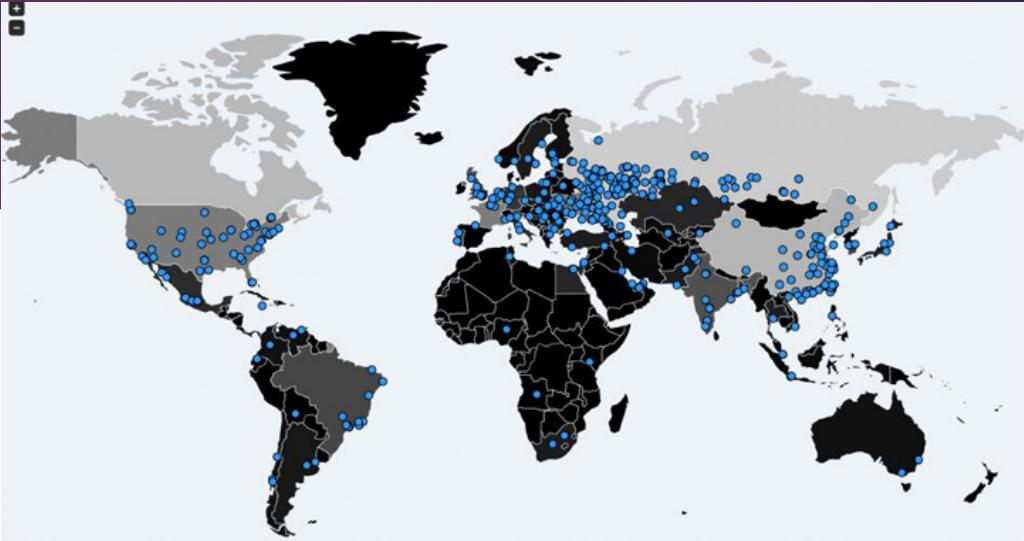
PUBLIC HEALTH

POWER GRID

Pain Points?

Latest Industry Issue:
WannaCry

- ▶ Isolated Silos
- ▶ Operating Systems
- ▶ Servers



Still more to come:
What will be done with the remaining NSA leaked
hacks?

“Healthcare data represents the ‘holy grail’ in terms of data theft.”



Patient Identity Theft: PHI/PII what can they steal?

- ▶ Patient First, Middle, Last Names
- ▶ Address
- ▶ DoB
- ▶ SSN
- ▶ Telephone Number
- ▶ CC info
- ▶ Drivers License
- ▶ Passport Info
- ▶ Insurance
- ▶ Blood Type
- ▶ Allergies
- ▶ Medications
- ▶ Diagnoses
- ▶ Procedures
- ▶ Emergency Contact - name and phone number
- ▶ NOW INCLUDING!!!
GENOMIC/DNA Data

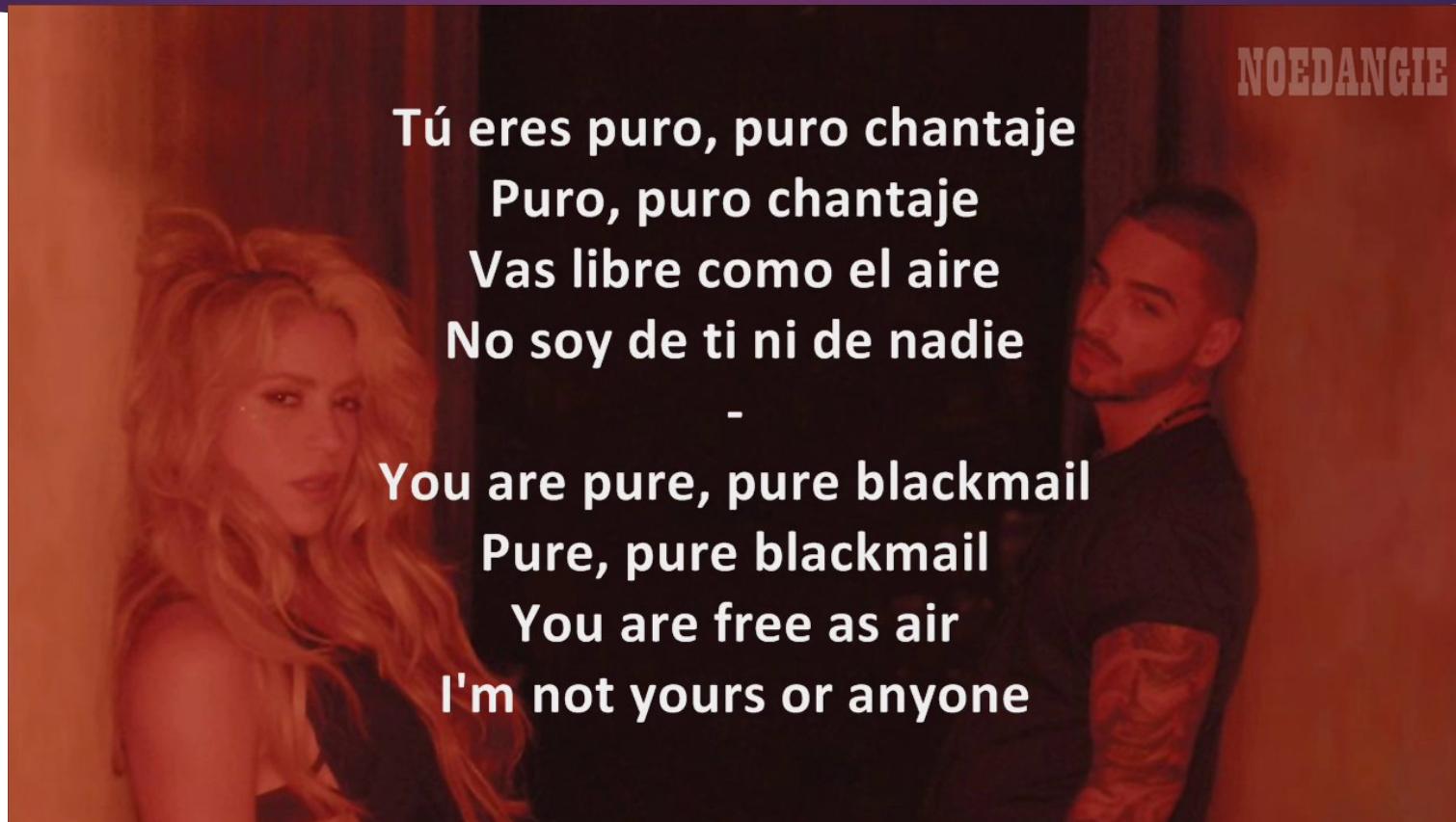
Dream Market and Alpha Bay

The screenshot shows a dark-themed web browser interface for the Dream Market. The top navigation bar includes links for 'Most Visited', 'Learn more about Tor', and 'The Tor Blog'. The main content area displays a grid of product listings:

- MEDICAL FULLZ (DOB, SSN, PHOTO, Insurance, Drugs)**: \$0.99 by TuttiFrutti_store (50) (4.88★). WW → WW. Includes a photo of a person in a mask holding documents. **ESCROW** button.
- Track 1/2 atm cards with pin - Dumps with pin cont**: \$10 by octopussi (36) (4.80★). WW → WW. Includes a photo of several credit cards. **ESCROW** button.
- 5g Critical-Mass AAA+**: \$60.2 by CLUBMEDIA (600) (4.93★). DE → EU. Includes a photo of marijuana buds. **NO ESCROW** button.
- 1 GR BLONDE HASH SUPER POLM**: \$14.24 by POWERSALES (13) (5.00★). DE → DE, EU. Includes a photo of hash. **ESCROW** button.

Pagination at the bottom shows pages 1 through 17, with page 7 currently selected. Navigation arrows are available for pages 18 and 2647.

What does this leave patient data open to?



Who wants this info and why do “THEY” care so much?



COST OF BUSINESS OR ACTIVITIES OF DAILY LIVING

- ▶ \$ of ONE Medical Record:
500 - 1000 USD vs 40 - 1000 LATAM

- ▶ \$ of ONE credit card:
50-150 USD vs 2-5 LATAM

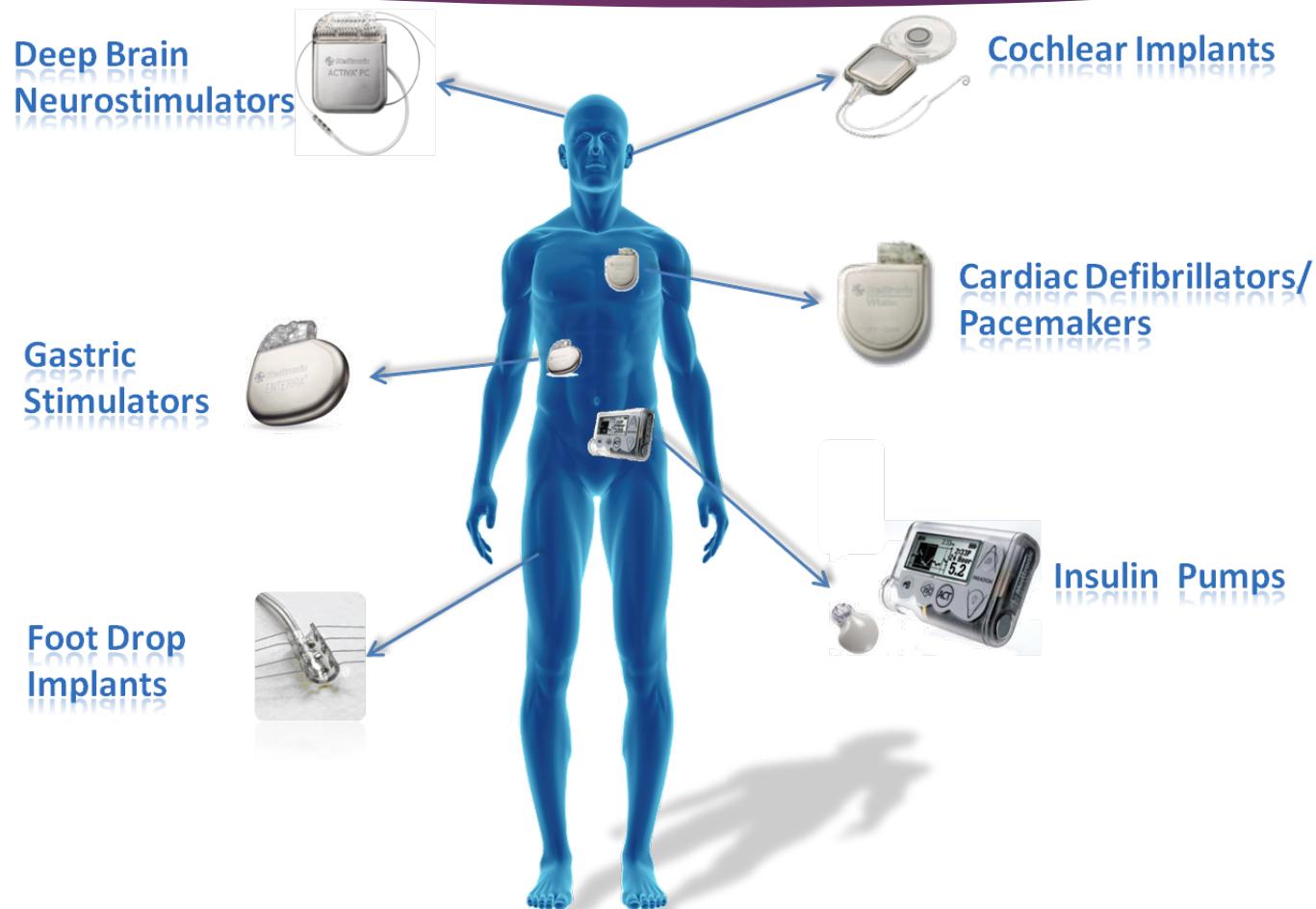
- \$ of Medical Database
- 5000-10,000 USD

Fun Attack Vectors

- ▶ EASY: LISTEN
- ▶ MEDIUM: LOOK
- ▶ COMPLEX: DO

Medical Devices

WIRELESS IMPLANTABLE MEDICAL DEVICES



Sharing Patient data



internet Tender: Bitcoin



- ▶ Obfuscated funding
- ▶ Anonymity
- ▶ Non-traceable
- ▶ Quick turnover and release

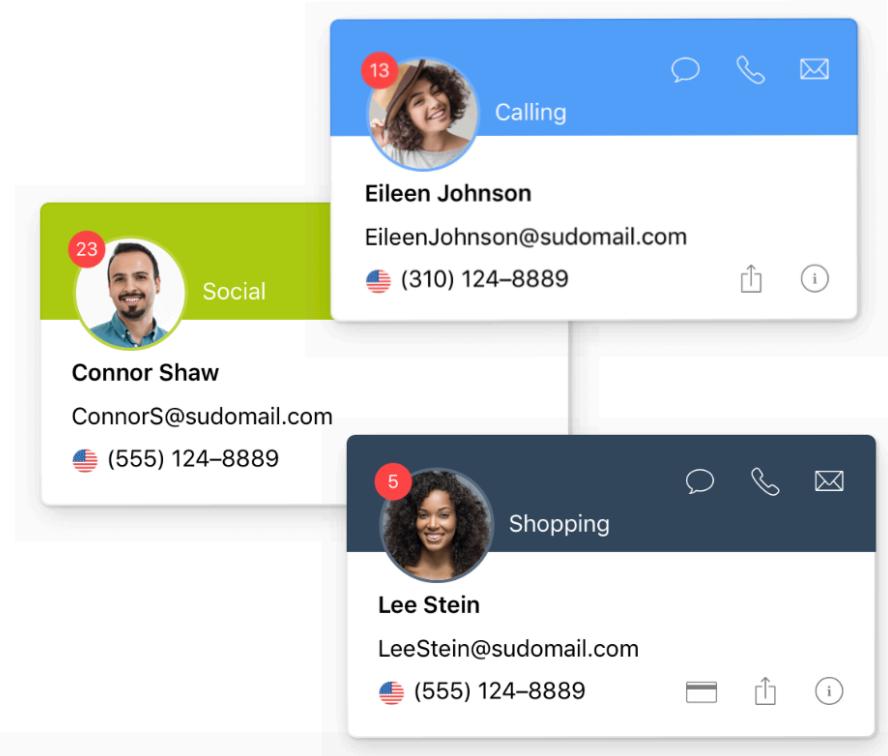
Recent patient attack: Plastic surgery clinic says “we wont Pay”



Hi, My name is . . .

Create special-purpose
avatars for any situation.

Have up to 9 Sudo avatars for free.
Each includes a custom phone number,
email address, private browser and
SudoPay virtual cards.



How can we take better care of Healthcare Information technology?

- ▶ Security:
- ▶ Boot to Root



Simple Guidelines to Better security

Assist doctors and hospitals in improving quality of care for patients

Publish transparent ratings on usability and security to transform information technology

Prevent information blocking

Enhance interoperability

Leverage health information technology to improve patient care

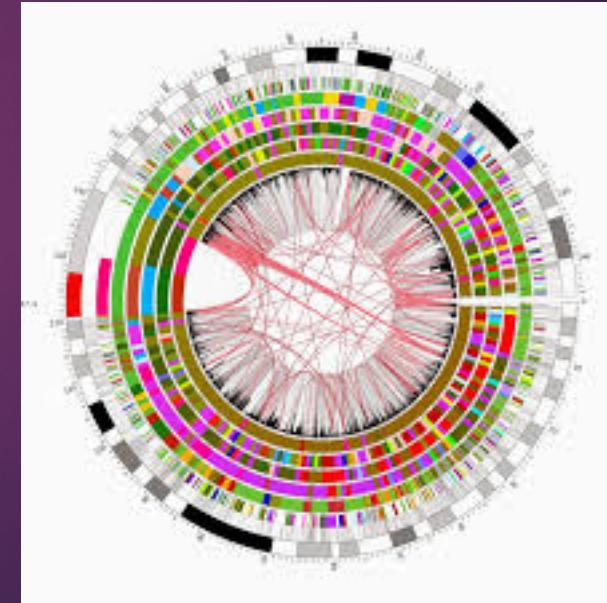
Empower patients and improving patient access to their electronic health information

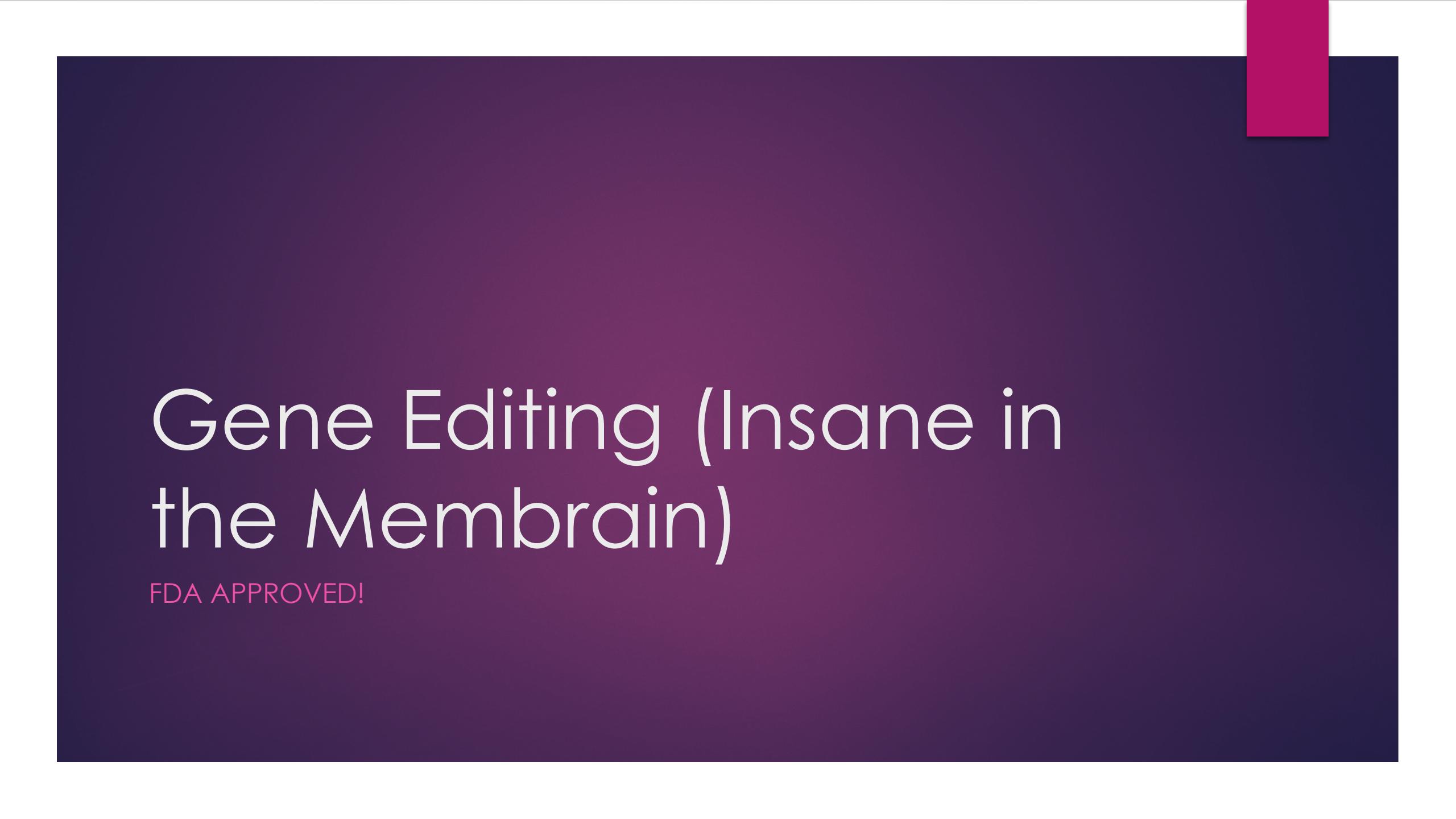
Direct Govt Accountability Office to study patient matching



AI in Healthcare

IBM WATSON, APPLE,





Gene Editing (Insane in the Membrain)

FDA APPROVED!

New Discoveries!

MISSING HIV COMPONENT FOUND

Big Data

TO THE RESCUE?

Paradigm Shift

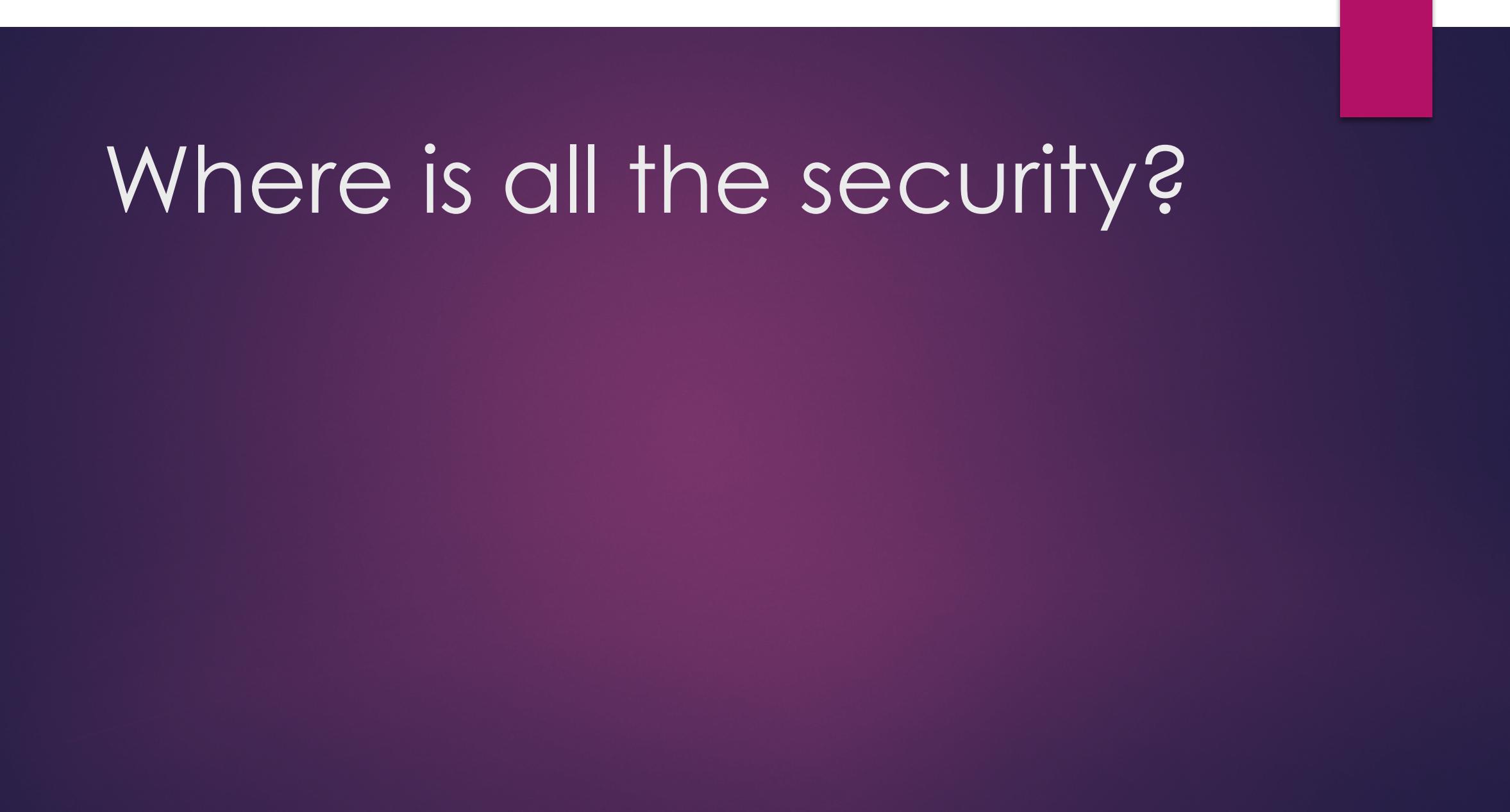
BIOHACKING

Politics

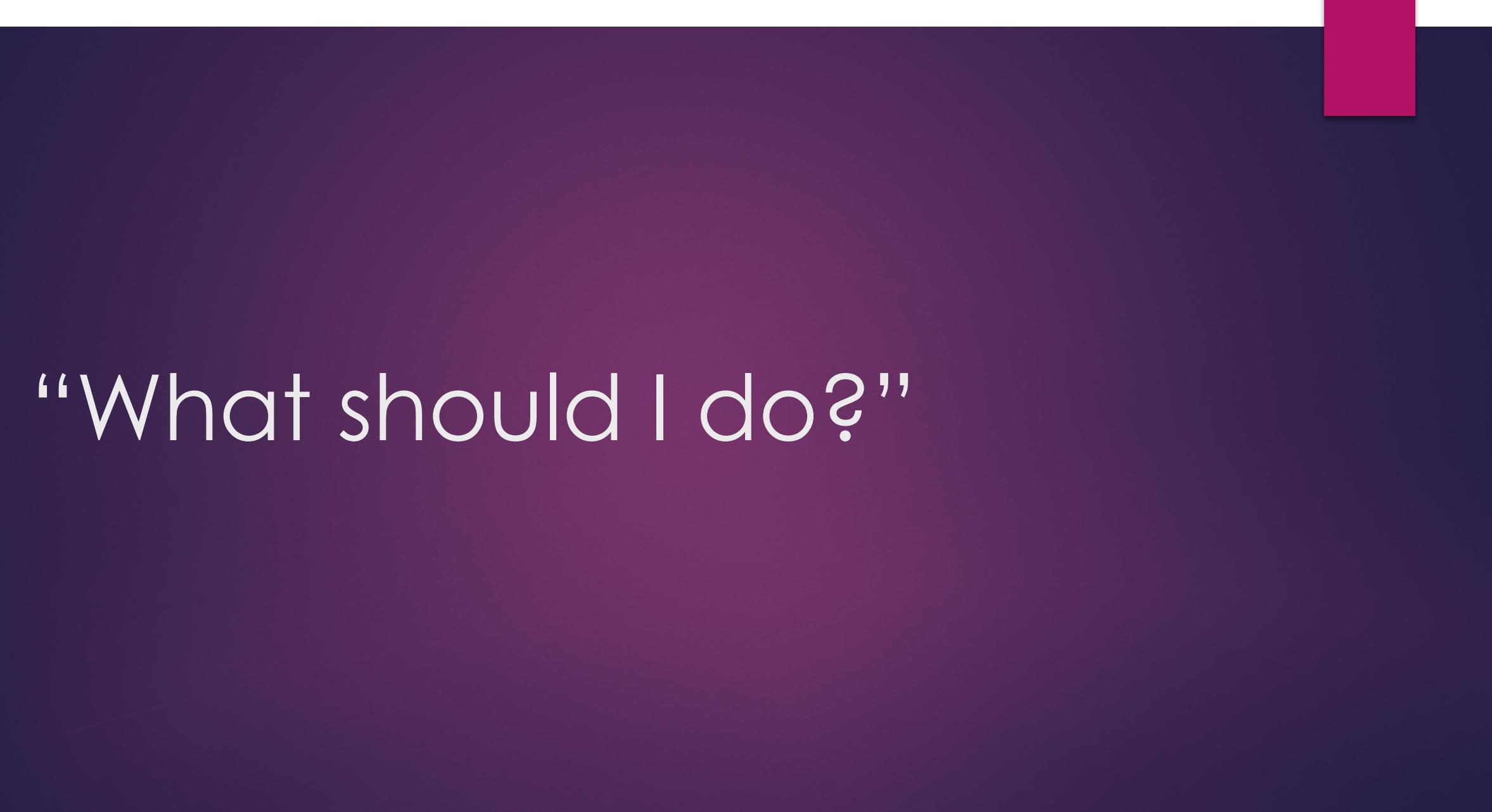
WHO KNEW MEDICINE WAS THIS HARD?

Incident Response and Forensics

THE DOCTOR WILL SEE YOU NOW...



Where is all the security?



“What should I do?”

!!!HIRE A HACKER!!!

!!!HIRE A HACKER!!!

!!!HIRE A HACKER!!!

DEF CON

BIOHACKING VILLAGE





Ordem e Progresso

Obrigada

NINA ALLI

@HEADINTHEBOOTH