

The background features a digital theme with glowing blue and green circuit patterns. Several padlocks are scattered across the scene, some in white and some in dark grey, symbolizing security and data protection. A dark grey horizontal band is positioned behind the main title text.

HOW TO STAY HIPAA COMPLIANT WITH MOBILE DEVICES

EMERGING TRENDS COMMITTEE HOT TOPICS

M.E.D.X App Presentation

A solid orange horizontal bar at the bottom of the slide.

DISCLOSURE

RIKESH T. PARIKH, M.D. CO-FOUNDER OF MOBILE ENCRYPTED DATA XCHANGE (M.E.D.X)

A peer-to-peer, HIPAA-compliant, mobile app for Android and iOS used to secure texting, photo, video, and document communications.



SUMMARY

- BACKGROUND OF CURRENT REGULATIONS REGARDING HIPAA WITH MOBILE DEVICES
- THE RISING USE OF THE SMARTPHONES IN THE WORKPLACE
- RISE IN MOBILE DEVICE BREACHES
 - EXAMPLES OF HIPAA TECHNOLOGICAL BREACHES AND FINES
- HOW PROTECTED HEALTH INFORMATION (PHI) IS STORED AND TRANSFERRED ON THE MOBILE DEVICE
- SECURING THE SMARTPHONE WITH ENCRYPTED APPS & A COMPARISON OF DIFFERENT APPS IN THE MARKET
- OVERVIEW OF HOW TO STAY SECURE ON THE MOBILE DEVICE

BACKGROUND >

LEGAL – PRIVACY AND SECURITY

THE HIPAA SECURITY RULE: ESTABLISHES A NATIONAL SET OF SECURITY STANDARDS FOR THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI). THE HIPAA SECURITY RULES APPLY TO COVERED ENTITIES.

COVERED ENTITY: ANY ENTITY INCLUDING HEALTH CARE PROVIDERS AND PROFESSIONALS SUCH AS DOCTORS, NURSES WHO TRANSMIT HEALTH INFORMATION IN ELECTRONIC FORM IN CONNECTION WITH CERTAIN TRANSACTIONS MUST COMPLY WITH THE RULES' REQUIREMENTS TO PROTECT THE PRIVACY AND SECURITY OF HEALTH INFORMATION, EVEN WHEN USING MOBILE DEVICES.

BUSINESS ASSOCIATE: A PERSON OR ENTITY WHO PERFORM CERTAIN FUNCTIONS OR ACTIVITIES THAT INVOLVE THE USE OR DISCLOSURE OF ePHI ON BEHALF OF OR PROVIDE SERVICES TO A COVERED ENTITY. A MEMBER OF THE COVERED ENTITY'S WORKFORCE IS NOT AN BUSINESS ASSOCIATE.



BACKGROUND > EMERGING TRENDS

- RISE IN MOBILE DEVICE USE IN THE HEALTHCARE WORKFLOW
- RISE IN HIPAA AUDITING (PHASE 2)
- RISE IN HIPAA VIOLATIONS AND FINES

BEING “*HIPAA COMPLIANT*” IS A MISNOMER

IT IS REALLY ABOUT CONSTANTLY *MITIGATING RISK* IN YOUR WORKPLACE

BACKGROUND > EMERGING TRENDS

RISE OF MOBILE DEVICE USE IN HEALTHCARE



*Data comes Wolters Kluwer 2013 Physician Outlook Survey conducted by Ipsos.

BACKGROUND >

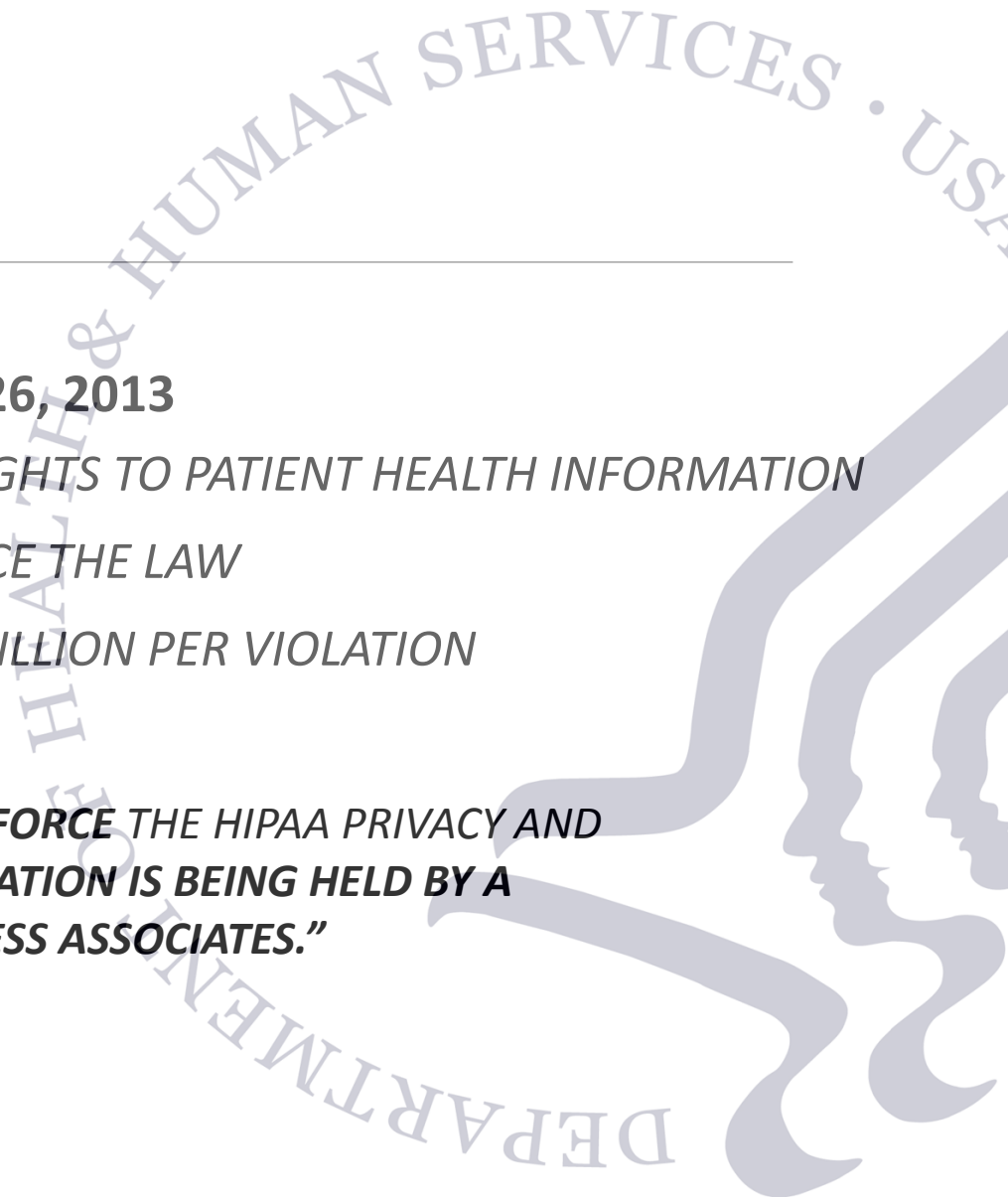
LEGAL – GAME CHANGER

FINAL OMNIBUS RULE: WENT INTO EFFECT ON MARCH 26, 2013

- ENHANCED PATIENT PRIVACY PROTECTION WITH NEW RIGHTS TO PATIENT HEALTH INFORMATION
- STRENGTHENED THE GOVERNMENT'S ABILITY TO ENFORCE THE LAW
- POTENTIAL FINES INCREASED TO A MAXIMUM OF \$1.5 MILLION PER VIOLATION

*“THESE CHANGES **STRENGTHEN** THE ABILITY OF MY OFFICE **TO ENFORCE** THE HIPAA PRIVACY AND SECURITY PROTECTIONS, **REGARDLESS OF WHETHER THE INFORMATION IS BEING HELD BY A HEALTH PLAN, HEALTHCARE PROVIDER, OR ONE OF THEIR BUSINESS ASSOCIATES.**”*

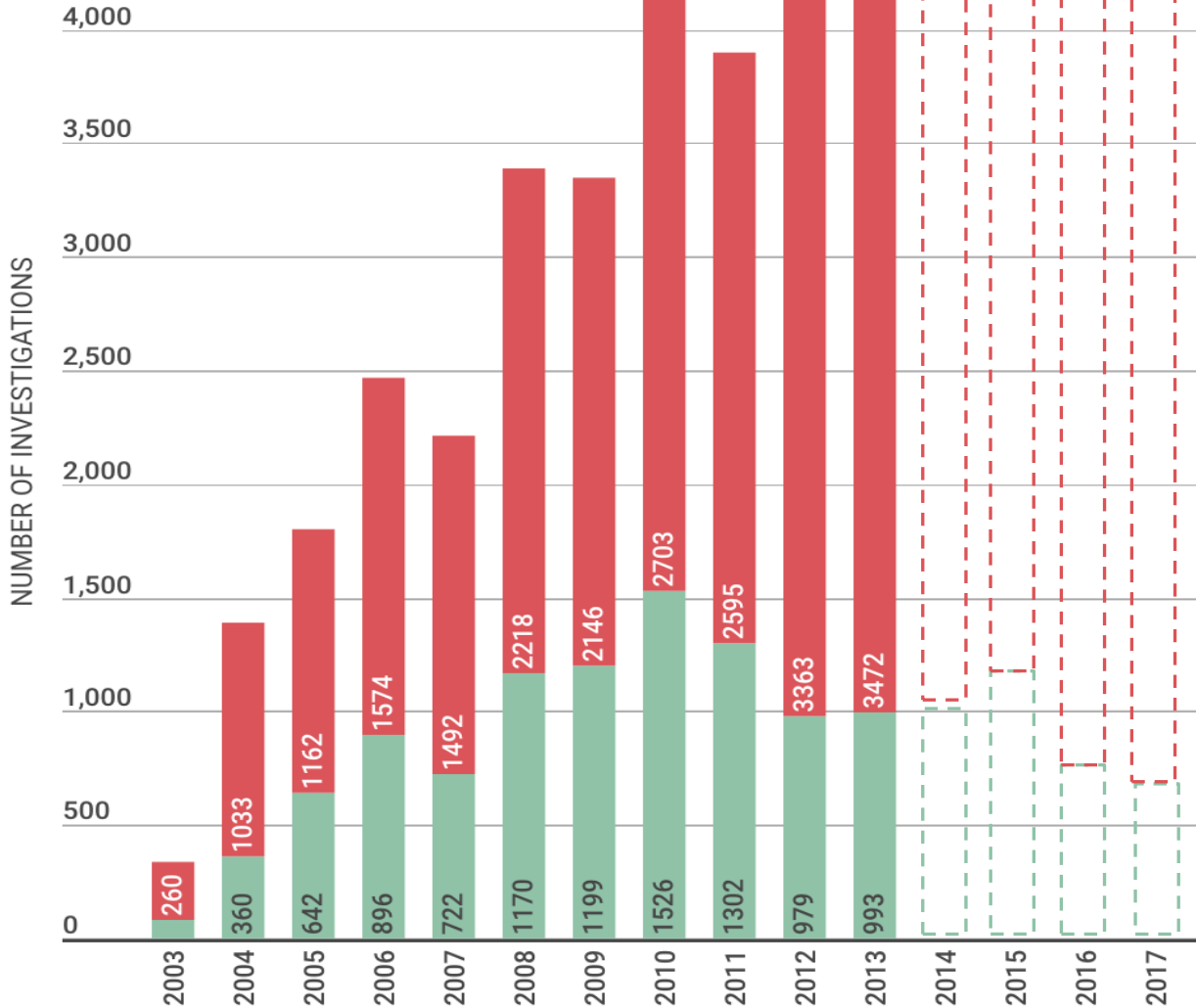
LEON RODRIGUEZ
FORMER DIRECTOR OF THE HHS OFFICE FOR CIVIL RIGHTS



BACKGROUND > LEGAL – GAME CHANGER



Omnibus Rule 2013



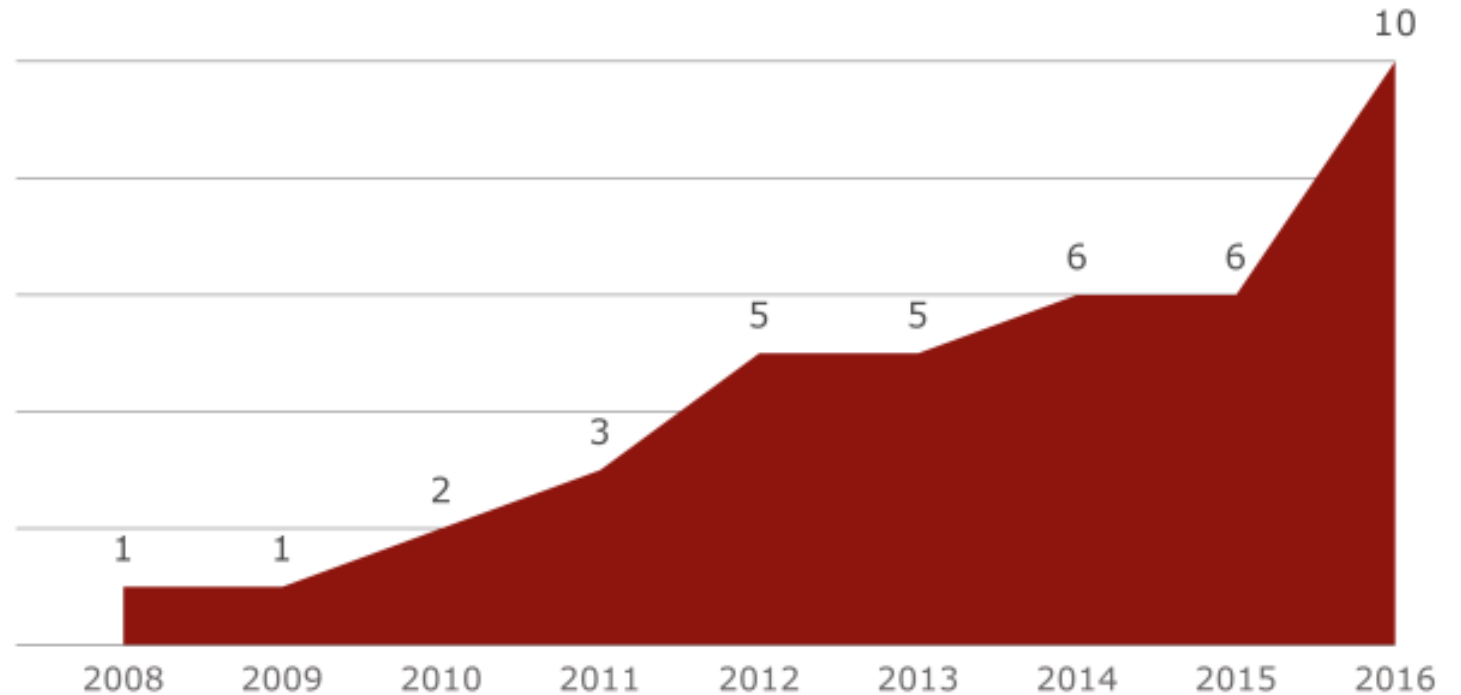
RISING BREACHES AND FINES >
HHS INVESTIGATIONS
SINCE 2003

● No Violation ● Corrective Action Taken (including fines)

RISING BREACHES AND FINES > MAJOR SETTLEMENTS: 2008-2016

THESE MAJOR SETTLEMENTS ARE QUITE HIGH: THE **AVERAGE AMOUNT FOR THE 10 issued IN 2016 IS MORE THAN \$2 MILLION.**

“We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals’ ePHI is secure.”

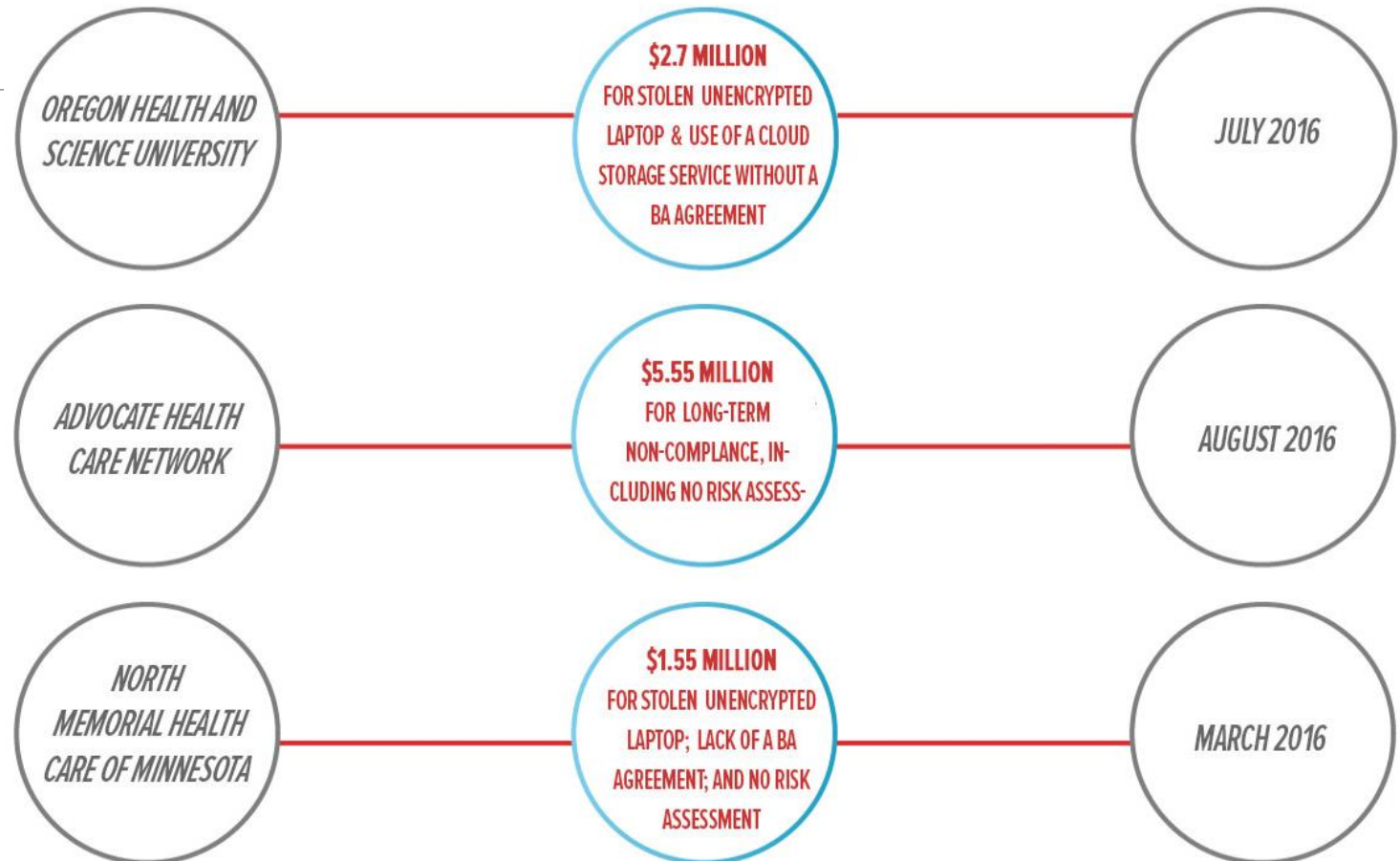


Source: HHS

RISING BREACHES AND FINES > CASE STUDIES

June 9, 2016 – AN OREGON PSYCHIATRIST USED A CELL PHONE TO PHOTOGRAPH A PATIENT CENSUS SHEET (WITH MULTIPLE INSTANCES OF PHI) AND ACCIDENTALLY SENT IT TO SIX PEOPLE.

April 17, 2014 – A STOLEN IPHONE THAT WAS NOT ENCRYPYTED OR PASSWORD PROTECTED HAD THE ePHI OF 412 PATIENTS. FURTHER INVESTIGATION REVEALED THAT CATHOLIC HEALTH SERVICES OF PHILADELPHIA HAD NOT COMPLETED A RISK ANALYSIS OR RISK MANAGEMENT PLAN. **ON JUNE 29, 2016, THEY SETTLED FOR \$650,000.00**

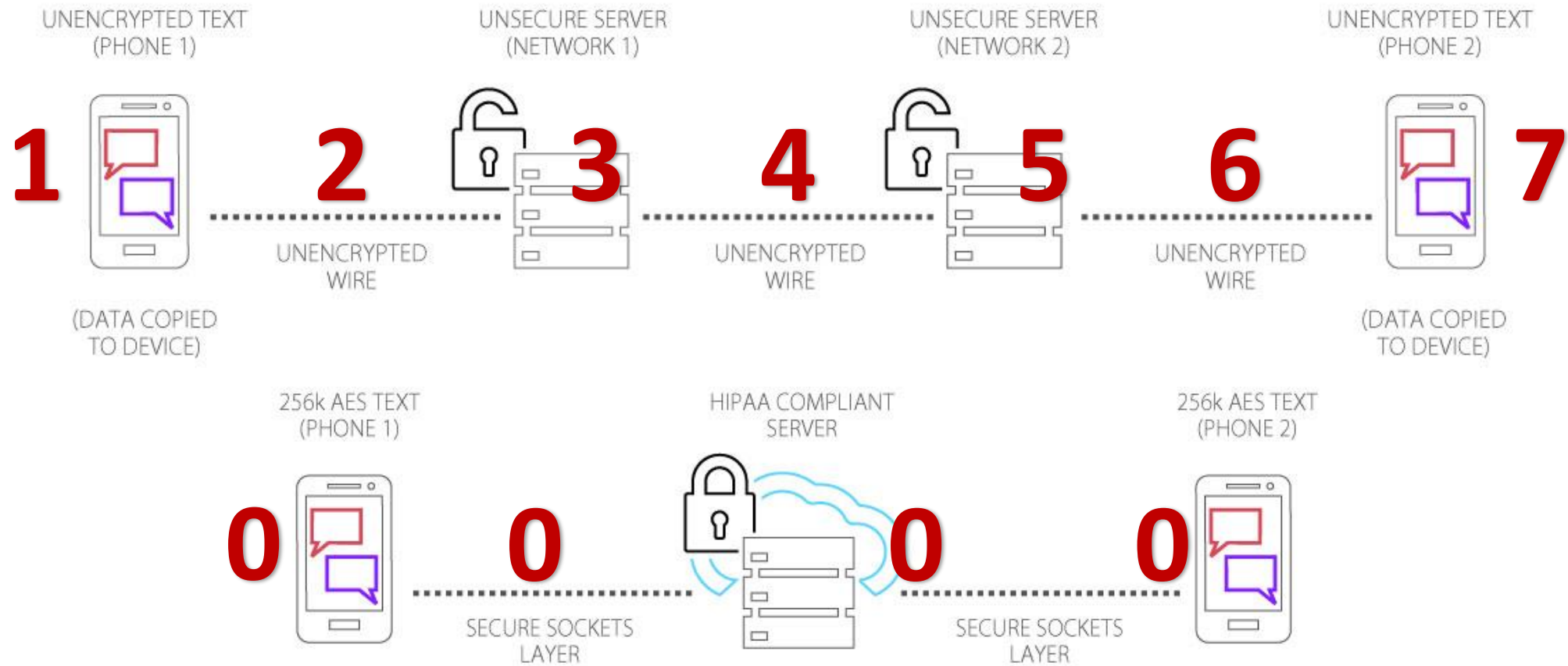


PHI STORAGE ON THE MOBILE DEVICE

80% OF DOCTORS AND NURSES USE THEIR SMARTPHONE FOR WORK PURPOSES RESULTING IN POTENTIAL STORAGE AND TRANSFER OF ePHI



PHI TRANSMISSION ON THE MOBILE



WHO IS SENDING PHI?

*“A LARGE PART OF THE APPEAL OF MOBILE APPLICATIONS TO PHYSICIANS IS THAT **APPS ARE EASILY INTEGRATED INTO THEIR WORKFLOW** -- DELIVERING INFORMATION WHEN AND WHERE THEY NEED IT.” - COMMONWEALTHFUND.ORG*



NOW WHAT?

IGNORE



RESIST THE TREND



BE PREPARED



STEP 1:

Protecting Yourself and your Office

INCLUDE MOBILE DEVICES IN YOUR ONGOING RISK ASSESSMENTS

- ❑ **ASSESS** HOW MOBILE DEVICES AFFECT THE RISKS (THREATS AND VULNERABILITIES) TO THE HEALTH INFORMATION IN YOUR ORGANIZATION.
- ❑ **IDENTIFY** YOUR MOBILE DEVICE RISK MANAGEMENT STRATEGY, INCLUDING PRIVACY AND SECURITY SAFEGUARDS.
- ❑ **DEVELOP, DOCUMENT, AND IMPLEMENT** THE ORGANIZATION'S MOBILE DEVICE POLICIES AND PROCEDURES TO SAFEGUARD HEALTH INFORMATION.
- ❑ **TRAIN** ON MOBILE DEVICE PRIVACY AND SECURITY AWARENESS.

STEP 2: PROTECTING THE MOBILE DEVICE

4 THINGS YOU AND YOUR STAFF CAN IMMEDIATELY IMPLEMENT



USE A PASSWORD OR OTHER USER AUTHENTICATION



INSTALL AND ENABLE ENCRYPTION



ACTIVATE REMOTE WIPING AND/OR REMOTE DISABLING



START USING SECURE, BYOD APPS TO HELP MANAGE RISK

MESSENGING APP FEATURES TO LOOK FOR

- ENCRYPTION* (IN-TRANSIT AND AT-REST)
- REMOTE WIPE & LOGOUT*
- SECURE DRIVE (FOR PHOTOS, VIDEOS, AND DOCUMENTS)
- SECURE CAMERA (DIRECTLY TO SECURE LOCATION)
- NO CACHED INFO (NO DATA ON THE DEVICE)
- AUDIT TRAIL REPORTING*
- COST (SOME SOLUTIONS REQUIRE THIRD-PARTY TOOLS)

*REQUIRED BY HIPAA SECURITY RULES

