The Role of Privacy & Security In Meaningful Use

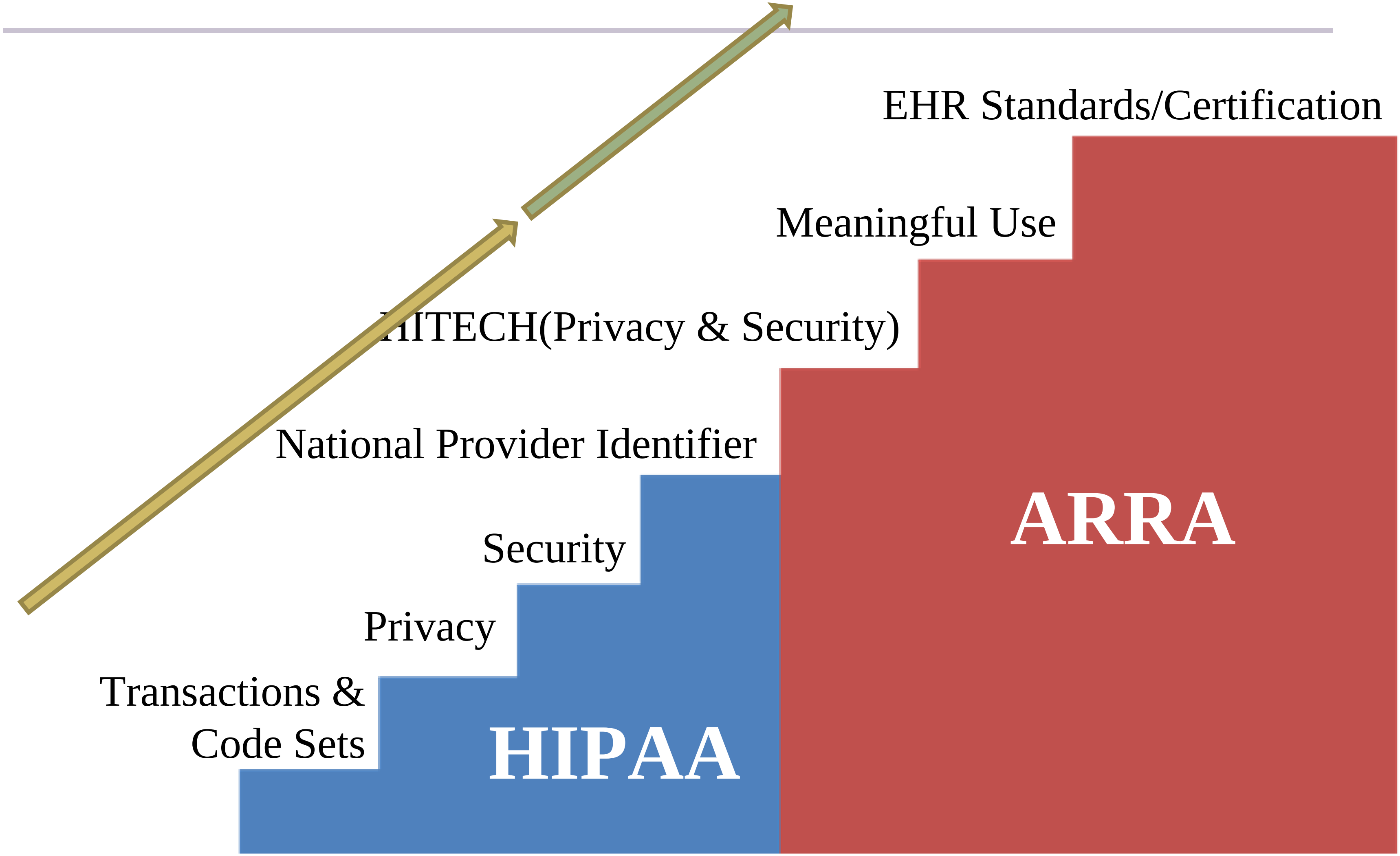
February 2010

Lesley Berkeyheiser, The Clayton Group
N-Tegrity Solutions Group
WEDI SNIP Co-Chair

N-Tegrity Solutions
Group

INTRODUCTION

wedi™



EHR Standards/Certification

Meaningful Use

HITECH(Privacy & Security)

National Provider Identifier

Security

Privacy

Transactions &
Code Sets

HIPAA

ARRA

What is HIPAA?

The Health Insurance Portability and Accountability Act

- Health Insurance Portability
- Standards for Electronic Claims Interchange (EDI)
- Privacy and Security Protection

Privacy Standards

- Notice of privacy practices
- Privacy Official
- Limited state law pre-emption
- Use/Disclosure PHI
- Consent vs. Authorization
- Business Associate rules
- Complaint procedures
- De-identified data
- Minimum Necessary
- Group health plan / employer rules
- Record Keeping
- Mitigation requirements
- Training requirements
- Right of member to access records
- Right to amend/agree and disagree
- Right of member to receive accounting of disclosures
- Rules for disclosures without consent
- Rules for research/marketing

IndividualRights

- Right to Notice of Privacy Practices
  - Clearinghouses and Business Associates do not have to send Notices
- Right to inspection and copies (access)
- Right to amend
- Right to authorize certain non-treatment disclosures
- Right to accounting of disclosures
- Right to request restrictions on use
- Right to request alternative channels of communication
- Right to complain to provider or HHS

What are Uses and Disclosures?

- Use – (data exchanged internally) The sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information
- Disclosure – (data exchanged externally) The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information

General Requirements

- Ensure
  - Confidentiality:
    Only the right people see it
  - Integrity:
    The information is what it is supposed to be
    – it hasn't been changed
  - Availability:
    The right people can see it when needed

Administrative Safeguards

- Protect against reasonably anticipated threats or hazards to the security or integrity of information
- Protect against reasonably anticipated uses and disclosures not permitted by privacy rules
- Ensure compliance by workforce

Administrative Safeguards

- Risk Analysis & Ongoing Risk Management
- Information Access Management
- Security Incident Procedures
- Contingency Plan
- Security Awareness and Training
- Business Associate Contracts
- Evaluation

Physical Safeguards

- Facility Access Controls
- Physical Safeguards
  - Workstation Use/Security
- Device and Media Control
  - Media re-use / Disposal
  - Backup and storage

Technical Safeguards

- Access Controls
  - Unique user identification
  - Automatic Logoff
- Audit Controls
- Integrity
- Person/Entity Authentication
- Transmission Security
  - Encryption

Privacy & Security Challenges

ISSUE # 5: Dentist Changes Process to Safeguard PHI□

- Covered Entity: Health Care Provider□Issue: Safeguards, Minimum Necessary

- An OCR investigation confirmed allegations that a dental practice flagged some of its medical records with a red sticker with the word "AIDS" on the outside cover, and that records were handled so that other patients and staff without need to know could read the sticker.

Privacy & Security Challenges

RESOLUTION # 5:

When notified of the complaint filed with OCR, the dental practice immediately removed the red AIDS sticker from the complainant's file.

To resolve this matter, OCR also required the practice to;

1. Revise its policies and operating procedures and to move medical alert stickers to the inside cover of the records.
2. Further, the covered entity's Privacy Officer and other representatives met with the patient and apologized, and followed the meeting with a written apology.

Along Comes ARRA

ARRA HITECH

American Recovery & Reinvestment Act of 2009

Health Information Technical for Economic and Clinical Health Act

Guidance & Regulations

Description	Dates
Guidance on breach notification – specifying the technologies and methodologies that render PHI unusable, unreadable or indecipherable.	April 18, 2009
Interim final regulations to implement breach notification for HIPAA covered entities and business associates.	April 18, 2009
Regulations to modify the HIPAA Enforcement Rule to implement revised penalty structure.	February 18, 2010
Regulations to extend certain HIPAA Security Rule provisions to business associates.	February 18, 2010
Guidance on technical safeguards to carry out security.	February 18, 2010; annual update

Guidance & Regulations

Description	Dates
Regulations to extend certain HIPAA Privacy Rule provisions to business associates	February 18, 2010
Regulations to modify the HIPAA Privacy Rule’s provisions regarding marketing and fundraising	February 18, 2010
Regulations to clarify that certain entities are HIPAA business associates	February 18, 2010
Guidance on the HIPAA Privacy Rule’s requirements for de-identification	February 18, 2010
Regulations to modify the HIPAA Privacy Rule’s accounting of disclosures provisions	June 18, 2010

Guidance & Regulations

Description	Dates
Guidance on what constitutes “minimum necessary” for purposes of the HIPAA Privacy Rule	August 18, 2010
Regulations to modify the HIPAA Enforcement Rule to implement willful neglect provisions	August 18, 2010
Regulations to modify the HIPAA Privacy Rule to generally prohibit exchanging health information for remuneration without individual authorization	August 18, 2010
Regulations to modify the HIPAA Enforcement Rule to implement provisions for sharing civil money penalties or settlements with harmed individuals	February 18, 2012

Privacy/Security- Standards Rule

- General Encryption and Decryption of Electronic Health Information - AES
- Encryption and Decryption of Electronic Health Information for Exchange - TLS, IPv6, IPv4 with IPsec
- Record Actions Related to Electronic Health Information - Policy
- Verification that Electronic Health Information has not been Altered in Transit - SHA-1 or higher
- Cross-Enterprise Authentication - Policy
- Record Treatment, Payment, and Health Care Operations Disclosures - Policy

Meaningful Use Overview

Policy Vision & Goals*

Vision

Enable significant and measurable improvements in population health through a transformed health care delivery system.

Goals

•Improve quality, safety, and efficiency

•Engage patients and their families

•Improve care coordination

•Improve population and public health

•Ensure privacy and security protections

*Source: Health IT Policy Committee Meaningful Use Workgroup's June 23, 2009 presentation

Meaningful Use

- Provide a summary of care record for at least 80% of transitions of care and referrals. This also implies the ability to receive a record and display it in human readable format
- Perform at least one test of the EHR capacity to submit electronic data to immunization registries.
- Perform at least one test of the EHR's capacity to submit electronic lab results to public health agencies.

Meaningful Use

- Perform at least one test of the EHR's capacity to submit syndromic surveillance data to public health agencies.

- Conduct or review a security risk analysis and implement updates as necessary

Meaningful Use

- Provide 80% of patients who request an electronic copy of their health information in the CCD or CCR format within 48 hours of their request
- Provide 10% of patients with online access to their problem list, medication lists, allergies, lab results within 96 hours of the information being available to the clinician.

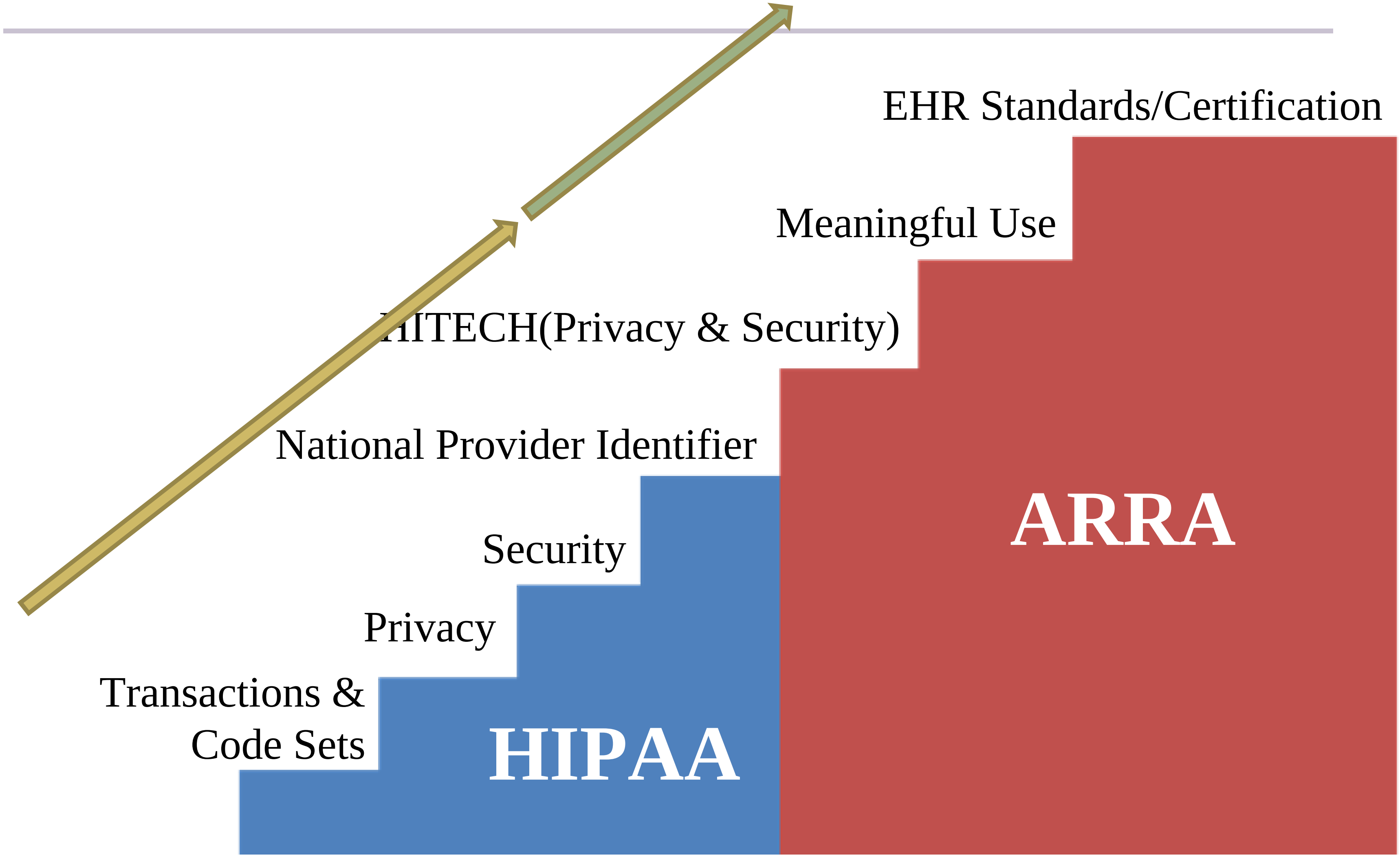
Meaningful Use

- Provide a clinical summary for 80% of all office visits (problem lists, medication lists, allergies, immunizations, and diagnostic test results) in paper or CCD/CCR format
- At least one test of health information exchange among providers of care and patient authorized entities.
- Perform Medication reconciliation for at least 80% of relevant encounters and transitions of care.

Meaningful Use NPRM:

Compliance with HIPAA privacy and security rules is required for all covered entities, regardless of whether they participate in the EHR incentive programs or not. Furthermore, compliance constitutes a wide range of activities, procedures, and infrastructure.

Put It All Together…



Transactions &
Code Sets

Privacy

Security

National Provider Identifier

HITECH(Privacy & Security)

Meaningful Use

EHR Standards/Certification

HIPAA

ARRA

Thank You