HIPAA SUMMIT

Update from the Office of eHealth Standards and Services

HIPAA: Transactions & Code Sets, Identifiers, Security and Enforcement

eHealth: Personal Health Records and ePrescribing

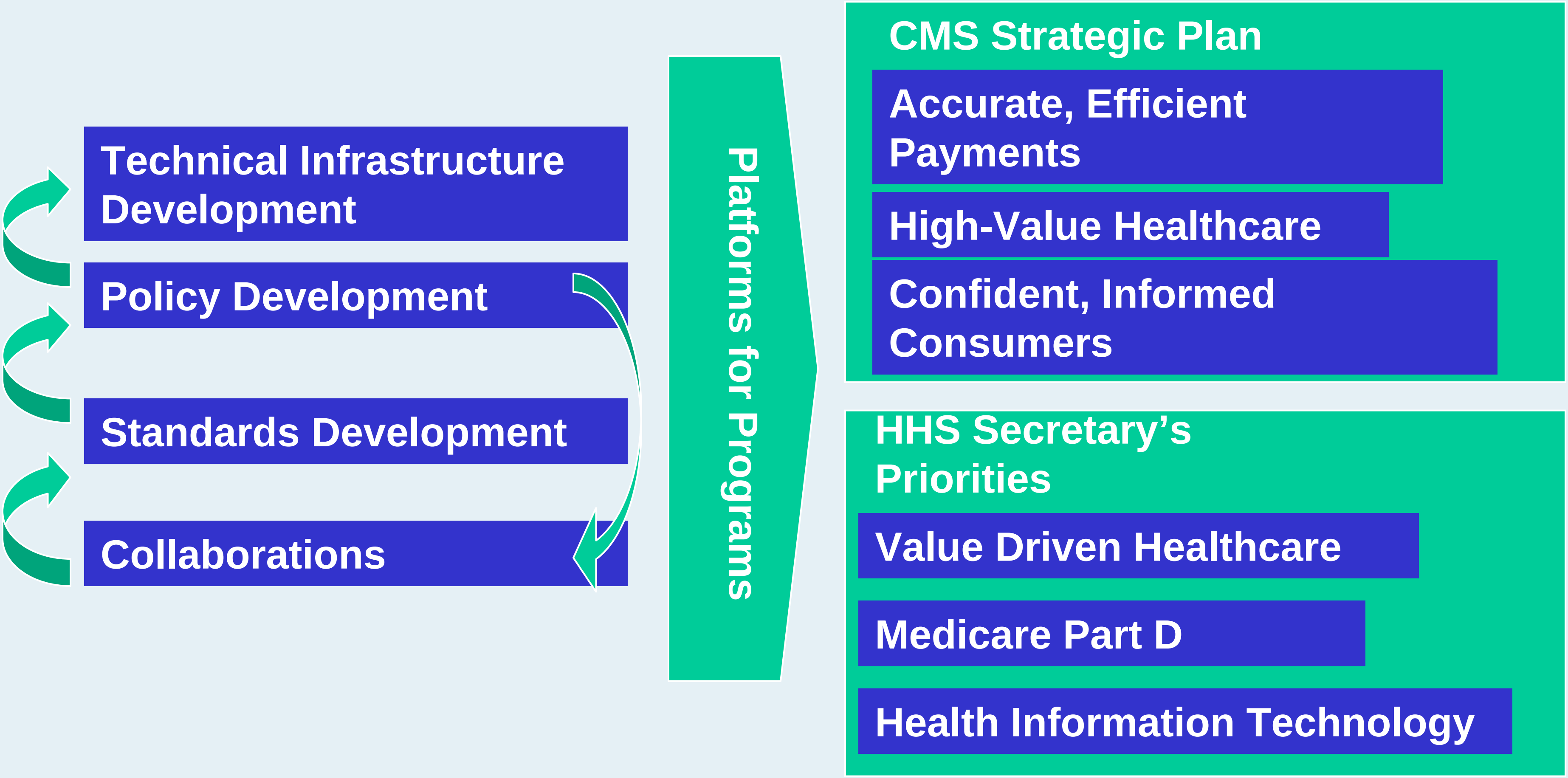
December 14, 2007

Lorraine Tunis Doo, Centers for Medicare & Medicaid Services

DISCUSSION TOPICS

- Strategic Overview
- HIPAA Update
- Enforcement
- Personal Health Records (PHR)
- E-prescribing

CMS E-Health Strategy



Technical Infrastructure Development

Policy Development

Standards Development

Collaborations

Platforms for Programs

CMS Strategic Plan

- Accurate, Efficient Payments
- High-Value Healthcare
- Confident, Informed Consumers

HHS Secretary’s Priorities

- Value Driven Healthcare
- Medicare Part D
- Health Information Technology

Secretary's Value-Driven Health Care – Four Cornerstones

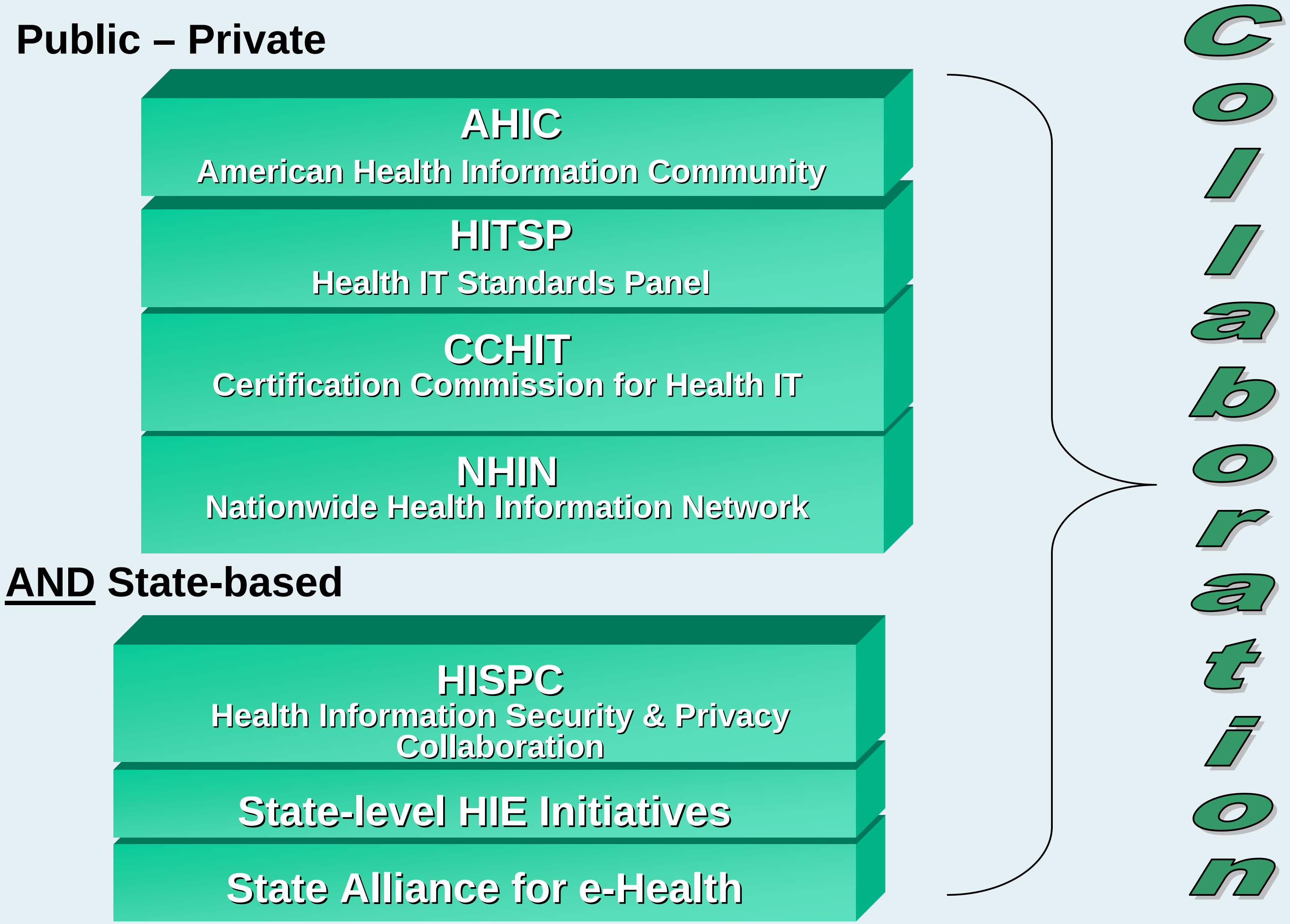
Interoperable Health Information Technology

Quality Transparency

Price Transparency

Incentives for Efficient Health Care

ONC Activities to Foster Health IT Adoption



Public – Private

AHIC
American Health Information Community

HITSP
Health IT Standards Panel

CCHIT
Certification Commission for Health IT

NHIN
Nationwide Health Information Network

AND State-based

HISPC
Health Information Security & Privacy Collaboration

State-level HIE Initiatives

State Alliance for e-Health

Collaboration

HIPAA Update

- ICD-10
- Electronic Health Care Claims Attachments
- 5010 and D.0
- Medicaid Subrogation
- NPI Implementation
- Security
- Enforcement

ICD-10 Update

- Policy discussions continue regarding the timing and implementation of a transition from ICD-9 to ICD-10
- Issues
  - Compliance date
  - Cost to industry
  - Transition issues

ICD-10 Update (Cont)

- CMS awarded contract to American Health Information Management Association (AHIMA) in September 2007
- AHIMA will assess the internal impact of a transition to ICD-10 on CMS systems, policies and operations
- Deliverables include impact analysis, project plan, training assessment and technical coding assistance
- Contract has one base year and four additional option years
- While no decisions on ICD-10 implementation have been made, CMS is being proactive

Claims Attachments

- This is one of the last transaction standards to be adopted under HIPAA
- Affects all covered entities under HIPAA (health plans, health care clearinghouses and certain health care providers)
- Standards proposed:
  - Six types of claims attachments - emergency department; ambulance; rehabilitation (9 disciplines); medications; laboratory results; clinical reports
- Final Rule to be published next year

Transactions Standards – new versions

- Discussions underway regarding need to convert to:
  - Updated version of HIPAA standard for non-pharmacy transactions (X12N version 5010)
  - Updated version of pharmacy transactions standard (NCPDP D.O)
  - New Medicaid subrogation standard (NCPDP)
- Timing must be coordinated with ICD-10, as version 5010 must be implemented before industry can transition to ICD-10
- CMS has contracted with Gartner to prepare industry analysis for the Regulatory Impact/Cost Benefit Analysis

NPI Implementation

- Status
  - May 23, 2007 compliance date (for all but small plans)
  - Contingency guidance released 4/2/07
  - Enforcement will begin effective 5/23/08
  - Data dissemination notice published 5/30/07
  - NPI Registry became operational 9/4/07
  - Approximately 2.37 million providers enumerated (as of 11/30/07)

NPI Implementation Issues (Cont)

- CMS has been actively tracking the process of NPI implementation in Medicare:
  - 86% of claims are being submitted with an NPI, either alone or paired with legacy number (11/30/07)
  - All institutional claims must contain an NPI for primary providers. NPI only or NPI plus legacy number by 1/1/2008.
  - All professional claims must contain an NPI for primary providers. NPI only or NPI Plus legacy number by 3/1/08.
  - Rejection rates of claims (by carriers and FIs) with NPIs ranges from 3% to 27%.

MEDICAID:

  - Connecticut and Delaware have already implemented NPI;
  - 31 states are on a positive track to be ready by 5/23/08 others are at moderate risk.

HIPAA Security Rule

- General Requirements of the Final Security Rule
  - Applies to Electronic Protected Health Information (EPHI) that a covered entity creates, receives, maintains, or transmits
  - Designed to ensure
    - – Confidentiality (only the right people see it)
    - – Integrity (the information is what it is supposed to be – no unauthorized alteration or destruction)
    - – Availability (the right people can see it when needed)

HIPAA Security Rule Update

- Issued Remote Access Guidance in December 2006
- Working with National Institute of Standards and Technology (NIST), Workgroup for Electronic Data Interchange (WEDI), and others to begin extensive education and outreach
  - WEDI Conference – November 2007
  - NIST revised guidance and workshop
- CMS to conduct Compliance Reviews
  - Consistent with authority under Enforcement Rule
  - PricewaterhouseCoopers (PwC) contract

Remote Use and Access to EPHI - Highlights of Guidance

- Published December 28, 2006
- Reiterates requirements and applicability of the HIPAA Security Rule
- Identifies strategies consistent with organizational capabilities
- Three action categories:
  - Conduct Security Risk Assessment
  - Develop and Implement Policies and Procedures (includes training)
  - Implement Mitigation Strategies
- Three risk categories:
  - Data Access
  - Data Storage
  - Data Transmission

Remote Use and Access to EPHI
Example of Risk Mitigation Suggestions - data storage

Risk	Mitigation
Laptop or other portable device is lost or stolen resulting in potential unauthorized/improper access to or modification of EPHI housed or accessible through the device.	✓Identify the types of hardware and electronic media that must be tracked, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards, and security equipment and develop inventory control systems; ✓Implement process for maintaining a record of the movements of, and person(s) responsible for, or permitted to use hardware and electronic media containing EPHI; ✓Require use of lock-down or other locking mechanisms for unattended laptops; ✓Password protect files; ✓Password protect all portable or remote devices that store EPHI; ✓Require that all portable or remote devices that store EPHI employ encryption technologies of the appropriate strength
Use of external device to access corporate data resulting in the loss of operationally critical EPHI on the on the remote device	✓Develop processes to ensure backup of all EPHI entered into remote systems; ✓Deploy policy to encrypt backup and archival media; ensure that policies direct the use of encryption technologies of the appropriate strength
Loss or theft of EPHI left on devices after inappropriate disposal by the organization	Establish EPHI deletion policies and media disposal procedures. At a minimum this involves complete deletion, via specialized deletion tools, of all disks and backup media prior to disposal. For systems at the end of their operational lifecycle, physical destruction may be appropriate

Remote Use and Access to EPHI - Guiding Principles

- The obvious: Workforce must be extremely cautious about offsite use of or access to EPHI
- Covered entities must evaluate their business environment – present and future
  - Ensure policies, procedures, and training have been deployed
  - Conduct ongoing training and awareness campaigns
  - Execute appropriate disciplinary actions and sanctions
- Covered entities must anticipate workforce error
  - Deploy strategies to address unintentional losses of devices or media
  - Mandate that devices and media are protected via passwords, biometrics etc.
  - Determine advantages of encryption on certain devices and media. If encryption is not deployed, select alternative safeguards

What Devices are Affected?

Devices, Media and Connectivity Tools:

- ❑ Laptops
- ❑ Home based personal computers
- ❑ Personal Digital Assistants (PDAs)
- ❑ Smart Phones
- ❑ Library, Hotel, and other public PCs
- ❑ Wireless Access Points
- ❑ USB Flash Drives
- ❑ CDs and DVDs
- ❑ Floppy Disks
- ❑ Backup Media
- ❑ Email
- ❑ Smart Cards

HIPAA Enforcement Process

- Complaint Driven – emphasizes voluntary compliance
- Complainant must submit sufficient detail to allow CMS to pursue allegations
  - complainant will be contacted for additional information if necessary
- Most Security complaints are initiated as Privacy complaints
  - “Dual Process” complaints are managed in collaboration with the Office for Civil Rights (OCR)

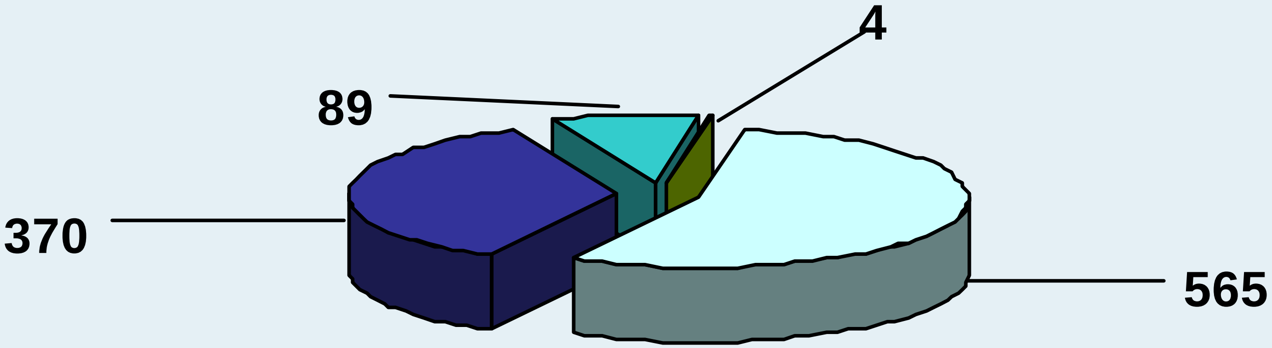
HIPAA Enforcement Process (con’t)

- CMS or OCR notifies “filed against entities” (FAE) of the complaint, and requests a response within 30 days. Response may include:
  - Attestation or information demonstrating compliance; or
  - Statement of facts explaining its disagreement with the allegations; or
  - A corrective action plan and timeline
- CMS monitors corrective action plans and conducts regular follow up to track status
- If appropriate, some cases are referred to the Department of Justice (DOJ) for consideration

Types of Complaints

- Transactions and Code Sets
  - Trading Partner Agreements
  - Incorrect application of the Implementation Guide
  - Misuse of code set instructions
  - Inability to process the 835 properly (balancing)
- Identifiers
  - No complaints for Employer Identifier
  - Contingency plans may be delaying complaints about NPI use
- Security
  - Unauthorized access to EPHI
  - Insufficient access controls
  - Loss of data (e.g. on portable devices)

CMS Enforcement Statistics Report
Open and Closed cases by type
As of October 30, 2007



Complaint Type	Total	Open	Closed
Transactions and Code Sets (TCS)	565	92	473
Security	370	140	230
National Provider Identifier (NPI)	4	0	4
Other- Includes invalid and test cases	89	10	79
Total	1028	242	786

Open – Outstanding issues remain. Entity may be under a corrective action plan or additional information from either the complainant, the filed against entity, or both is being sought.

Closed – No further action required. All issues have been sufficiently resolved. Please note that 39 of the 223 security cases have been closed via corrective actions.

Personal Health Records (PHRs)

- Potential CMS roles to meet beneficiary needs for PHRs:
  - Make Medicare data available to PHRs
  - Support standards for PHRs
  - Support interoperability between PHRs, and between PHRs and EHRs
  - “Certify” PHRs as meeting certain functionality, security and privacy requirements
  - Educate beneficiaries on the uses and benefits of PHRs

PHR Work to Date

- 2005 RFI soliciting public feedback on CMS’ role with regard to PHRs
  - Over 50 responses from PHR vendors, health plans, providers, and other associations
  - Interest in real-time claims data, benefit information, and health screening reminders
  - Assurance of privacy and security critical
  - CMS should NOT build its own PHR
- 2006 Feasibility test using Medicare claims data
  - Successfully tested the transfer of Medicare claims data for a group of beneficiaries into existing internet-based PHRs
  - Claims data translated into plain English
  - Transferred over 200,000 Medicare claims

Medication History Pilot (Medicare Advantage and Part D)

- 2007 Medication History & Registration Summary (i.e., “Clipboard”) Pilot
  - Supports AHIC Consumer Empowerment Workgroup recommendation
  - Voluntary study with Medicare Advantage organizations and Part D drug plans
  - BCBSA and AHIP have been active partners
  - Agency for Healthcare Research and Quality (AHRQ) and Office of the National Coordinator (ONC) to conduct evaluation

Medicare Fee-for-Service Pilot

- 2007 Medicare Fee-for-Service (FFS) Pilot
  - Contract awarded in September 2007
  - Will test outreach to, and adoption of PHRs by FFS Medicare beneficiaries
  - Use existing PHR – HealthTrio
  - Medicare contractor to provide claims data - Palmetto
  - Target 500k beneficiaries in South Carolina
  - Plan to leverage successful Part D outreach efforts
  - Launch expected in early 2008; Pilot will run for approximately 9 months
  - Office of the Assistant Secretary for Planning and Evaluation (ASPE) to fund evaluation

How Pilots will be Evaluated

- One contractor will conduct evaluation for both Plan based and FFS pilots
  - Utilization Statistics
    - Number of registrants
    - Number of repeat users
    - Other demographics (age, sex, disability etc)
  - Focus groups and/or surveys of stakeholders to assess:
    - Perception of privacy and security features
    - Accuracy of claims based data
    - Ease of use
    - Favored functions and desired functionality
    - Perceived value for managing health conditions
    - Most effective outreach methods (to impact adoption)

Business Process & Infrastructure to support CMS PHR initiatives

- 2007 Business Process & Infrastructure Design (contract awarded in July 2007)
  - Identify technical and business infrastructure requirements to support large-scale PHR efforts
    - Data sources
    - Data use policies and procedures
    - Compliance with privacy and security regulations
  - Develop alternatives analysis with options for integration with mymedicare.gov
  - Identify financing requirements and options
  - Prepare formal Concept of Operations for CMS

PHR Outreach and Messaging

- 2007-2008 Messaging and Communication
  - Explore what beneficiaries know and understand about PHRs
  - Identify perceived benefits and drawbacks of PHRs
  - Assess the influence of CMS materials, messages and non-CMS resources and tools on beneficiary understanding and use of PHRs
  - Identify information, messages and materials that may help beneficiaries understand and use PHRs

Potential Future PHR Activities

- 2008 - 2011 – Build technical infrastructure to support large-scale beneficiary use of PHRs
  - Leverage results of the design efforts to begin building the infrastructure and expand pilot efforts

- 2010 - ? – Implement Education and Outreach initiatives
  - Begin widespread focused beneficiary outreach and education

E-prescribing and MMA

- Medicare Modernization Act (MMA) 2003 created ambulatory e-prescribing for Part D plans
  - E-prescribing foundation standards implemented January 1, 2006
  - Pilot testing of initial standards in CY 2006
  - Report to Congress April 2007
  - Final uniform standards by April 1, 2008
  - Final standards effective no later than one year after promulgation of final uniform standards

E-prescribing Foundation Standards

- Adopted by Secretary based on National Committee on Vital and Health Statistics (NCVHS) recommendations and industry experience, went into effect January 1, 2006

  - **NCPDP SCRIPT Standard, Version 5.0* -** For transactions between prescribers and dispensers for new prescriptions, refills, changes, cancellations and messaging

  - **ASC X12N 270/271, Version 4010 and Addenda -** For eligibility and benefits inquiries and responses between prescribers and Part D sponsors

  - **NCPDP Telecommunications Standard, Version 5.1 -** For eligibility and benefits inquiries and responses between dispensers and Part D sponsors

E-prescribing Pilot Summary

- Pilot conducted in CY 06 to test initial standards for which there was not adequate industry experience:
  - Formulary & Benefit Information (NCPDP Formulary & Benefits Standard Version 1.0)
  - Exchange of Medication History (NCPDP SCRIPT 8.1)
  - Fill Status Notification (NCPDP SCRIPT 8.1)
  - Structured and Codified SIG (Structured and Codified SIG Standard 1.0)
  - Clinical Drug Terminology (RxNorm)
  - Prior Authorization Messaging (ACS X12N 278/275 with HL7)
- Conducted by CMS through a cooperative agreement with AHRQ
- Findings released in report to Congress April 2007

E-prescribing Pilot Conclusions

- Formulary & Benefits and Medication History are ready for Part D use
- Fill Status Notification is technically sound but there is no pressing marketplace demand
- RxNorm, Prior Authorization and Codified SIG still need work
- Long-term care settings will be ready for e-prescribing with workarounds
- More time, more pilot testing will be needed
- Pilot findings informed NPRM, expected to be published later this year

E-prescribing Next Steps

- Complete initial standards work
- Accelerate education and outreach
- Integrate controlled substances
- Develop process for future standards
- Tie closer to overall HIT/EHR Adoption Strategies
- Incentives, mandates?

Overall Summary and Conclusion

- Collaboration with internal HHS and external partners is critical to moving forward with CMS' E-Health Strategy
- Approaches will continue evolve over the next several years with changing politics, priorities, and technology innovations
- Publication of regulations will guide industry to action
- Publish additional guidance on remote access and other security issues as appropriate
- Publicize enforcement statistics, actions and case examples
- Maintain ongoing partnership with industry organizations to identify and address relevant issues that require guidance or communication

QUESTIONS