# HIPAA PRIVACY & SECURITY

**DEMONSTRATING A GOOD FAITH BUSINESS PRACTICE**

***-ENFORCEMENT***

***-OVERVIEW OF LAW***

***-BEST PRACTICE PROCESS***

**DAVID NIKSSARIAN**
**NIKSSARIAN INSURANCE SERVICES, INC.**

30 YEARS SERVING THE AGRICULTURE INDUSTRY

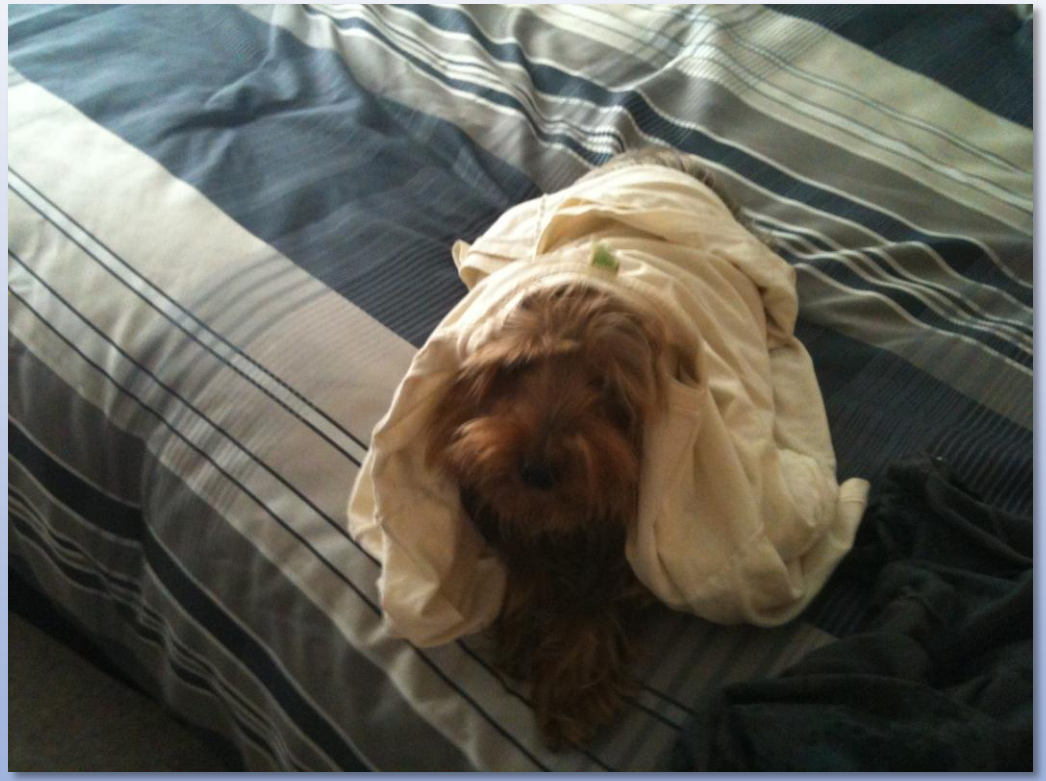
INSURANCE AGENCY SPECIALIZING IN HEALTH/EMPLOYEE BENEFIT PROGRAMS; ALSO WORKERS' COMPENSATION, AND EMPLOYMENT PRACTICES LIABILITY INSURANCE

**MARY JANE EADSON, J.D.**
**EADSON COMPLIANCE CENTER, LLC**

ENTIRE CAREER WORKING IN AGRICULTURAL INDUSTRY

LEGAL COMPLIANCE CONSULTANT TO AGRICULTURAL HR & BENEFIT DEPARTMENTS, HEALTH AGENTS AND BROKERS, TPAS, AND CARRIERS

# PENALTY ENFORCEMENT (Scary Stuff!)



# STATISTICS

- **HHS-OFFICE OF CIVIL RIGHTS HAS RECEIVED 77,190 COMPLAINTS**
  - ✓ 18,559 REQUIRED CORRECTIVE ACTION.

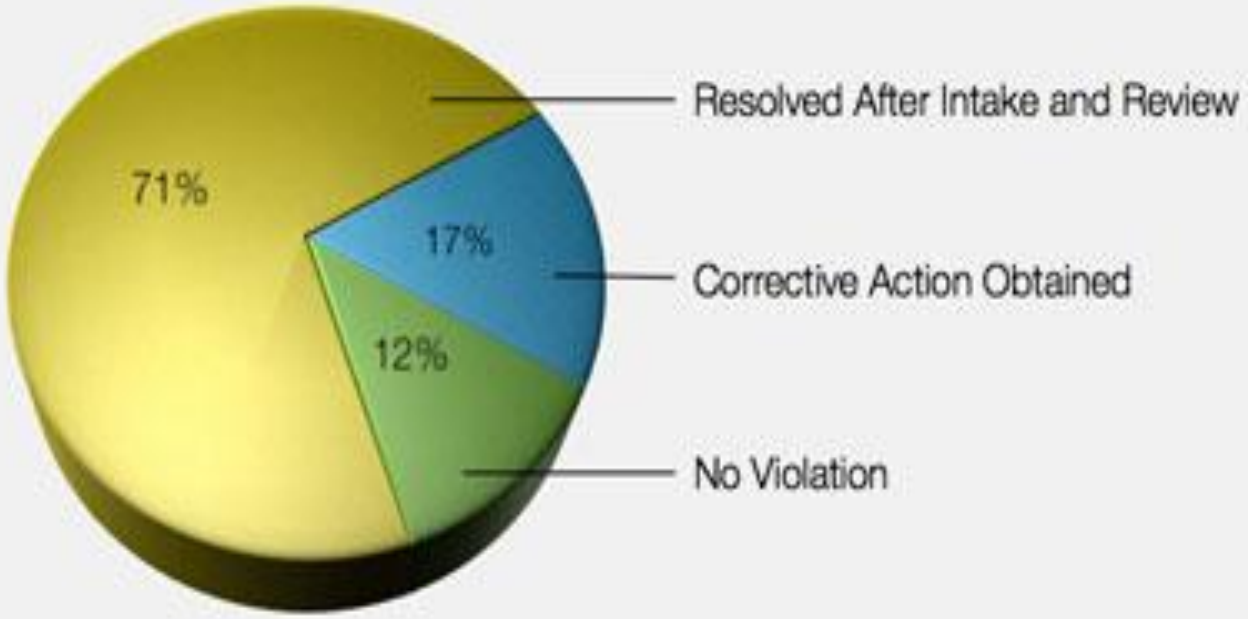
**<u>COMMON REASONS</u>**

1. **IMPERMISSABLE USE OR DISCLOSURE OF PHI**
2. **LACK OF SAFEGUARDS OF PHI**
3. **USES OR DISCLOSURE OF MORE THAN MINIMUM NECESSARY PHI**
4. **LACK OF PATIENT ACCESS TO THEIR PHI**
5. **LACK OF SAFEGUARDS OF ELECTRONIC PHI**

**PHI = PERSONAL HEALTH INFORMATION**

# Enforcement Results California

April 14, 2003 through December 31, 2010



# HEADLINES

**3/14/2012 – BLUE CROSS BLUE SHIELD OF TENNESSEE SETTLEMENT OF $1.5 MILLION**

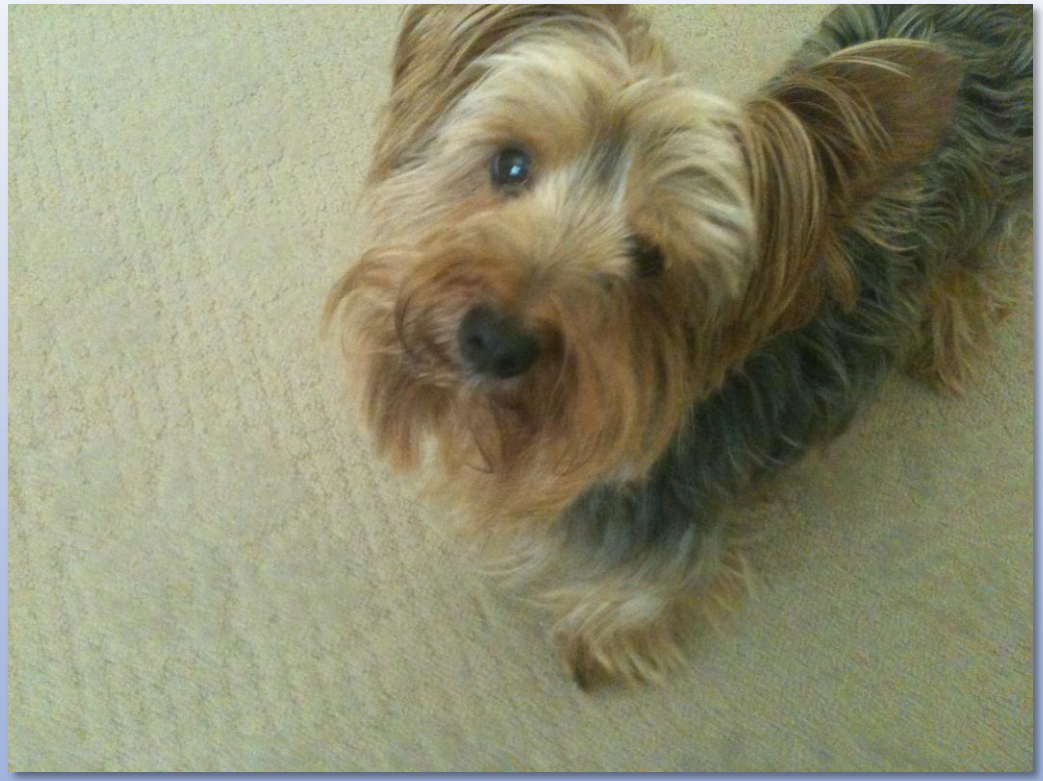
**2/22/2011 – HHS IMPOSES $4.3 MILLION PENALTY ON CIGNET HEALTH**

**2/14/2011 – MASSACHUSETTS GENERAL SETTLES HIPAA INVESTIGATION FOR $1 MILLION**

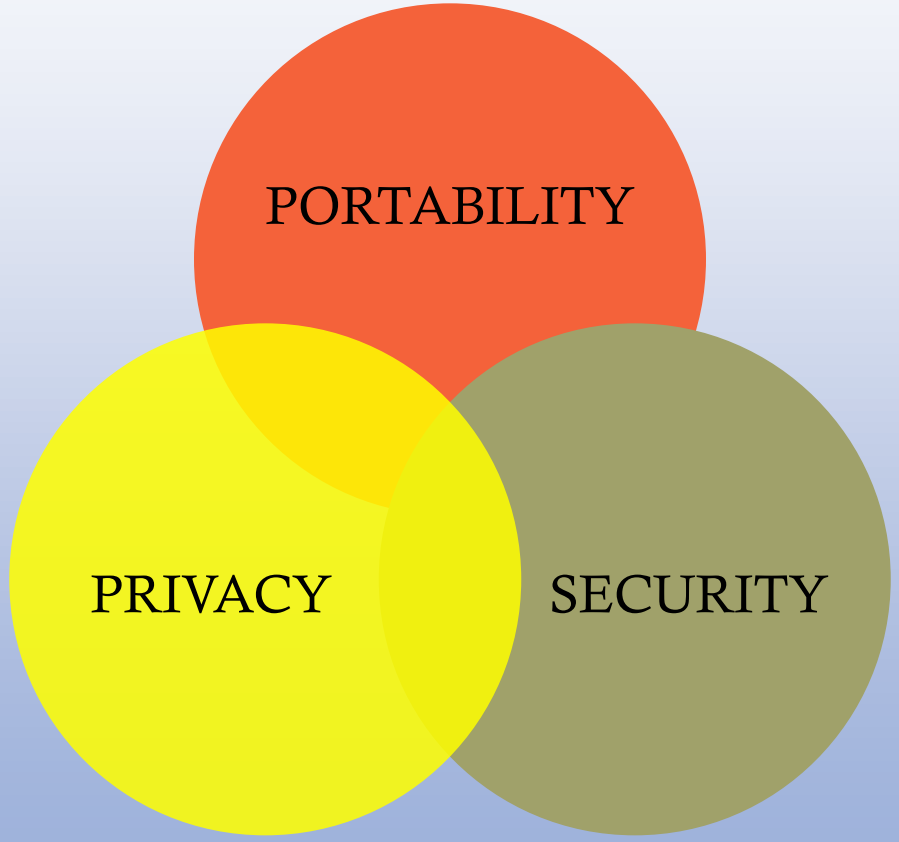
# CIVIL & CRIMINAL PENALTIES

| VIOLATION | MINIMUM | MAXIMUM |
|---|---|---|
| INDIVIDUAL DID NOT REASONABLY KNOW THAT HE/SHE VIOLATED HIPAA | $100 PER VIOLATION UP TO $25,000 ANNUALLY | $50,000 PER VIOLATION WITH AN ANNUAL MAXIMUM OF $1.5 MILLION |
| HIPAA VIOLATION DUE TO REASONABLE CAUSE – NOT WILFUL NEGLECT | $1,000 PER VIOLATION UP TO $100,000 PER VIOLATION | SAME AS ABOVE |
| HIPAA VIOLATION DUE TO WILFUL NEGLECT AND NOT CORRECTED* | $50,000 PER VIOLATION UP TO $1.5 MILLION ANNUALLY | SAME AS ABOVE |
| *CRIMINAL PENALTY | | + 1 YEAR IMPRISONMENT |

# OVERVIEW



# HIPAA – 3 SPHERES OF LAW



# PRIVACY

**APPLIES TO COVERED ENTITIES:**

- **HEALTH PLANS**
- **HEALTH CARE CLEARINGHOUSES**
- **HEALTH CARE PROVIDERS**

# PRIVACY

**APPLIES TO BUSINESS ASSOCIATES:**

- **EMPLOYER WITH GROUP HEALTH PLAN (PLAN SPONSOR)**
- **CONSULTANTS**
- **VENDORS**

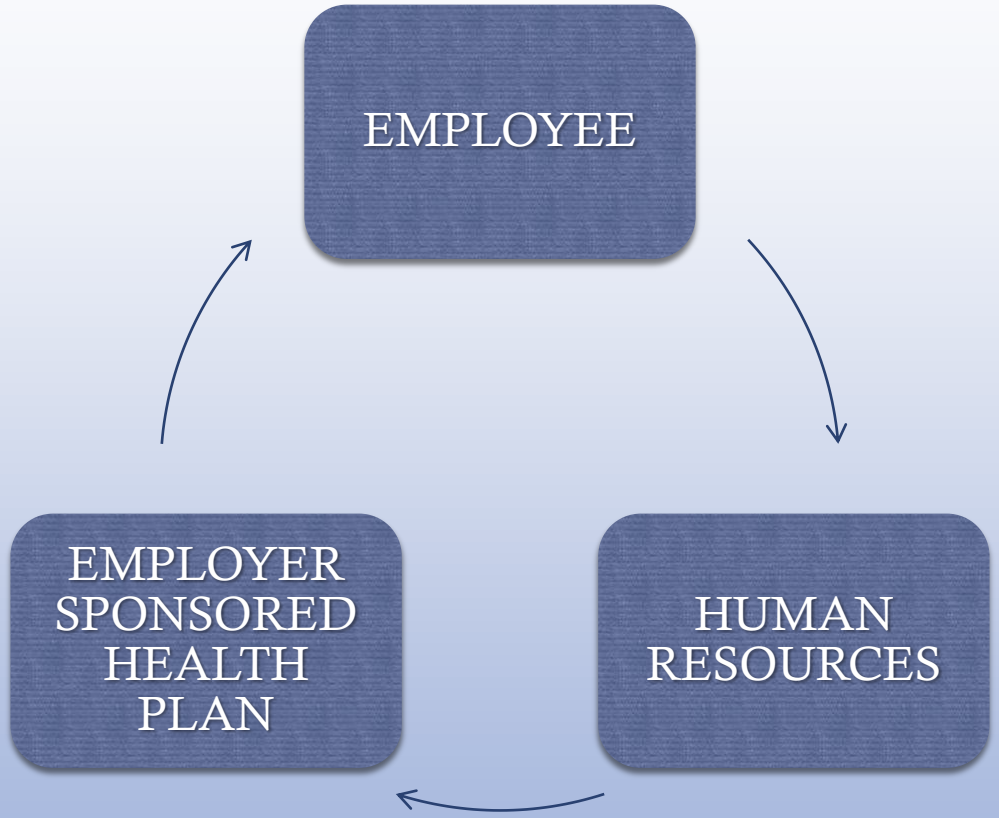
# EXAMPLES

- **ENROLLMENT**
- **BENEFIT QUESTIONS**
- **CLAIMS QUESTIONS**

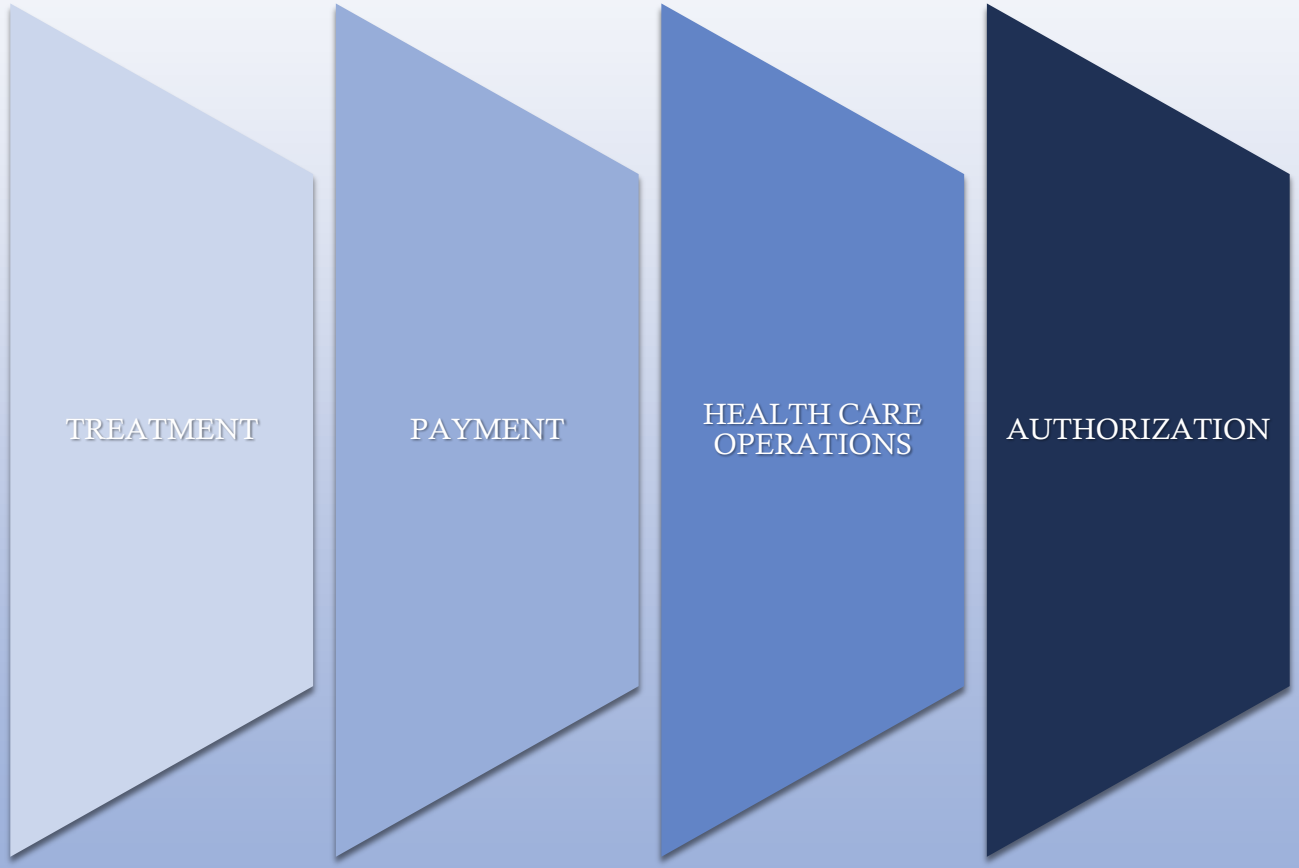
# PRIVACY BASICS

**PROTECT USE & DISCLOSURE OF PROTECTED HEALTH INFORMATION OF AN INDIVIDUAL**

# ROLE OF HUMAN RESOURCES



# WHEN MAY I DISCLOSE PHI?



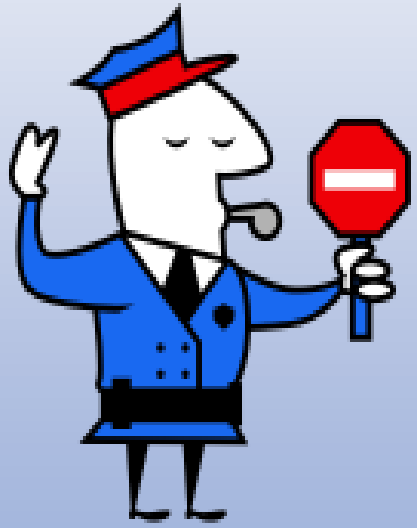
# HOW MAY I DISCLOSE PHI?

- **IN A REASONABLE MANNER**

- **FOR THE MINIMUM PHI NECESSARY FOR PURPOSE**

# WHEN MAY I DISCLOSE PHI?

- **INDIVIDUAL HOLDER**
- **HEALTH PLAN**
- **BUSINESS ASSOCIATE**
- **OTHER INDIVIDUAL**



# SECURITY

- APPLIES TO ELECTRONIC PROTECTED HEALTH INFORMATION
- SAFEGUARDS TO:
  - ADMINISTRATIVE/OPERATIONS: IDENTIFY/ANALYZE POTENTIAL RISKS TO ELECTRONIC PHI AND IMPLEMENT SECURITY MEASURES
  - PHYSICAL: LIMIT ACCESS TO FACILITIES WHERE ELECTRONIC PHI IS HOUSED
  - TECHNICAL: IMPLEMENT AUDIT, INTEGRITY AND TRANSMISSION CONTROLS TO INFORMATION SYSTEMS WITH PHI

# WAIT…THERE'S MORE!

# FINAL RULES

- **RELEASED JANUARY 17, 2013**

- **"The *most sweeping changes* to HIPAA Privacy and Security Rules since they were first implemented"**

- **"These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to *vigorously enforce* the HIPAA Privacy and Security protections …"**

**Leon Rodriguez**
**Director**
**HHS Office for Civil Rights**

# FINAL RULES

- **EXPAND HIPAA PRIVACY AND SECURITY RULES TO BUSINESS ASSOCIATES**
- **PENALTIES ASSESSED TO NEGLIGENCE MAXIMUMS ($1.5 MILLION)**
- **CERTAIN BREACHES OF UNSECURED PHI MUST BE REPORTED TO HHS**
- **PATIENT RIGHTS TO PHI EXPANDED**
- **PATIENT RIGHT TO PROHIBIT ACCESS OF PHI TO HEALTH PLAN**
- **PROHIBITS SALE OF AN INDIVIDUALS' HEALTH INFORMATION W/O PERMISSION**

# FINAL RULES

**•MOST SIGNIFICANT CHANGE IS TO THE DETERMINATION OF A REPORTABLE BREACH TO OFFICE OF CIVIL RIGHTS AND AFFECTED PARTY(IES)**

**•PREVIOUSLY REQUIRED TO REPORT IMPERMISSABLE USE IF COVERED ENTITY DETERMINED THAT THE USE POSED A SIGNIFICANT, FINANCIAL, REPUTATIONAL HARM TO AFFECTED INDIVIDUALS**

**•FINAL RULE: COVERED ENTITY/BUSINESS ASSOCIATE MUST REPORT BREACH TO OCR AND AFFECTED PARTY(IES) UNLESS [THEY] CAN DEMONSTRATE A LOW PROBABILITY THAT PHI HAS BEEN COMPROMISED**

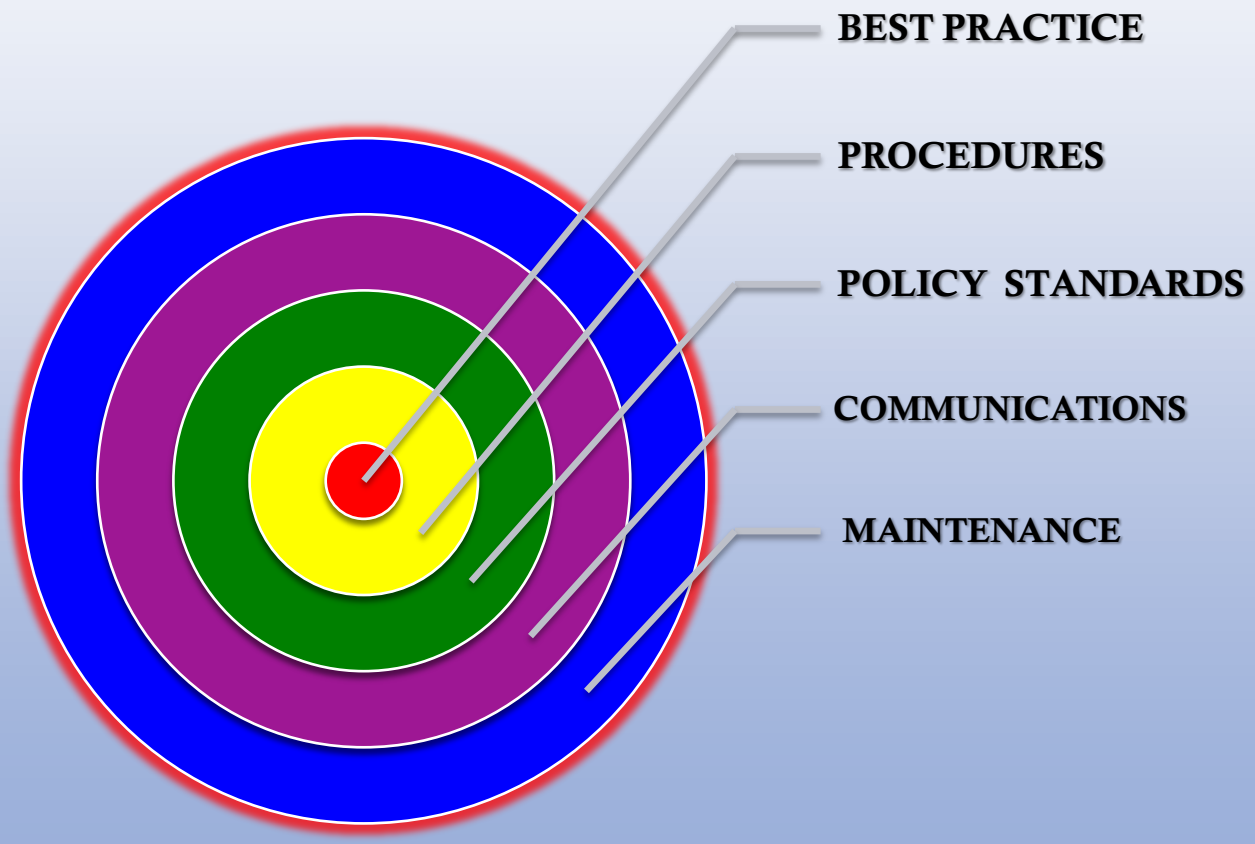
**•PRESUMPTION THAT ALL IMPERMISSABLE USE OF PHI IS A BREACH**

# RELATED PRIVACY RULES

- **SECURITY OF PERSONAL INFORMATION**
- **SOCIAL SECURITY CONFIDENTIALITY**
- **SOCIAL SECURITY TRUNCATION ON PAY STUBS**
- **MEDICAL INFORMATION CONFIDENTIALITY ACT**

# ORGANIZING BEST PRACTICES

# TARGETING GOOD FAITH BUSINESS PRACTICE



# BEST PRACTICES

## BEST METHOD TO SAFEGUARD PHI IS NOT TO CREATE PHI

- DO YOU NEED THE SSN ON THAT REPORT? IF NOT, THEN HAVE PROGRAMMING REMOVE IT

- IF YOU RECEIVE A REPORT WITH SSN LISTED, REMOVE THE COLUMN IF NOT NEEDED

# BEST PRACTICES

## DATA TRANSMITTAL

- PHI CANNOT BE TRANSMITTED UNSECURED

- E-MAIL IS NOT A SECURED METHOD

# BEST PRACTICES

**RECORD STORAGE:**

***CURRENT AND SHORT TERM***

**RECORD STORAGE:**

***LONG TERM***

# BEST PRACTICES

## HEALTH PLAN BILLING

- SAFEGUARD IF SSN INCLUDED
- PROCESSING BY OTHER DEPARTMENTS

# BEST PRACTICES

## ENROLLMENT CARDS/FORMS

- WHO IS RESPONSIBLE FOR COLLECTING?
- DATA ENTRY?
- WHERE ARE THEY FILED?
- WHERE ARE THEY STORED LONG-TERM?

# BEST PRACTICES

## DOUBLE LOCK RULE

- HAVE TWO LOCKS BETWEEN OUTSIDE & PHI
- SECURITY (BURGLAR) ALARM COUNTS AS ONE
- INEXPENSIVE LOCKED CABINET VS. COMPLAINT

# BEST PRACTICES

**JANITORIAL SERVICES**

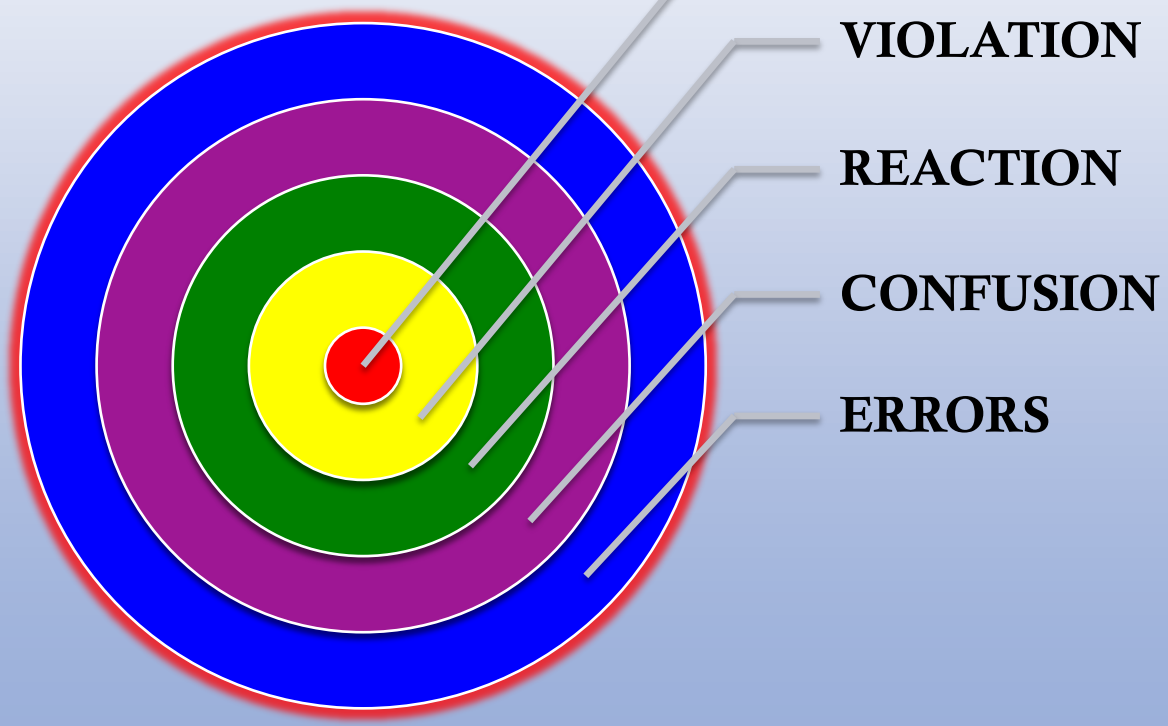
- **PROCEDURE FOR ACCESS/TIMING**
- **BUSINESS ASSOCIATE AGREEMENT**

# BEST PRACTICES

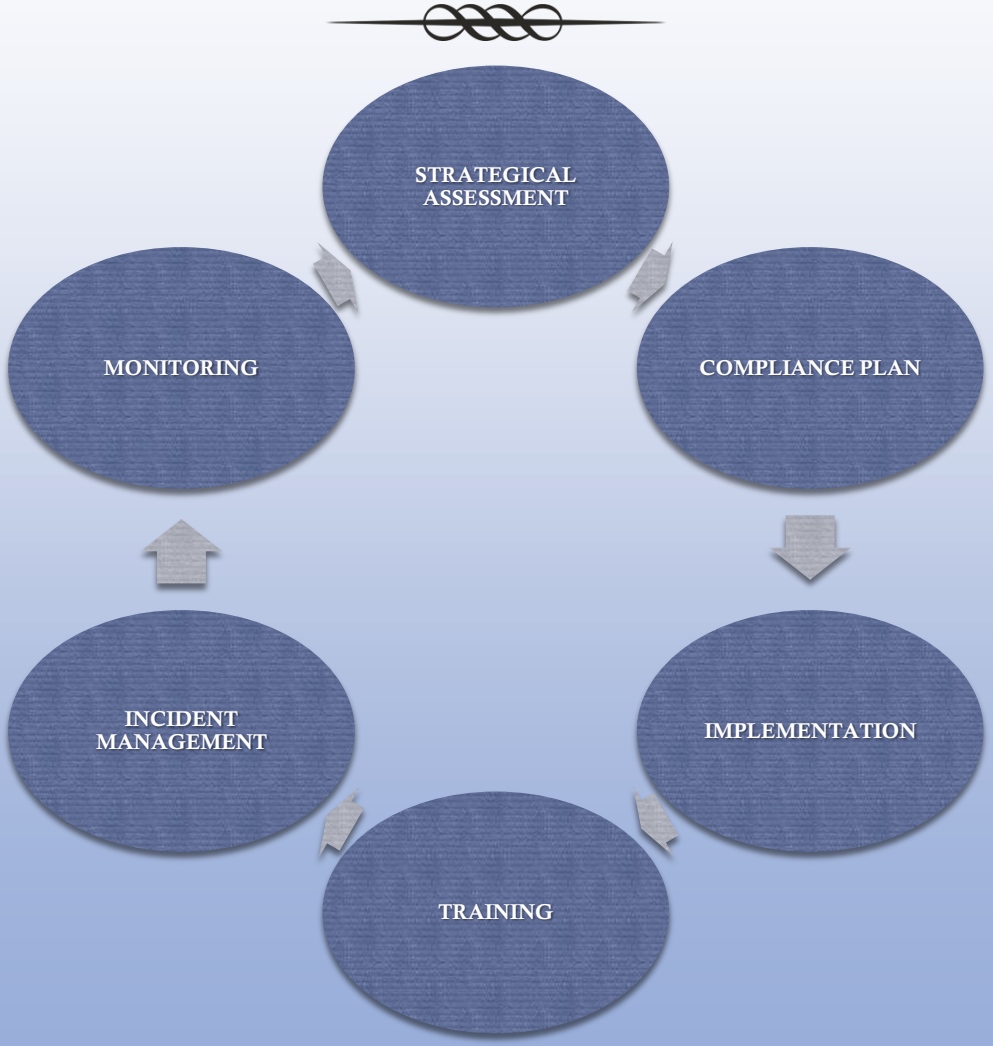
**INTERNET**

- **FIREWALLS**
- **ANTI-VIRUS SOFTWARE**
- **AUTO TIMING ON SCREEN SAVERS**
- **ENCRYPTION**

# MISSING THE MARK



# CONTINUING THE BEST PRACTICE PROCESS



# OUR ROLE PROVIDES TRUST

- ***TRANSPARENCY*** **– OPENESS AND CLARITY TO ALL ACTIVITIES CONCERNING THE CAPTURE, COLLECTION, DISSEMINATION AND USE OF PROTECTED HEALTH INFORMATION**

- ***STEWARDSHIP*** **– WE ASSUME A RESPONSIBITY OVER THE HANDLING AND PROTECTION OF EMPLOYEE INFORMATION *REGARDLESS OF* THE SOURCE OR TYPE OF INFORMATION**

# “MOST PEOPLE DON’T DO WHAT’S RIGHT…THEY DO WHAT’S CONVENIENT AND THEN REPENT.” *Bob Dylan*

EADSON COMPLIANCE CENTER
mary@eadsoncompliance.com
www.eadsoncompliance.com
760/468-4082

NIKSSARIAN INSURANCE SERVICES, INC.
davidn@nikins.com
www.nikins.com
831/233-6700

# THANKS FOR ATTENDING