The Next Revolution in Nursing Informatics

Kathleen A. McCormick, Ph.D, RN, FAAN, FACMI, FHIMSS
Sigma Theta Tau International
November 17, 2013

Objectives

- To describe the forces shaping Healthcare and Nursing Informatics Today
- To define the 6 phases in technology that impact Nursing Informatics

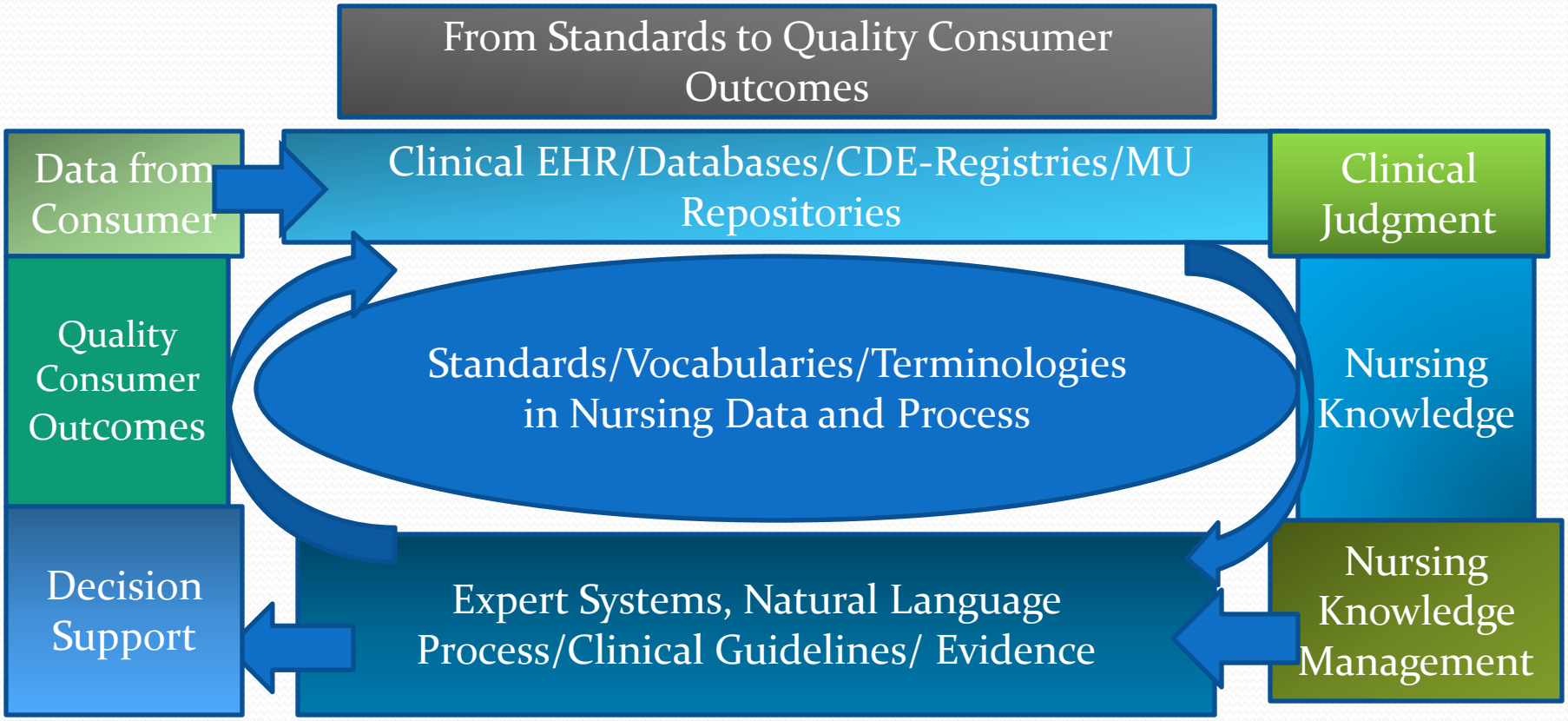
Forces Shaping Healthcare and Nursing Informatics

- Big Data – Genomics, Insurance, Pharmaceutical data
- Personalized Healthcare – treatments matched to your healthcare condition and genetic profile
- Quality and outcomes of care throughout the patient continuum
- Consumer involvement in healthcare and informatics

Common to all the forces in Healthcare

- Shared Data
- Data Standards
- Continuum of Care
- Meaningful Use
- Quality and Safety

Relationship Between Standard Terminology and Quality



The Six Phases of Technology that Impact Nursing Informatics

- The Mainframe
- The Minicomputer
- The Personal Computers
- The World Wide Web (WWW)
- Mobile Networks

Where is the Money Going to be in Nursing Informatics in the Next Decade?

$$$$$$The MONEY$$$$$$

Technavio

- Predicted market to swell **to $9.3 Billion** by 2014

Challenge -7 TYPES OF mHealth Patil, 2011

1. Improving management and decision-making by health-care professionals
2. Real-time and location-based data gathering, e.g. surveillance
3. Provision of health care to remove and difficult to serve locations
4. Fostering Learning & Knowledge exchange among health professionals
5. Promoting Public Health
6. Improving Accountability
7. Self-management of patient care

The PROMISE

- CompTIA – 81% of MDs use Smartphones
- Manhattan Research – 62% of MDs use Tablets
- Spyglass Consulting group - 69% of hospital NURSES said they use their smartphones for personal and clinical communications while on the job,
- Frost and Sullivan – Smartphones are more ubiquitous to manage Chronic Conditions
- Accountable Care Act – Mobile devices can reduce hospital readmissions

Challenge -The Data about Cell Phones Pew Internet

- 85% of adults have a cell phone
- 31% used cell phone for health information
- 17% use cell phone for health advice
- 80% of cell phone users use text messages
- 9% use cell phone text for health alerts

The Data about Smartphones

Pew Internet

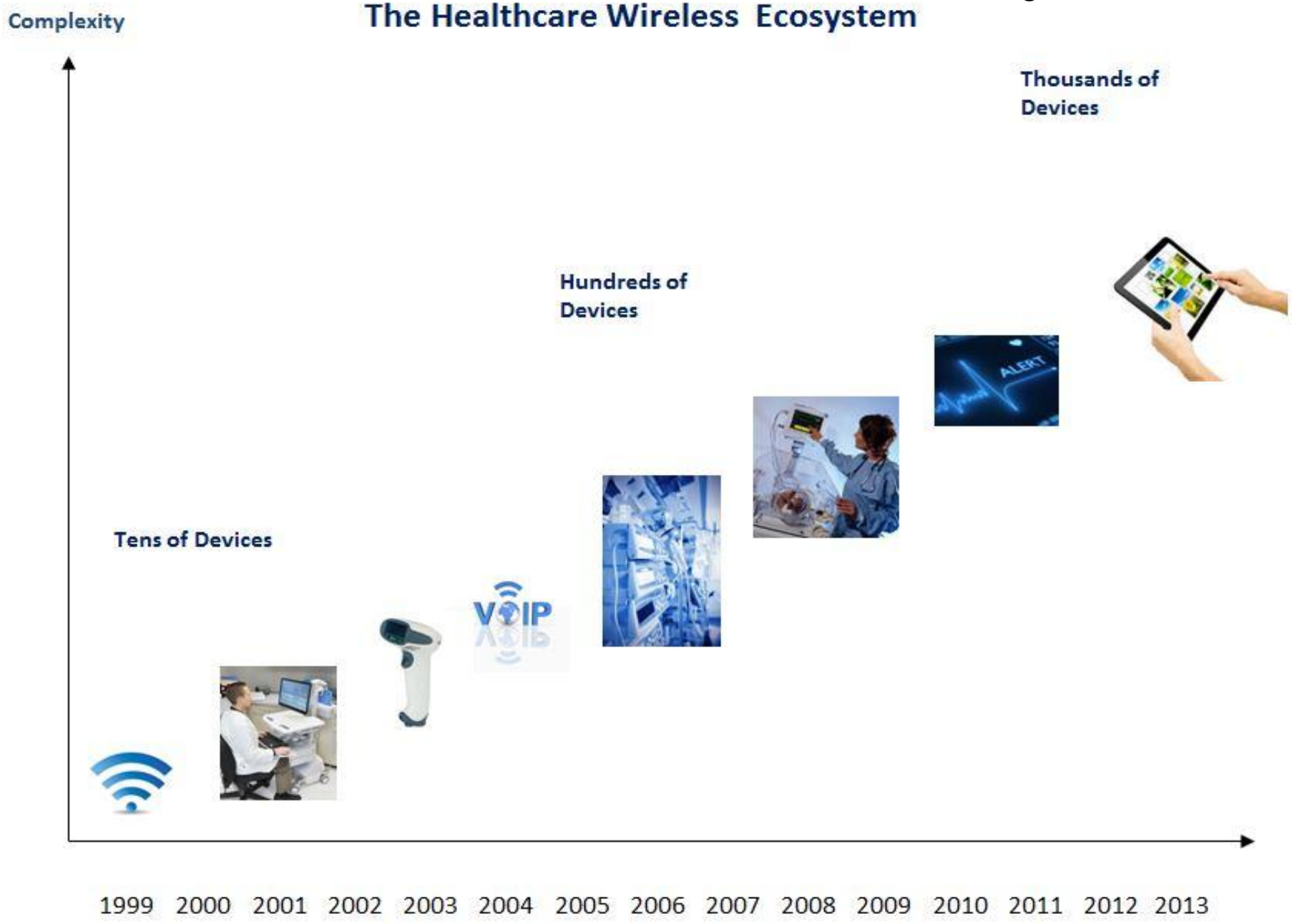
- 53% of adults have a SMARTPHONE
- 52% of smartphone users seek health information especially after a health crisis
- Women 30-64 use smartphones for health text alerts
- 19% of smartphone users use it for 1 health application – exercise, diet, weight control
- African Americans, Latinos who use smartphones are 18-49 years and have a college degree

The VOLUME Technavio

- There will be an estimated 13, 000 health applications aimed at consumers by Summer 2013
- Growth rate is predicted to be 24% between 2010 and 2014
- Apple shipped more IPADS in 2 years than MACS in 20 years (David Hoglund, 2012)

DHoglund, 2013

The Healthcare Wireless Ecosystem



$$$$$$Costs of Mobile Health Vulnerabilities$$$$ S. Murphy in McCormick,Gugerty HIT 2013

- Average large companies have lost $429,000 due to mobile computing mishaps and
- 50% of companies have experienced a data breach due to insecure devices

Clinician Use of Smartphones

Liz Johnson and others, in McCormick and Gugerty HIT 2013

- Document patient visits
- Manage clinical workflows
- Conduct research on technical and clinical issues
- Receive alerts on patient's conditions
- Interactive grand rounds – access to x-rays, medication profiles, laboratory data-evidence (DLiebovitz in HIT 2013)
- Ordering prescriptions in CPOE (SMurphy in HIT 2013)
- 71% of healthcare environments are thinking about developing their own custom mobile applications – DHoglund 2012

Challenge - Most Popular Health Apps –Apple 2011

- Cardio – 16.36%
- Other – 15.36%
- Diet – 14.15%
- Stress/Relaxation – 11.44%
- Women's Health – 7.27%
- Strength Training – 6.97%
- Calculator- 6.03%
- Mental Health – 5.8%
- Chronic Conditions – 5.45%
- Sleep – 4.13%
- Emergency – 2.73%
- Smoking Cessation – 2.23%
- Medication Adherence – 1.36%
- Personal Health Record – PHR – 0.71%

Dhoglund 2013

New ONC Challenge Grant show PHR Promise- Dr. Mirro-EMR Daily News 4/11/2013

- Parkview Cardiology Physicians Group - EHR
- Indiana HIE
- PHR – NoMoreClipboard (NMC)
- 184 patients post revascularization + diabetes
- Transmit blood pressure, heart rate, blood glucose, height, weight and BMI to doctors
- RESULT – average 8.7 interactions in 6 months
- Significant declines in HbA1c and improved patient activation scores

Challenge - Background

- By 2013 **mobile phones** will be the predominant access via:
  - Google Android
  - Apple IOS
  - Windows 8
  - **Vendors** Predominating in HIT:

Allscripts

Epocrates

GE Healthcare

Voxiva, Inc.

Barriers – Ponemon Institute 2011

http://www.amednews.com/article/20111219/business/312199967/2/

- 72 % of organizations do NOT protect their data
- 79% do NOT use password locks with devices (75% have disabled it for smartphones-DHoglund)
- 77% do NOT use encryption to protect data
- 74% allow BYOD usage
- 54% do NOT have policies governing proper use of mobile devices
- Healthcare Breaches have risen 32% - Sibelius Comments (due to unencrypted or lost or stolen mobiles devices mHIMSS meeting)

Biggest Barriers - High Threats and Vulnerabilities

NIST 2012 Guidelines for Managing and Securing Mobile Devices in the Enterprise

- Confidentiality – transmitted ad stored data cannot be read by an unauthorized party
- Integrity – detect unintentional changes to transmitted and stored data
- Availability – ensure that users can access resources whenever needed

Barriers – Threats and Vulnerabilities NIST 2012

- Lack of Physical Security Controls – I LOST IT
- Use of Untrusted Mobile Devices – How did I know get this application
- Use of Untrusted Networks- How did I get on this
- Use of Applications Created by Unknown Parties
- Interaction with other Systems
- Use of Untrusted Content
- Use of Location Services

Barriers - 6 Mobile Architectures

- Challenges
- 1. NATIVE
- 2. SPECIAL
- 3. HYBRID
- 4. HTML5 WITH VIDEO AND AUDIO AND 3 D GRAPHICS
- 5. MESSAGE
- 6. NO CLIENT

- Barriers
- 1. No developed interface standards across devices
- Over 100 tool vendors

Barriers – Threats Posted by Mobile Apps

- PRIVACY – 54% have uninstalled or not installed apps because of concerns about personal information
- Data Management – 41% backup photos, contacts
  - 32% clear browsing history
  - 19% turned off location tracking
  - 33% have lost or had a phone stolen
  - 12% had unwanted access to their content
  - 45% between 18-24 years had phones stolen

Barriers – mHIMSS Survey February 2012

- Inadequate Privacy and Security – 60%
- Lack of funding – 48%
- Bringing in self-owned devices to work versus supplied by the enterprise

Barrier – Distraction to Health Professionals –Gill et al 2012-From ECRI

- 55% of technicians who monitor heart bypass machines during surgery talked on their cellphones during surgery - Forbes, 2012

Barrier

- It has not been determined how to relay side-effects of new medications on cell phones or smartphones to clinicians and consumers

Barrier

- According to the CEO of Pinch Media, **only 5%** of apps are used after initial download **just 30 days**


FAILURE
SUCCESS

Security Solutions for Mobile Devices NIST Supplements SP 800-53

- Centrally manage and secure mobile devices
  - Organizationally Provided –
    - Develop Threat Models to define which services are needed, then design and acquire one or more solutions that provide these services.
    - Restrictions on Mobile Devices and Access Levels
    - Develop system threat models for mobile devices
    - Define the resources that are accessed through mobile devices
  - Personally-Owned
    - Use a messaging server management capability of the company that sold you the phone – BUT have telephone number can get into personal apps
    - Use a product from a third party which is designed to manage one or more brands of phone – e.g. gmail

What goes into a THREAT MODEL- NIST 2012

- Physical security controls from being lost and stolen
- Only reason someone wants to steal the device is to get access to your organizations resources

---

Mitigation:

- Encrypt sensitive data, or don't store it on mobile devices and create 2 layers of authentication

Threat Model

- Assume all phones are untrusted unless user access it monitored and controlled and continuously monitored with enterprise applications data

---

Mitigation:

- Do not allow BYOD (Bring our own device)
- Run devices on secure, isolated sandboxes using device integrity scanning applications

Threat Model

- External networks can be assumed to be untrusted networked allowing eavesdropping

---

Mitigation:

- Use strong encryption technologies to protect the confidentiality and integrity of communications and use dual manual authentication mechanisms

Threat Model

- Use of applications created by unknown parties should be untrusted
- _____

  Mitigation:
- Prohibit installing 3rd party applications
- Implement a secure sandbox that isolates the organization for the users
- Implement whitelisting approved applications
- Blacklist unapproved applications

Threat Model

- Interaction with other systems for data synchronization and storage – do not attach an organizationally owned mobile to a personal laptop and visa versa

---

Mitigation:

- Define policies to prevent this and education the users
- Disallow the use of remote backup services from BYOD

Threat Model

- Use of untrusted content – malicious QE codes translated to URLs from device cameras
- _____

  Mitigation:
- Educate users about the inherent risks of untrusted content
- Restrict peripheral use on mobile devices
- Disable cameras at work to prevent QR codes

Threat Model

- GPS services make mobile devices at increased risk of targeted attached

---

Mitigation:

- Disable the location service – GPS
- OPT out of location services whenever possible

Categories of Security Policies Needed – NIST 2012

- General Policy – enforcing enterprise security policies such as restricting access to hardware and software, managing wireless network interfaces, and automatically monitoring and reporting when policy violations occur, how provisioning should be handled. How device management servers are administered and how policies in those servers are updated. The policy should be documented in a system security plan. The mobile device security policy should be consistent with the non-mobile systems
- Data communication and storage- support strongly encrypted data communications and data storage, remotely wiping the device if it is lost or stolen and if there are risks of untrusted third parties

Categories of Security Policy Continued – NIST 2012

- User and device authentication – requires dual authentication: 1) into the device, and 2) before accessing organization resources, resetting passwords remotely, automatically locking idle devices, and remotely locking devices if left in unsecured locations
- Applications – restricting which applications may be installed, installing and updating applications, restricting the use of synchronization services, digitally signing applications, distributing the organization's applications from a dedicated mobile application store, and limiting or preventing access to the enterprise based on the mobile device's operation system or mobile device management software client version

Test of System Confidentiality, Integrity, and Availability

- Before rolling out – test for :
  - Connectivity
  - Protection
  - Authentication
  - Application functionality
  - Solution management
  - Logging and
  - Performance

Operations and Maintenance NIST 2012

- Upgrade for patches then acquire, test and deploy them
- Ensure clock synched with local time
- Configure access control features
- Detect and document anomalies within the device infrastructure – assess audit logs, perform vulnerability scans and penetration testing
- Reassess policies regularly consistent with upgrades

Solutions – Questions to Ask before Adding an APP?

- What are your goals?
- What need/problem will the app address/solve?
- Will the app provide enough useful information on an on-going basis that will draw the user back to use the app again and again?
- Who is your target audience and are they mobile users?
- What experience are you trying to achieve for the user? Mobile app or mobile website - there is a difference.
- Is it worth the cost? What will your ROI be?
- How will you measure success?
- Which platforms will your app be available through (eg, Apple, Android)?
- Will your app be available for free or will you require a fee?
- Will your app be geared toward marketing (eg, ER wait times, maps and directions, find a physician), internal (eg, physician access to clinical lab reports, physician access to complete medical records), or patient-centered apps (eg, help patients keep track of their medications, find a physician and stay connected with him or her)?

Feeling Overwhelmed

Relevance to Nursing- These are works in Progress

Relevance to Nursing

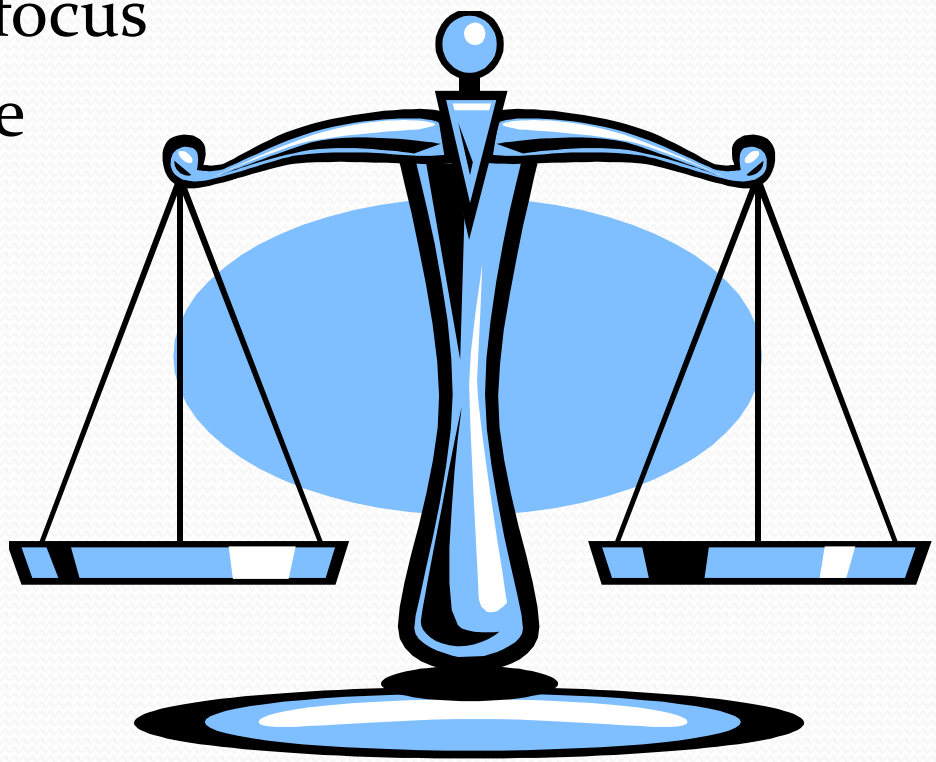
- Participate in both growing activities
- Investigate committees to sit on
- Talk with others in the same boat
- Make your voice heard through publications and participation

Organizational Considerations-

Policies, Training, Communication

Summary and Conclusions

- The mobiles hold promise, challenges, and rewards
- The risks need to be mitigated
- Privacy Security is the focus
- Education is imperative
- Policies are essential



Contact Information

- Thank You
- Contact Information:
- Kathleen A. McCormick, Scimind, LLC
- scimind@verizon.net