EHRs/NHII: HIPAA Security and EHRs, a Near Perfect Match

Margret Amatayakul, RHIA, CHPS, FHIMSS

Steven S. Lazarus, PhD, FHIMSS

Margret A

Margret\A Consulting, LLC

Strategies for the digital future of healthcare information

- **Information management and systems consultant, focusing on electronic health records and their value proposition**
- **Adjunct faculty, College of St. Scholastica; former positions with CPRI, AHIMA, Univ. of Ill., IEEI**
- **Active participant in standards development**
- **Speaker and author (Silver ASHPE Awards for "HIPAA on the Job" column in *Journal of AHIMA*)**

- Strategic IT planning
- Compliance assessments
- Work flow redesign
- Project management and oversight
- ROI/benefits realization
- Training and education
- Vendor selection
- Product/ market analysis

Steve Lazarus

Boundary Information Group

Strategies for workflow, productivity, quality and patient satisfaction improvement through health care information

- **Business process consultant focusing on electronic health records, and electronic transactions between organizations**
- **Former positions with MGMA, University of Denver, Dartmouth College; advisor to national associations**
- **Active leader in the Workgroup for Electronic Data Interchange (WEDI)**
- **Speaker and author (two books on HIPAA Security and one forthcoming on electronic health record)**

- Strategic IT business process planning
- ROI/benefits realization
- Project management and oversight
- Workflow redesign
- Education and training
- Vendor selection and enhanced use of vendor products
- Facilitate collaborations among organizations to share/exchange health care information

Agenda

- EHR
- EHR and NHII
- EHR and Security
- EHR, NHII, and Security
- Clinical practice support
- Connectivity
- Personalized care
- Population health

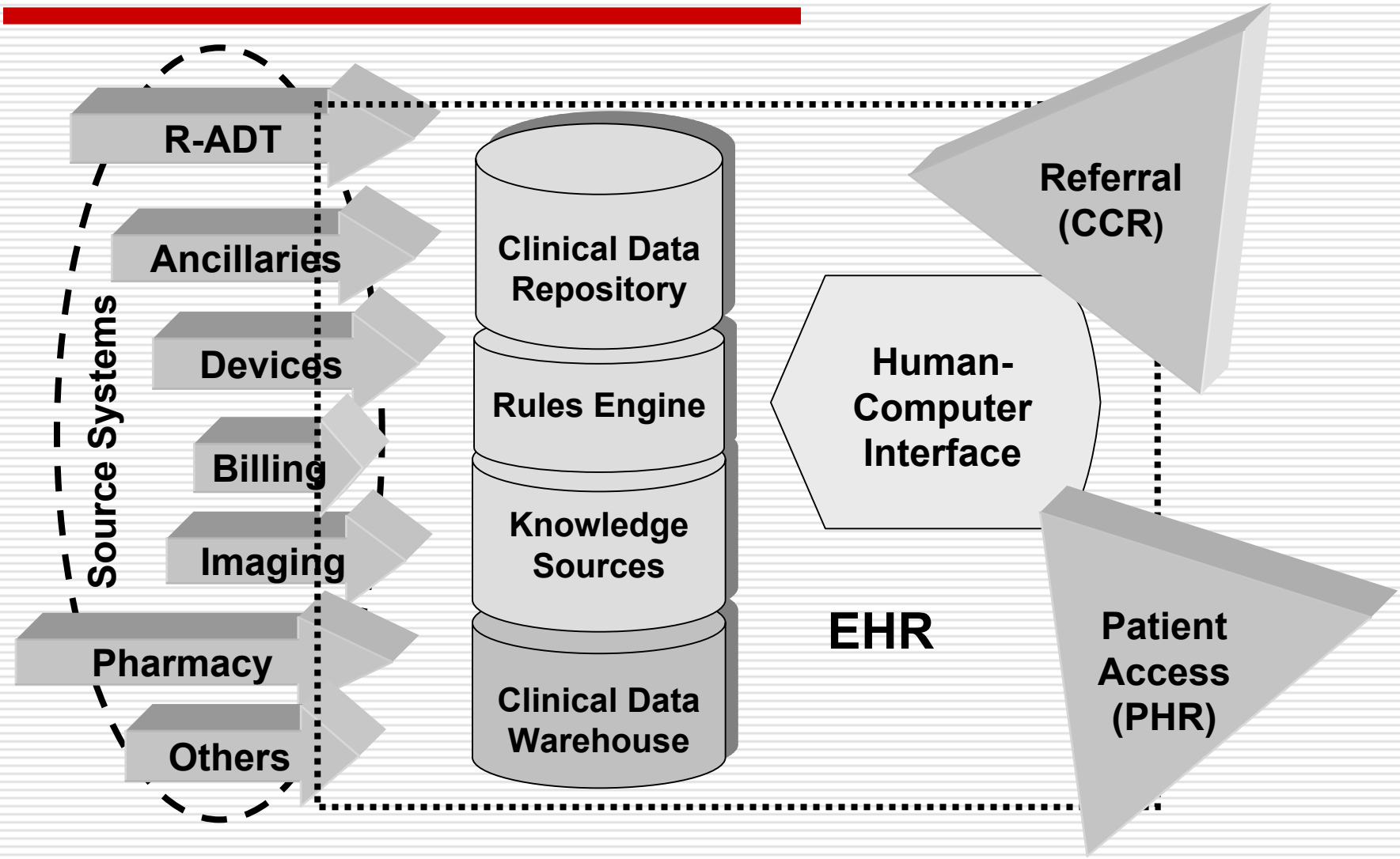
EHRs/NHII: HIPAA Security and EHRs, a Near Perfect Match

Electronic Health Record

EHR Definition

- **System that . . .**
  - **Collects data from multiple sources**
  - **Is used by clinicians as the primary source of information at the point of care**
  - **Provides evidence-based decision support**

EHR Schematic



"System"

- **Hardware**
  - Computers, workstations, printers, other devices
- **Software**
  - Programs that provide instructions for how the computers should work
- **People**
  - Users, administrators, technicians, vendors, etc.
- **Policies**
  - How the system will be used, what benefits are to be achieved
- **Processes**
  - Procedures, screen designs, report layouts, workflow changes, etc.

Point of Care

- Human-computer interface
- Work flow
- Customizable screens
- Ergonomics
- Value proposition

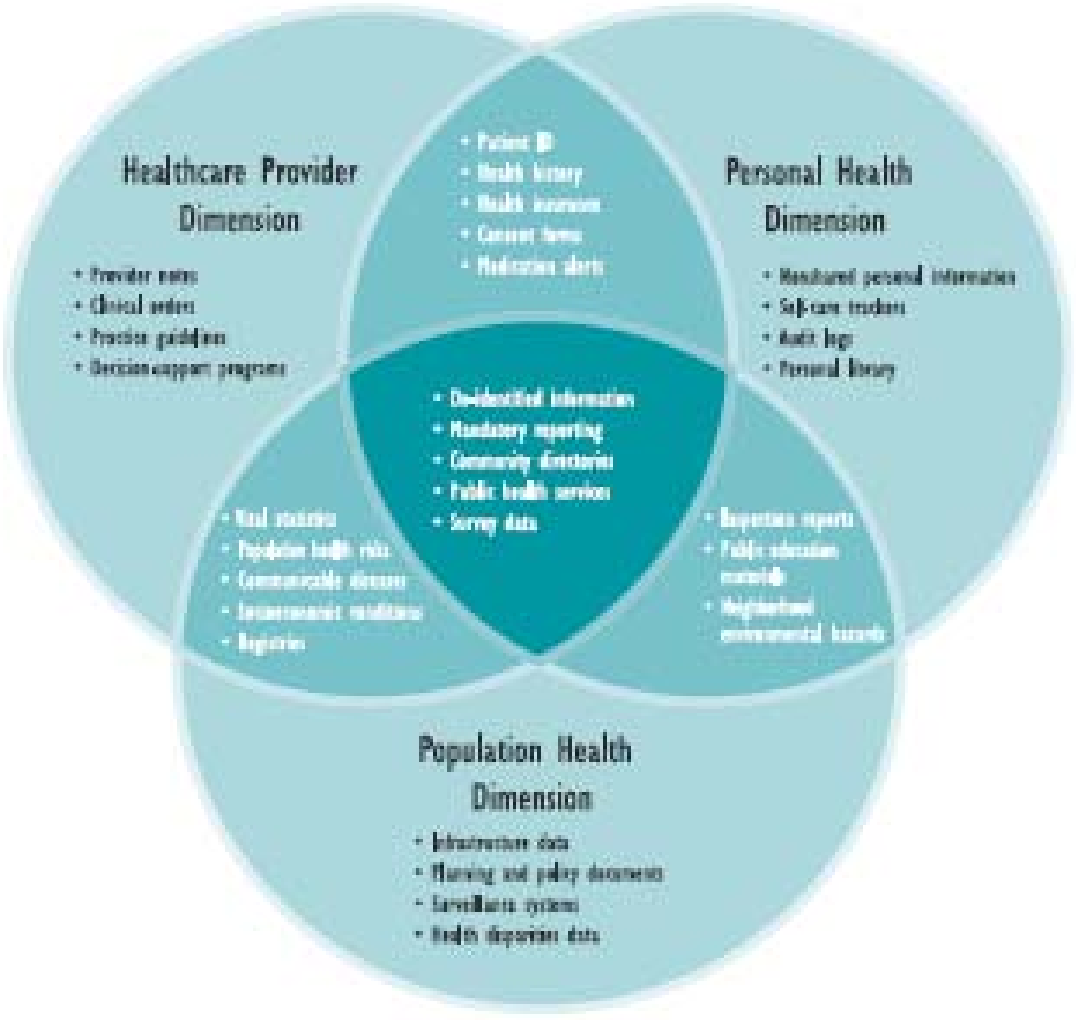
Decision Support

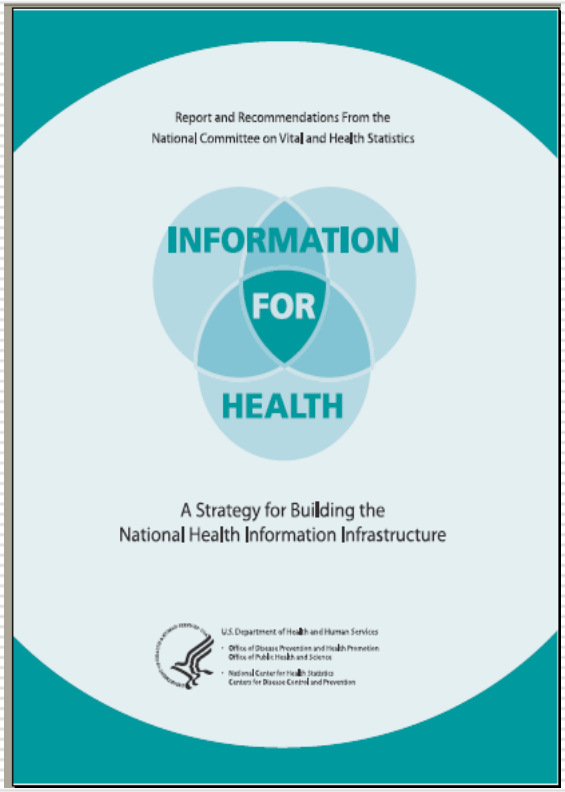
- Reminders
- Alerts
- Structured data entry templates
- Order sets
- External resources
  - Formulary
  - Practice Guidelines

EHRs/NHII: HIPAA Security and EHRs, a Near Perfect Match

National Health Information Infrastructure

NHII





Definition

- An initiative set forth to improve effectiveness, efficiency, and overall quality of health care
- Comprehensive knowledge-based network of interoperable systems of clinical, public health, and personal health information that would improve decision-making by making health information available when and where it is needed
- Set of technologies, standards, applications, systems, values, and laws that support all facets of individual health, health care, and public health

What it is not

- Not a centralized database of medical records
- Not a government regulation
- Not an EHR, PHR, CCR – but a framework within which those and other elements contribute

Local/Regional Initiatives

- Santa Barbara County Care Data Exchange
- Indianapolis Network for Patient Care

- Different approaches, similar goals:
  - Provide a simple and secure way to electronically access patient data across organizations
  - Provide a public utility available to all physicians, caregivers, and consumers
  - Construct an experiment to determine whether a community would share the cost of a regional IT infrastructure[1]

1 The Santa Barbara Vision, Sam Karp, Director, June 22, 2004

LHII Security

- Local security inoperability
  - Encryption standard
  - Public key administration
- Use local "utility"
  - Create and mange security standards
  - May serve to provide security services to some participants (e.g., hardened data center)

NHII Security

- Access and security
  - Authentication
  - Access controls to allowed data
  - Monitors and records access requests
- Identity correlation, using
  - Centralized master person index
  - Intelligent matching of similar records
- Information locator service
  - Links to patient records
  - Demographic data of all patients

EHRs/NHII: HIPAA Security and EHRs, a Near Perfect Match

EHR and Security

Balancing Act

- EHRs can provide greater privacy and security, e.g.,
  - Access controls can be more granular
  - Authentication mechanisms provide audit trails and non-repudiation
  - Disaster recovery plans assure greater availability
  - Encryption can provide confidentiality and data integrity
- But, . . .
  - Information flows more easily, risk of mishap is greater
  - Collection of large volumes of data more feasible and risky
  - Sharing of information for treatment, payment, and operations misunderstood
  - New methods to attack data are continuously being developed

Weakest Links

- The weakest links in the security chain are:
  - People, e.g.,
    - Concerns about "restrictive" access controls
    - Reluctance to authenticate
    - Lack of patient education
  - Policies, e.g.,
    - Widespread use of templates without understanding organization-specific risks
    - Inconsistent management responsibility and accountability
  - Processes, e.g.,
    - Open campuses
    - "Emergency mode"
    - Ownership of record issues

EHR Security Issues

- If an organization make a very large investment in EHR
  - The organization needs to be prepared to make a commensurate investment in security
- EHR is not one more stovepipe, with source documents or print outs as back up
  - The *vision* of EHR is to use the technology for all aspects of patient care

Threat Sources

- **Accidental Acts**
  - Incidental disclosures
  - Errors and omissions
  - Proximity to risk areas
  - Work stoppage
  - Equipment malfunction
- **Deliberate Acts**
  - Inattention/inaction
  - Misuse/abuse of privileges
  - Fraud
  - Theft/embezzlement
  - Extortion
  - Vandalism
  - Crime
- **Environmental threats**
  - Contamination
  - Fire
  - Flood
  - Weather
  - Power
  - HVAC

Vulnerabilities

- Administrative
  - Policy
  - Accountability
  - Management
  - Resources
  - Training
  - Documentation
- Physical
  - Entrance/exit controls
  - Supervision/monitoring
  - Locks, barriers, routes
  - Hardware
  - Property
  - Disposal
- Technical
  - New applications
  - Major modifications
  - Network reconfiguration
  - New hardware
  - Open ports
  - Architecture
  - Controls

Risk Analysis

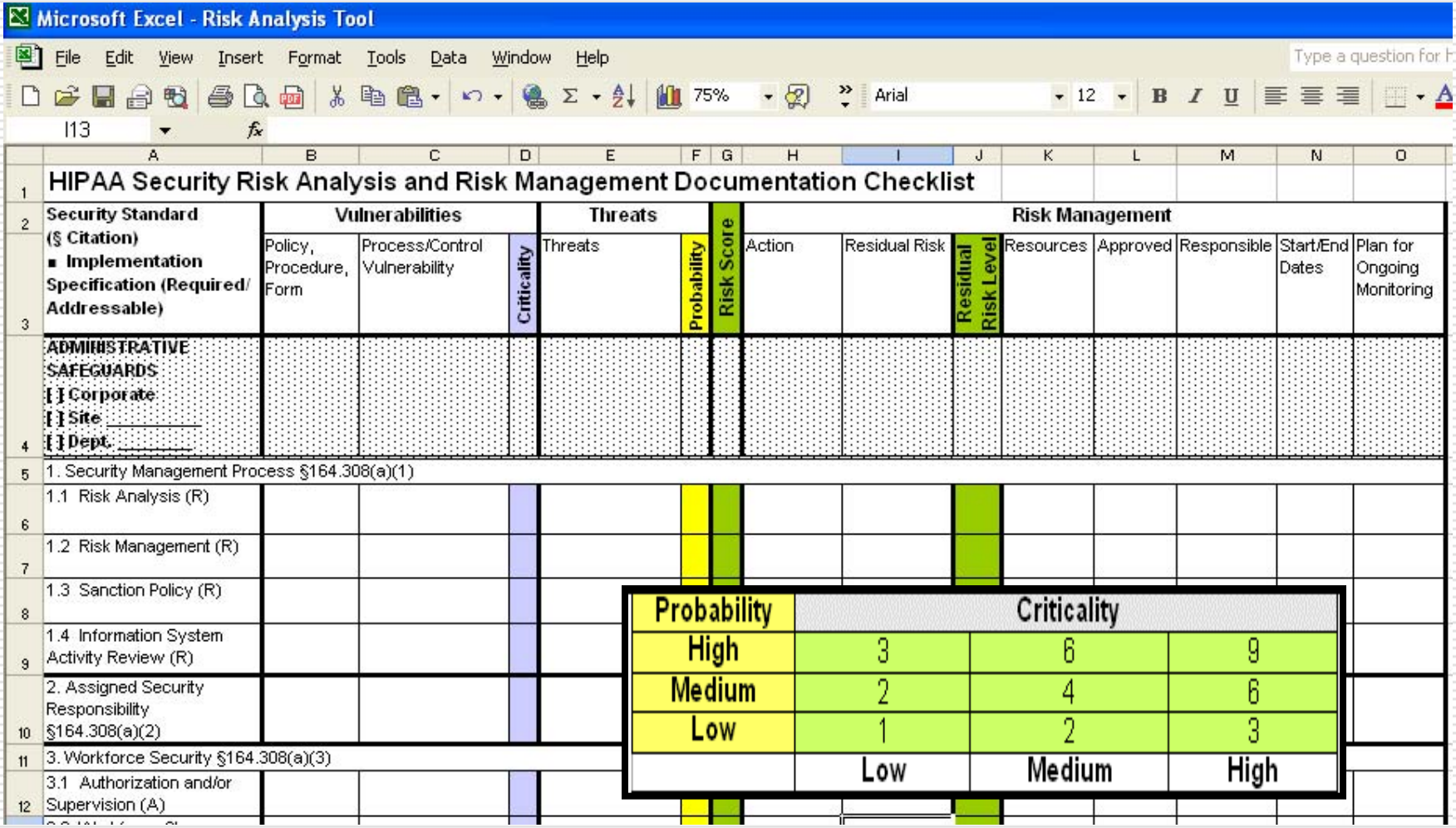
Probability of Occurrence

- Has the *threat* occurred before?
- How frequently?
- Does threat source have:
  - Access, knowledge, motivation?
  - Predictability, forewarning?
  - Known speed of onset, spread, duration?
- Are controls available to:
  - Prevent?
  - Deter?
  - Detect?
  - React?
  - Recover?

Criticality of Impact

- What harm does the *threat exploiting the vulnerability* do to:
  - Patient care?
  - Confidentiality?
  - Potential for complaint/lawsuit?
  - Productivity?
  - Revenue?
  - Cost of remediation?
  - Licensure/ accreditation?
  - Public relations/ consumer confidence, goodwill, competitive advantage?

Risk Management



Probability	Criticality		
High	3	6	9
Medium	2	4	6
Low	1	2	3
	Low	Medium	High

The Latest Apps

- CPOE and e-Rx
- Clinical messaging
- EHR
- Web portals
- CCR
- PHR

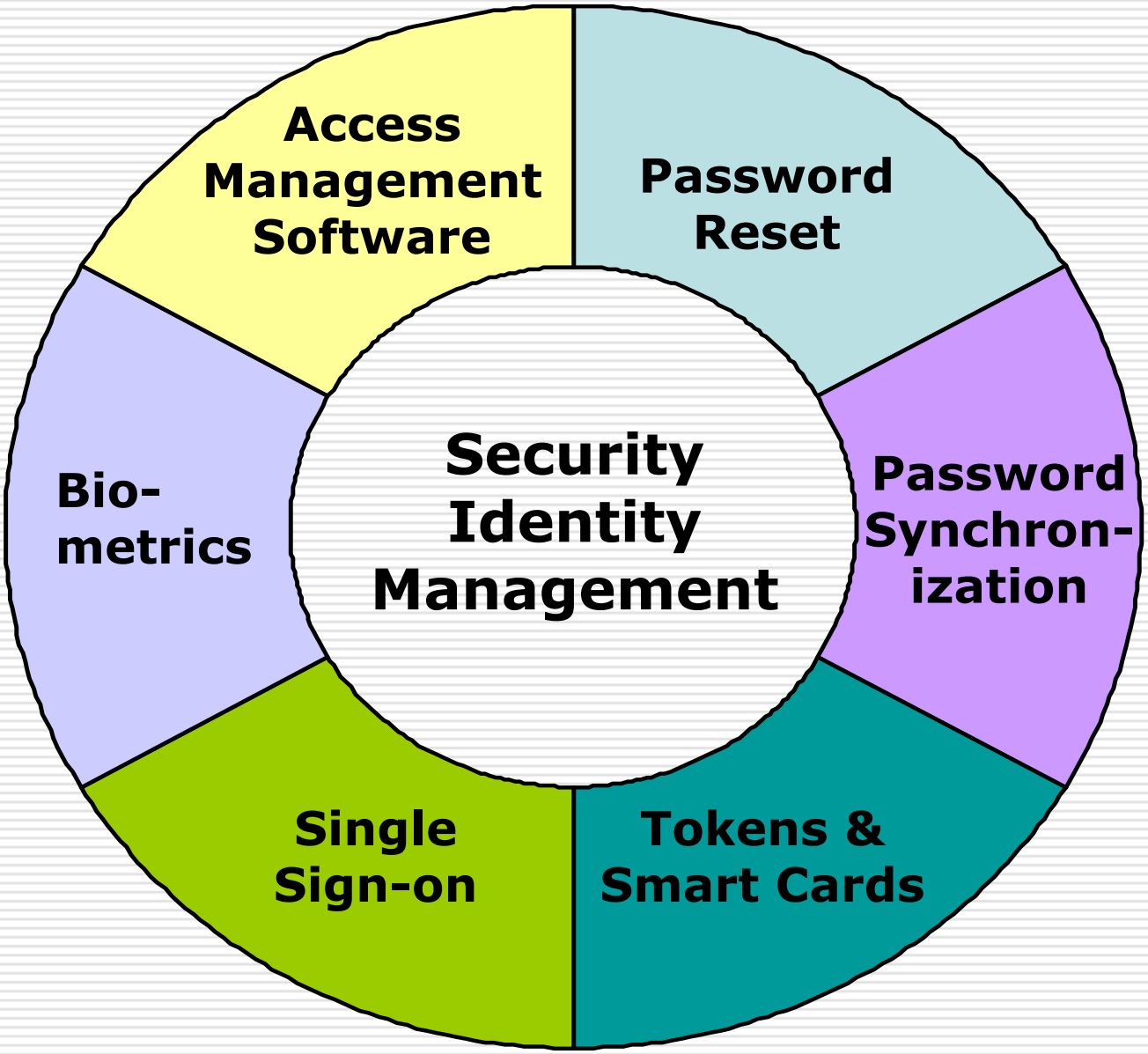
Probability

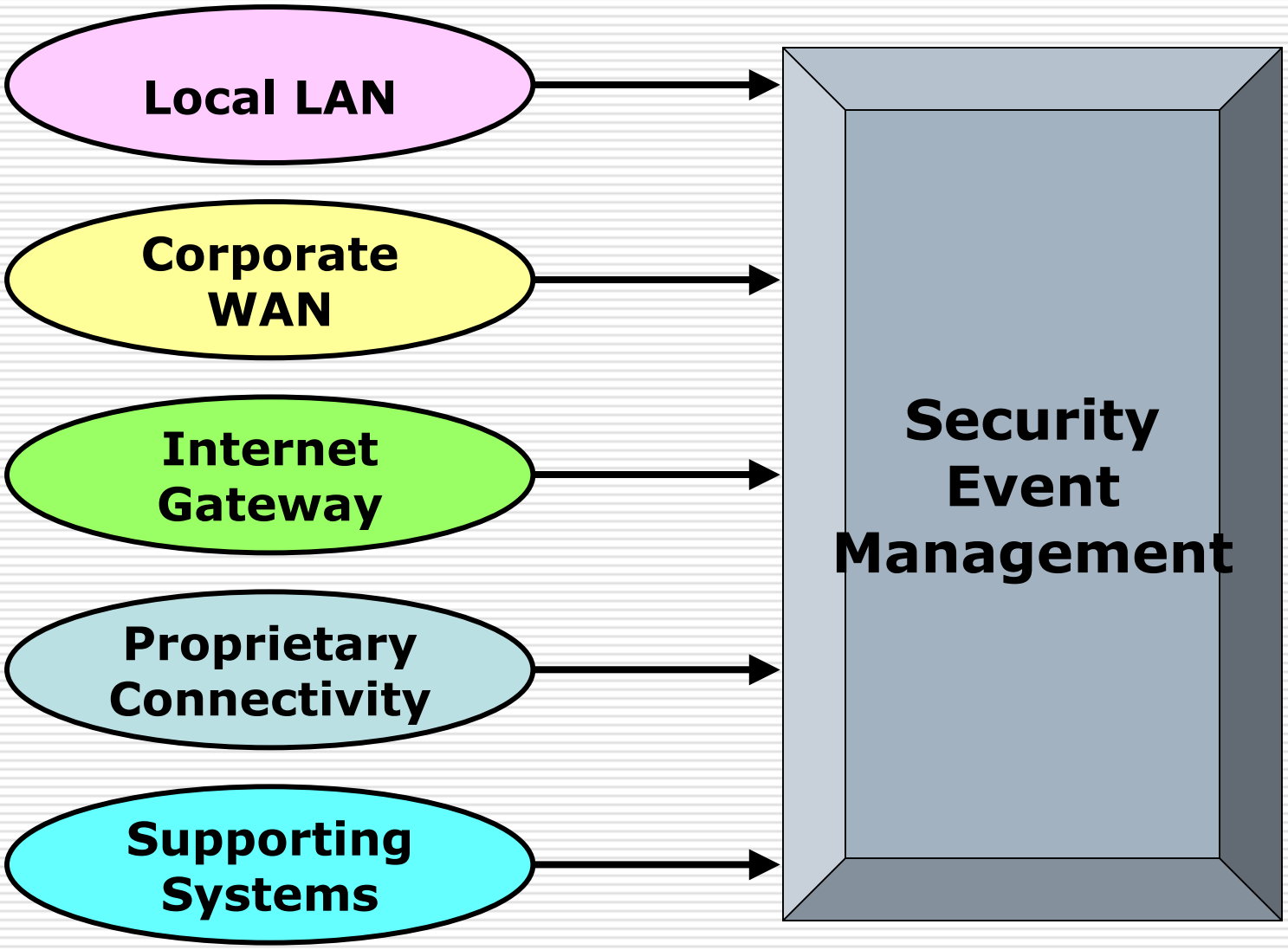
- Critical data
- Unknown viewers
- Ties everything together
- Entrée
- Begins sharing
- Patient access

Criticality

EHRs/NHII: HIPAA Security and EHRs, a Near Perfect Match

EHR, NHII, and Security

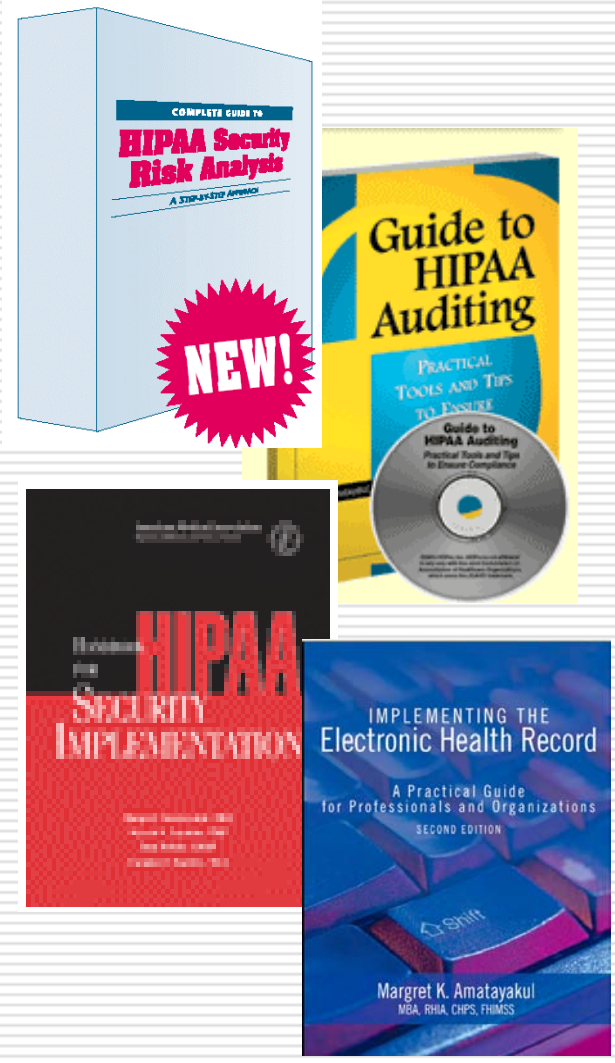




Transmission Protections

- Access controls
- Alarms
- Audit trail
- Encryption
- Entity authentication
- Event reporting
- Integrity controls
- Message authentication

References & Resources



www.brownstone.com

www.hcpro.com

https://catalog.ama-assn.org

www.ahima.org

Contact Information

- **Margret Amatayakul, RHIA, CHPS, FHIMSS**
  Margret\A Consulting, LLC
  Schaumburg, IL
  MargretCPR@aol.com
  www.margret-a.com
- **Steven S. Lazarus, PhD, FHIMSS**
  Boundary Information Group
  Denver, CO
  SSLazarus@aol.com
  www.boundary.net