# Evolution of Privacy & Security at Henry Ford Health System

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

# THE HFHS ECOSYSTEM

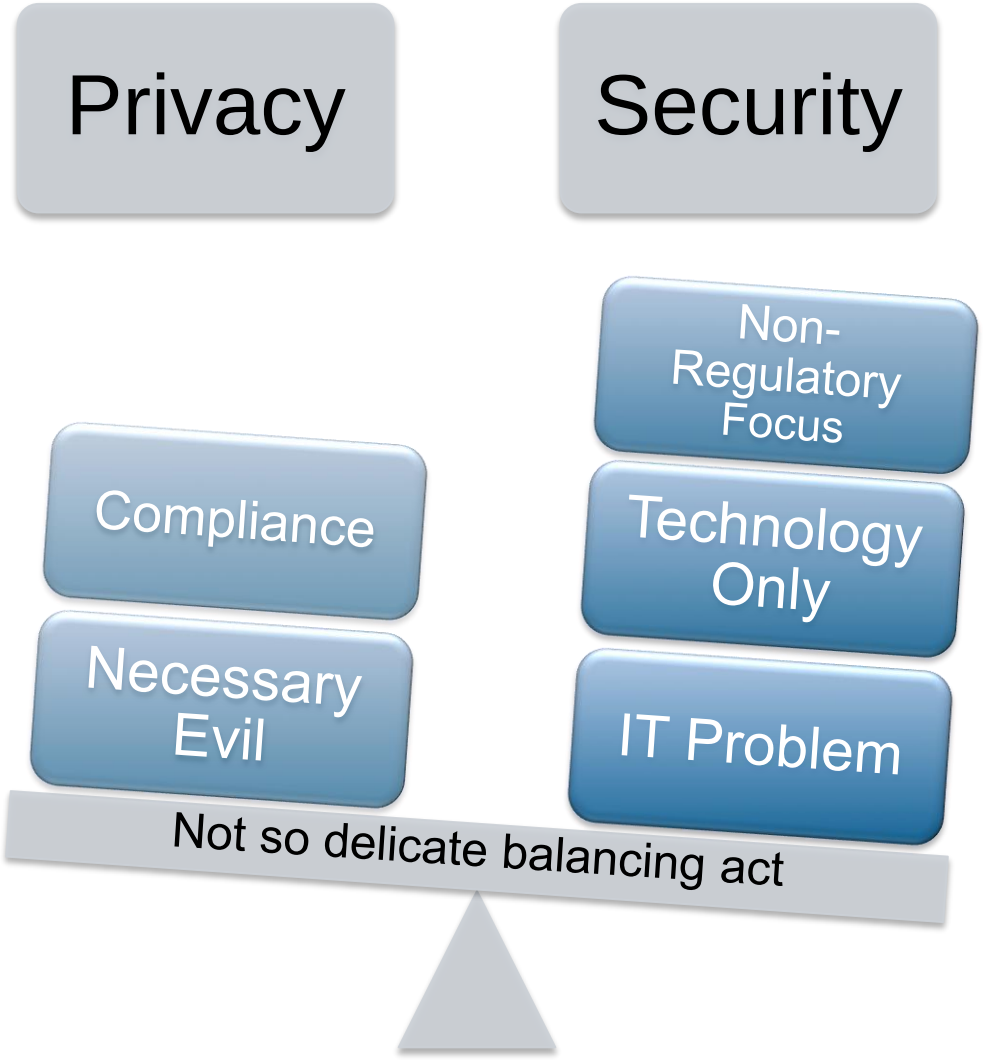
- $6 Billion in Revenues
- $200 Million in uncompensated care
- 6 Acute Care Facilities (Approx. 2500+ beds)
- 60+ Physician Practices
- Substance Abuse & Behavioral Health Facility
- Research Program
- Specialty Centers & Institutes
- Approx. 31,000 workforce members (FTEs, Contract, Researchers, etc.)
- 1300+ Member Medical Group
- 1000+ Member Physician Network (Non-Employed & Private Practice)
- 30+ Primary Care Centers
- Health Plan serving approximately 640,000 members
- Home Health & Hospice Division
- Retail Pharmacy Division
- Optical Care Division
- Occupational Health
- Long Term Care Facility & Extended Care Division

# DEFINING CHARACTERISTICS

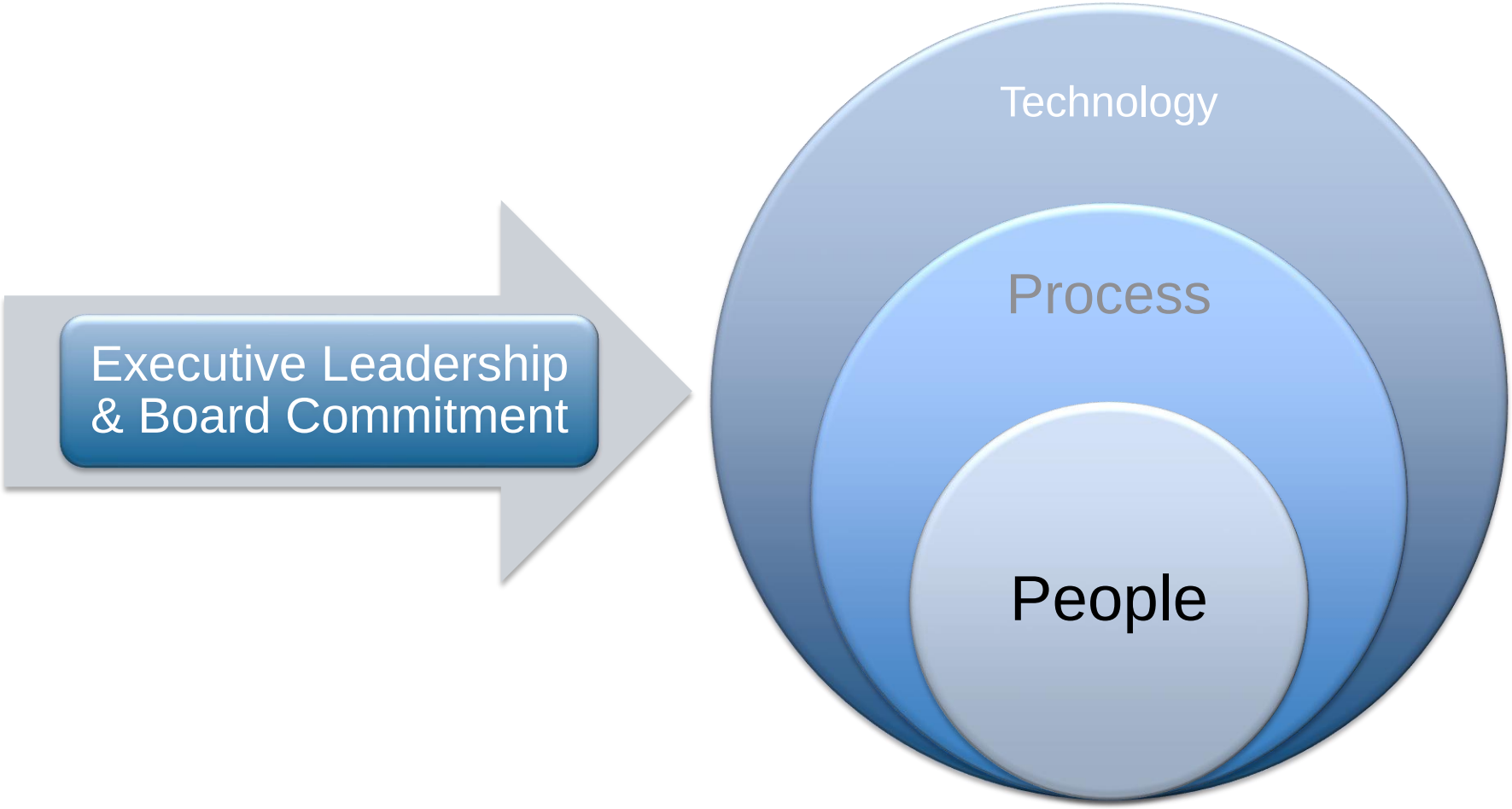
**Our PEOPLE!**

The culture we have created with our **workforce** has resulted in a unique energy and a "**can-do spirit**" that is the foundation of Henry Ford Health System. We have a passion around engaging our **people** and operate on the belief that an engaged **workforce** creates in better, safer patient.

# INDUSTRY PERSPECTIVE



# OUR CULTURE OF CONFIDENTIALITY

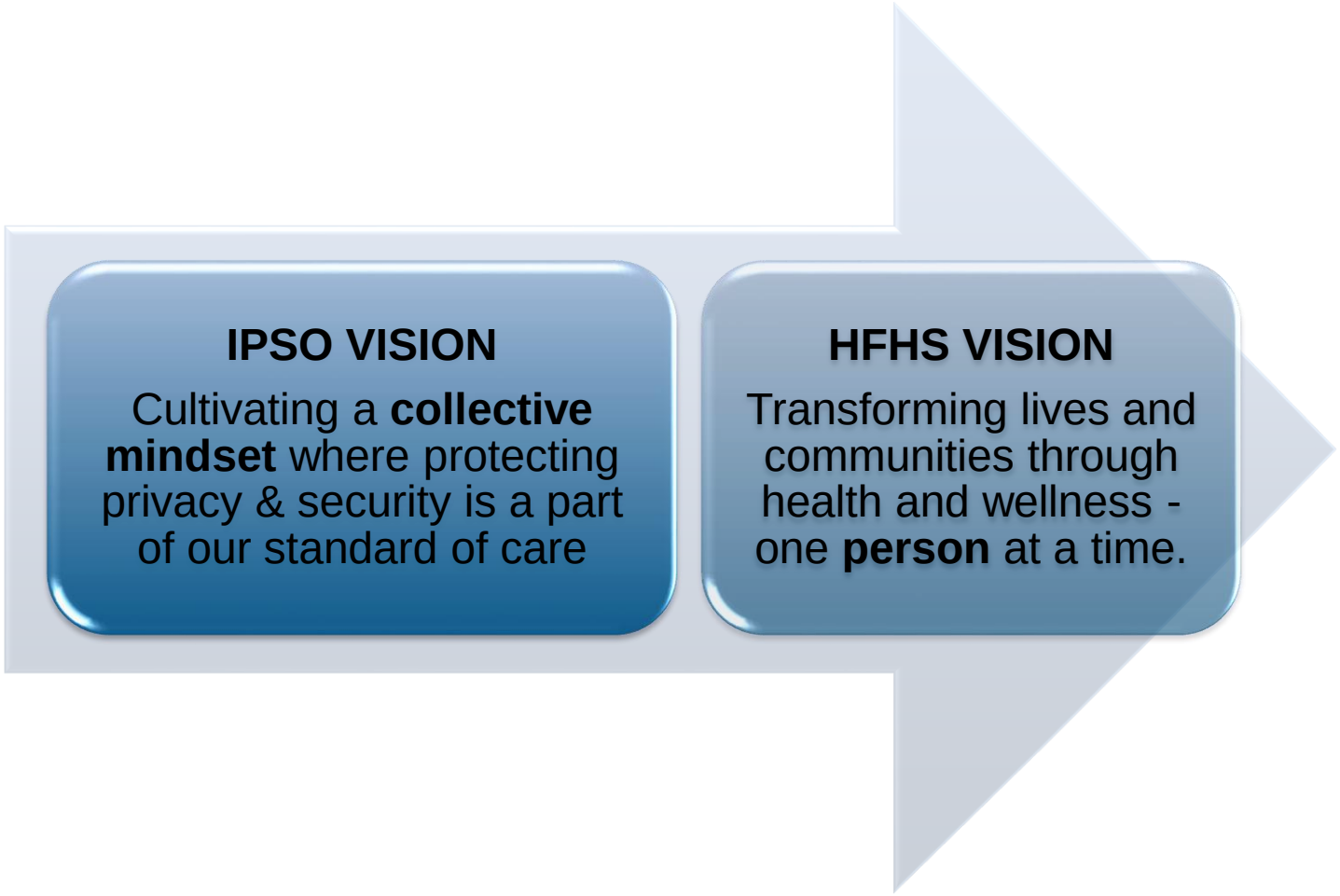


# IPSO MISSION

**IPSO MISSION**
To establish a system-wide **culture of confidentiality** through education, accessibility, and a **customer focus** where privacy & security is viewed as paramount in our daily operations.

**HFHS MISSION**
To improve **people's** lives through excellence in the science and art of health care and healing.

# IPSO VISION


IPSO VISION
Cultivating a **collective mindset** where protecting privacy & security is a part of our standard of care
HFHS VISION
Transforming lives and communities through health and wellness - one **person** at a time.

# IPSO GOVERNANCE STRUCTURE

# CENTRALIZED INVESTIGATIVE PROCESS

Any routine investigations and incidents that may result in a breach must be forwarded to the IPSO for a Code A(ssessment) and potential Code B(reach) Alert

Investigations are led by the IPSO in conjunction with operational management and Human Resources

All investigative documentation (i.e., notes, interview transcripts, audit logs, etc.) should be stored in our centralized repository to ensure the ability for metric reporting and auditing

Corrective Action always recommended by the IPSO in accordance with the outcome of the investigation

Re-education **required** for the entire department within 30 days of investigation closure not just the offender

# IPSO COUNCILS & RESPONSE TEAMS

## Enterprise Privacy & Security Council

- The oversight council that approves System policies and procedures related to privacy & security regulations

## Code B Alert Team

- The rapid-response workgroup established to centrally respond and manage all System data breaches

## Office for Civil Rights Response Team

- Reviews all OCR data requests related to privacy & security violations and respond on behalf of the System and/or specific business unit

# BUSINESS ASSOCIATE MANAGEMENT PROGRAM

## Inventory

- Conducted enterprise wide inventory of all business associates
  - Current total approx. 1450+

## Risk Rank

- Risk ranked each business associate
  - Type of Data
  - Services Performed
  - Disclosures
  - Network Connections

## Manage

- Implemented management plan to ensure contract & BA compliance
  - BA Education
  - Signature Authority
  - Terminations

# BRANDED PROGRAMS, INITIATIVES & COMMUNICATION PLANS

## CODE B(REACH) ALERT PROGRAM

Issued & managed by the IPSO for all media reportable data breaches or data breaches with significant risk

Branded communication plan consistently utilized throughout the system and managed corporately instead of at the business unit level

*External:* Includes the notification to the prominent media outlets and OCR

*Internal:* Typically includes a copy of the communication to the patients, FAQs about the breach and instructions for forwarding patient inquiries to toll-free call center

Requires immediate attention by all System leadership and should be shared with staff for a 90 day period

### Code A(ssessment) Alert

Alerts issued by the IPSO led by the CIPSO

Limited to the IPSO, PR, Legal Affairs, Risk Finance & Insurance

Provides a summary and initial analysis of potential data breach

Includes initial data analysis culminating in an official breach risk assessment to determine if an actual breach has occurred

# COMMUNICATION, EDUCATION & REPETITION

**Our Workforce**

- Morning Post Messages & System Emails – Scheduled to deliver key privacy & security messages
- Annual Mandatory Education – iComply & Job Specific
- Privacy & Security refresher trainings conducted by the IPSO team
- Manager's Update – Monthly email to all leaders detailing key messages

**Our Board Members**

- Quarterly privacy & security Board updates
- Updates to the Trustee newsletter

**Our Patients & Communities**

- "privateTALK" or "secureSPEAK" with the CIPSO – Scheduled chat sessions where questions can be addressed in an online forum
- Intranet Webpage, Internet Webpage & Social Media Sites

# THE iCOMPLY PROGRAM

Branded System wide program coordinated by the IPSO to safeguard “system” information


# THE iCOMPLY PROGRAM

- **Phase I:** Targeted portable storage devices
  - **Required** employees to visit one of 20 “IT staffed” stations to turn in all personal flash drives for our approved IronKey solution; register any portable hard drives or personal laptops for follow-up by IT
  - Employees could enter a drawing for an iPad 2 by completing a crossword puzzle based on our privacy & security policies
  - Removed 5000 flash drives in 4 weeks
- **Phase II:** Targeted “culture” through educational modules
- **Phase III:** Focused on reducing our “unsecured” printer footprint
- **Phase IV:** Targeted the culture again to reinforce HITECH/Omnibus

# THE iCOMPLY PROGRAM

- **Phase V:** BYOD & Mobile Device Management
- **Phase VI:** Vendor Management Risk Management Program
- **Phase VII:** Cybersecurity Program Maturity Assessment
- **Phase VIII:** Why iComply Video Series
- **Phase VII:** Threat Intelligence Sharing Initiative

# SUPPORTIVE TECHNOLOGY STRATEGIES

- Investments into a state of the art electronic health record
- Invested in a Governance, Risk & Compliance application to centralize the management of enterprise risk including privacy & security
- Strategies developed around virtualization, cloud computing & storage
- Invested in Mobile Device Management software to secure devices
- Developing strategies around medical device security
- Developing strategies around secure texting (i.e., iComply Phase X)

# HOW DID OUR CULTURE RESPOND?

- Incident reporting increases approximately 30% every year
- Employees "**Think Privacy & Security First"**…when in doubt, they call the IPSO team…we are partners & not "necessary evils"!
- Patients frequently access our webpage or their MyChart account to submit questions about the privacy & security of their PHI
- Department leadership frequently requests refresher training for their teams in the absence of an incident
- See technology as the **enabler** of our "culture of confidentiality" and not the **enforcer**

# ARE WE PERFECT?

# MY RESPONSE…Iterally!

- WHAT?  WTHeck!!!!!
- HAVEN'T WE BEEN HERE BEFORE?
- YOU GOT TO BE KIDDIN' ME!

On a serious note, this proved that **education**…**education**…**education** has to be a part of your program and defense strategy.

No amount of technology would solve good people who do the absolute wrong thing!

# INCREASED WORKFORCE EDUCATION & TRAINING

**Increased** Morning Post Messages & System Emails – Scheduled to deliver key privacy & security messages weekly

**Created** physician specific education to support our provider workforce team members

Continued Privacy & Security refresher training schedule conducted by the IPSO team

**Created** a iComply Corner in every Manager's Update – Monthly email to all leaders detailing key messages

**Created** "Why iComply" video series featuring hospital CEOs and Executive leadership explaining why "they comply".

# QUESTIONS

**Meredith R. Phillips, CHC, CHPC, HCISPP, ITL**
Chief Information Privacy & Security Officer

Henry Ford Health System
One Ford Place, Suite 2A10
Detroit, MI 48202

313-874-5168
mphilli2@hfhs.org