

CMS' Framework for HIPAA Privacy Rule Implementation, Ongoing Compliance, and Data Stewardship

Mike Pagels, M.P.A., Technical Advisor

Office of E-Health Standards and Services
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services

Overview

- CMS and Federal Privacy Laws.
- CMS' Approach to HIPAA Privacy Rule Implementation.
- Going Forward—Ongoing Compliance and Data Stewardship.

Major Privacy Laws Governing CMS' Programs

- The Privacy Act of 1974 -- applies to all individually identifiable data held in CMS' systems of records. This includes all program data held by CMS for the Medicare, Medicaid/SCHIP, and Part C and D programs.
- The HIPAA Privacy Rule -- applies to protected health information (PHI) held by a covered entity, i.e., health plans, providers, and clearinghouses.

CMS Programs and HIPAA Privacy

- Medicare Fee-for-Service program is a HIPAA covered entity as a health plan.
- Medicare Advantage and Prescription Drug Plans, as health plans, are covered entities in their own right.
- State Medicaid Agencies/SCHIP programs are covered entities (health plans) in their own right and also subject to Title 19's privacy provisions.
- Quality Improvement Organizations (QIO) are not covered entities – QIOs are oversight organizations under Title 11 and subject to strict confidentiality provisions.

Phased Approach for Privacy Implementation

- Executive Buy-In,
- Review CMS Business Functions,
- Identify New Business Processes,
- Develop Workplans for Data Management Systems,
- Communication/Outreach.

Major Implementation Buckets

- Medicare's Notice of Privacy Practices,
- Business Associate Agreements,
- Designated Record Set,
- Privacy Accountability Database,
- Medicare's Standard Authorization,
- Privacy Complaints,
- Privacy Board.

Ongoing Compliance Activities

- Annual privacy reminders to agency business partners and others who get CMS data.
- More protective Data Use Agreements.
- Updated annual Privacy and Security Computer Based Training.
- Limited Data Sets and Public Use Files.

CMS' Data Governance Board

- Reviews strategic issues related to data governance and privacy.
- Clarifies and resolves common data governance and stewardship challenges relating to privacy, security, trust, and enterprise-wide compliance.
- Aligns the agency's mission and initiatives with data collection, use, and disclosure policies and privacy policies.
- Chaired by CMS' Senior Agency Official for Privacy and comprised of agency's executive leadership (staffed by the Office of E-Health Standards and Services).

Stewardship Issues Going Forward

- Ensuring data disclosures, including precedent-setting data requests, are aligned with CMS Strategic Plan.
- Building security and privacy protections into data systems life cycle development, including surveillance activities for data use agreements.
- Documenting agency privacy policies and procedures to ensure a consolidated, consistent, and coordinated compliance program.

Questions?

