

\_experience the commitment



# HIPAA Regulation of Medicaid Uses and Disclosures of Health Information

Michael J. Mahoney, JD  
Director of Regulatory Affairs and Counsel

# Agenda

- What is HIPAA?
- What's Regulated and What's Not?
- Privacy: Principal Principles
- Internal Uses of PHI by Medicaid Agencies
- Disclosures of PHI by Medicaid Agencies
- Questions and Discussion



# Not on the Agenda

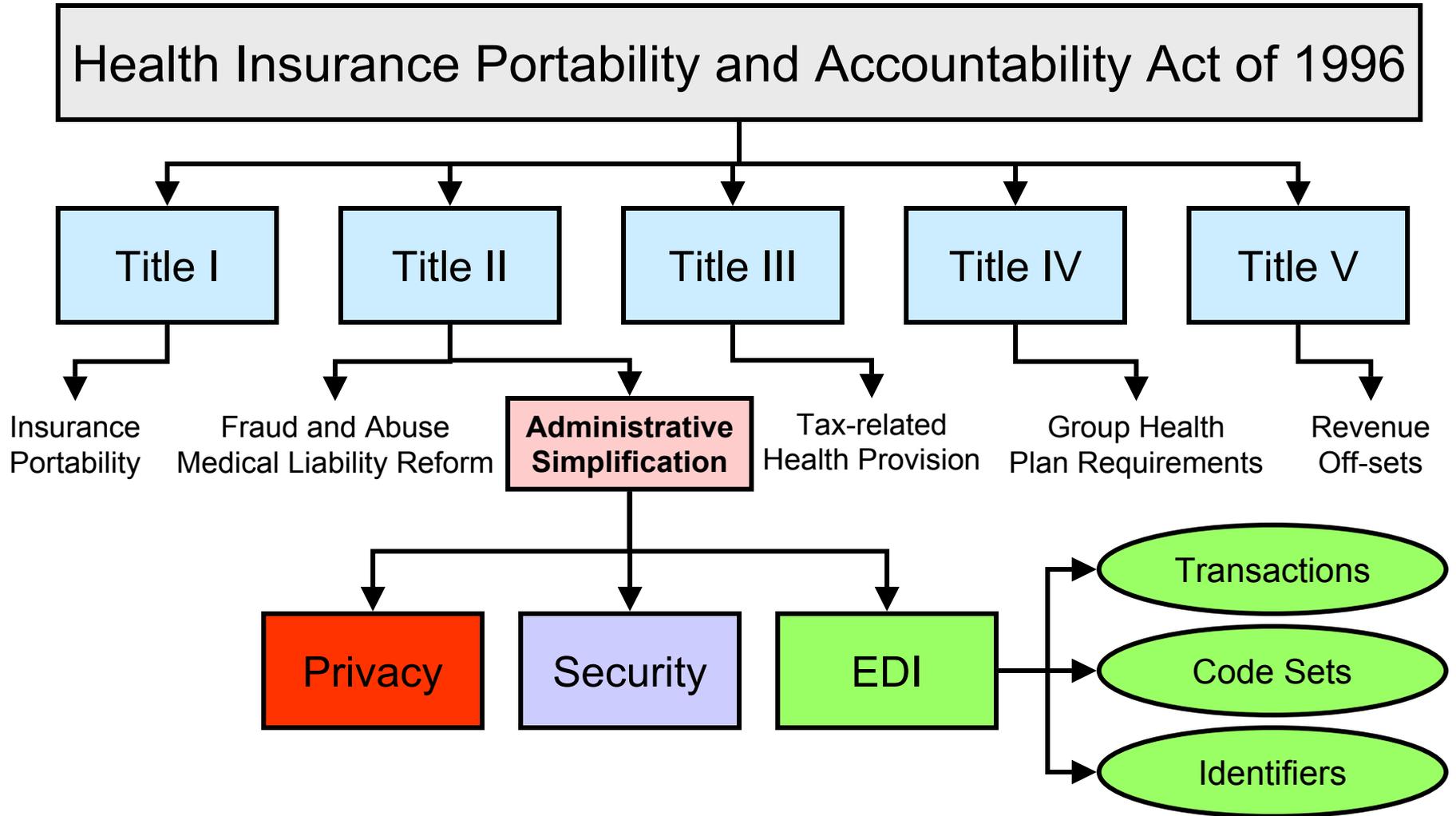
- Will not try to make you follow the various twists and turns that the privacy regulations have taken from:
  - November 1999 Notice of Proposed Rule Making
  - December 2000 “Final” Rule
  - July 2001 Guidance
  - May 2002 Proposed Modifications
  - August 2002 Final Rule
  - December 2002 Guidance



# What is HIPAA?



# Highly Impossible Program for Anyone to Administer?



# Administrative Simplification Background

- The result of government and private industry efforts to create a legal framework to encourage standardizing electronic data interchange in the health care arena
- Simultaneously aimed at protecting the privacy and security of health information
- Privacy regulations were necessitated by Congress' failure to adopt privacy legislation within 3 years of HIPAA's enactment in 1996



# Administrative Simplification Components

## Components of Title II, Subtitle F of HIPAA:

- Electronic health transactions and code sets
- Unique Identifiers
  - Employer ID
  - Health Plan ID
  - Provider ID
  - Individual ID (?)
- Security and Electronic Signature
- Privacy



# Compliance Deadlines

- Electronic health transactions and code sets
    - Compliance required by 10/16/03, provided that a request for extension was filed with DHHS by 10/15/02
  - Unique Identifiers
    - IRS EIN: 7/30/04
    - 2 years from effective dates for others
  - Security
    - 2 years from effective date
    - Electronic signature likely to be dropped
  - Privacy
    - **Compliance required by 4/14/03**
- (Small health plans generally have an additional year to comply)



# Penalties: Civil

- Violations of the Administrative Simplification regulations are punishable civilly as follows:
  - A fine of not more than \$100 per person per violation (but not more than \$25,000 per person per violation of a single standard in a calendar year)
  - Not applicable where:
    - ✓ The person did not know, and by exercising reasonable diligence would not have known, of the violation
    - ✓ The failure to comply was due to a reasonable cause and not to willful neglect
    - ✓ The failure to comply is corrected with 30 days of discovering the violation



# Penalties: Criminal

- Knowingly use a unique health identifier, or obtain or disclose individually identifiable health information:
  - A criminal fine of not more than \$50,000 and/or
  - imprisonment of not more than 1 year
- If the offense is “under false pretenses”:
  - A fine of not more than \$100,000 and/or
  - imprisonment of not more than 5 years
- If the offense is “with intent to sell, transfer or use for commercial advantage, personal gain, or malicious harm”:
  - A fine of not more than \$250,000 and/or
  - imprisonment of not more than 10 years



# Civil Liability Likely

- HIPAA Administrative Simplification regulations are likely to emerge as the common law standard of care for protection of health information (privacy and security)
  - Common law tort liability for disclosure of confidential health information becoming well established (breach of confidence, invasion of privacy, etc.)
  - Statute/regulations can be at least persuasive in defining minimum acceptable protection



# What's Regulated and What's Not?

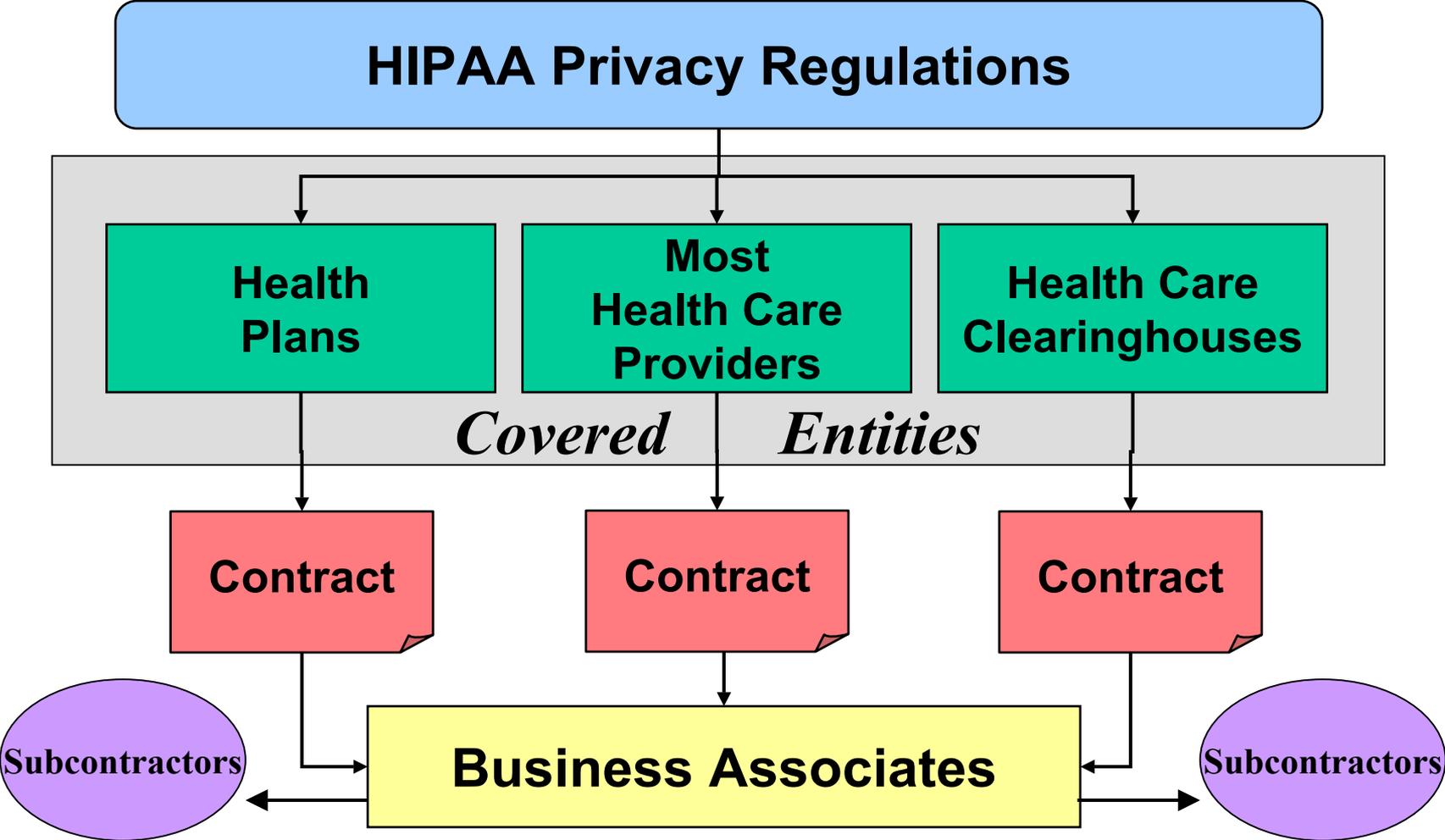


# Covered Entities

- Regulated directly:
  - Health plans (including Medicaid agencies)
  - Healthcare clearinghouses
  - Providers conducting regulated electronic transactions (directly or indirectly)
- Regulated by contract:
  - Business associates and their subcontractors
  - Chain of trust & trading partners
  - Employers (?)



# Covered Entities (con't)



# Protected Health Information

- All individually identifiable health information that is:
  - Transmitted by or maintained in any electronic media; or
  - Transmitted or maintained in any other form or media (e.g., paper and verbal)
- Exceptions:
  - Certain federally-protected education records
  - Employment records held by a covered entity in its role as employer



# Individually Identifiable Health Information

- Information that is a subset of health information, including demographic information collected from an individual, that (i) is created or received by a covered entity and (ii) relates to:
  - An individual's (i.e., the person who is the subject of the information) physical or mental health or condition (past, present or future);
  - The provision of health care to an individual; or
  - The payment for health care rendered to an individual
  - And:
    - ✓ That identifies the individual; or
    - ✓ For which there is a “reasonable basis” to believe that the information can be used to identify the individual.



# PHI Is Broadly Defined

- Privacy Rule does not apply to de-identified information, but “safe harbor” rigorously defined to require deletion of:
  - Name
  - Geographic subdivision smaller than a state
  - Any elements of dates relating to an individual
  - Telephone, fax or e-mail address
  - SSN or health plan, medical record, account, or certificate/license numbers
  - Vehicle or device identifiers
  - URLs or IP address numbers
  - Biometric identifiers or full face photograph
  - Other unique identifying number, characteristic or code



# Privacy: Principal Principles



# Relevant Privacy Principles: Definitions

- Definition of Use and Disclosure:
  - Use means the sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information
  - Disclosure means the release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information



# Relevant Privacy Principles: TPO

- No patient consent, authorization or other approval (written or verbal) is needed to use or disclose PHI for treatment, payment, and/or health care operations (TPO)
- Other uses and disclosures of PHI require the specific, written authorization of the individual (required elements include purpose of disclosure, expiration date/event, etc.), except:
  - When required by law
  - When specifically permitted by the Privacy Rule
  - When the Privacy Rule requires only an opportunity for the individual to agree or object



# Relevant Privacy Principles: Min. Necessary

- When using or disclosing PHI, and when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose, except:
  - Disclosures to, or requests by, a health care provider for treatment purposes
  - Uses or disclosures made to the individual
  - Uses or disclosures made pursuant to an authorization
  - Disclosures to the Secretary of HHS
  - Uses or disclosures required by law or for compliance with the Privacy Rule



# Minimum Necessary (con't)

- Each covered entity must identify those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties
- Each covered entity must make reasonable efforts to limit the access of such persons to only the minimum amount of PHI necessary



# Relevant Privacy Principles: Verification

- Prior to any permissible disclosure (excluding where the individual is entitled to agree or object), a covered entity must:
  - Verify the identity of the person requesting PHI and the authority of the person to have access to such information (unless the covered entity already knows the person's identity and authority)
  - Obtain any documentation, statement, or representation that is a condition of disclosure under the Privacy Rule



# Relevant Privacy Principles: Preemption

- HIPAA preempts contrary state laws, except when:
  - The Secretary of HHS determines that the state law is necessary for certain specified purposes (e.g., prevent fraud or abuse) or is principally focused on controlled substances
  - The state law relates to health information privacy and is more stringent than HIPAA (e.g., greater restrictions on use or disclosure, provides greater rights of access or amendment, narrows scope or duration of authorizations)
  - The state law provides for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention
  - The state law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals



# Relevant Privacy Principles: NOPP

- Individuals who are the subject of PHI are entitled to receive a written Notice of Privacy Practices from each covered entity that describes its permitted and required uses and disclosures of PHI and explains the individual's privacy-related rights
- Health plans must provide the NOPP:
  - To then-covered individuals by 4/14/03
  - To new enrollees at the time of enrollment
  - To then-covered individuals within 60 days of a material revision to the NOPP
- At least once every 3 years, health plans must notify then-covered individuals of the availability of the NOPP and how to obtain a copy



# Internal Uses of PHI by Medicaid Agencies



# Many Different Medicaid Uses & Users



[www.mhccm.org](http://www.mhccm.org)



# Definition of Treatment

- The provision, coordination, or management of health care and related services by one or more health care providers, including:
  - The coordination or management of health care by a provider with a third party
  - Consultation between health care providers relating to a patient
  - The referral of a patient for health care from one provider to another
- By definition, plans do not engage in “treatment” unless they step into the role of “provider”



# Definition of Payment

- Activities undertaken by a health plan to obtain premiums or fulfill its responsibility for coverage and the provision of benefits, or by a provider or plan to obtain or provide reimbursement for the provision of health care
- The above include, but are not limited to:
  - Determinations of eligibility or coverage, COB, and adjudication and subrogation of claims
  - Risk adjusting amounts due
  - Billing, claims management, collection, obtaining payment, and data processing
  - Medical necessity and utilization reviews
  - Certain disclosures to consumer reporting agencies relating to collection of premiums or reimbursement



# Definition of Health Care Operations

- Quality assessment and improvement activities, including:
  - Outcomes evaluation and development of clinical guidelines (but not studies intended to produce generalizable knowledge, which are subject to rules on research)
  - Population-based activities relating to improving health or reducing health care costs
  - Protocol development
  - Case management and care coordination
  - Contacting patients and providers about treatment alternatives



# Definition of Health Care Operations (con't)

- Review of the competence or qualifications of health care professionals
- Evaluating practitioner and provider performance
- Evaluating health plan performance
- Conducting health care training programs
- Training of non-health care professionals
- Accreditation, certification, licensing, and credentialing activities
- Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, or a contract of reinsurance



# Definition of Health Care Operations (con't)

- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs
- Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating the entity, including:
  - Formulary development and administration
  - Development or improvement of payment methodologies or coverage policies



# Definition of Health Care Operations (cont')

- Business management and general administrative activities, including but not limited to:
  - Management activities relating to Privacy Rule compliance
  - Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer
  - Resolution of internal grievances
  - The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, and related due diligence
  - Consistent with the requirements of Section 164.514, creation of de-identified health information or a limited data set, and fundraising for the benefit of the covered entity



# Marketing Restrictions are Deceiving

- Must obtain a written authorization to use or disclose PHI for marketing
  - But “marketing” does not encompass mass communications
  - And is narrowly defined in the Privacy Rule due to four exclusions and two exceptions
- Unless a Medicaid agency is providing PHI to a third party for the marketing of that entity’s products, or providing PHI to a business associate so that it can conduct marketing for the agency, marketing is a “use,” not “disclosure,” issue



# Mass Communications

- Mass communications are not “marketing” under HIPAA; marketing rules apply only to communications targeted to individuals based on knowing their PHI
- Mass communications by definition do not involve use of PHI (since audience is not targeted based on knowledge of recipients’ PHI)
- Authorization is needed to disclose PHI in mass communications
  - Patient “success stories”
  - Patient photos
  - Other disclosures not within an exception under the Privacy Rule



# Marketing Exclusions

- **(Targeted) communications made to an individual:**
  - **To describe a health-related product or service (or payment for such product or service) provided by, or included in a plan of benefits of, the covered entity making the communication**

Informing beneficiaries about the physicians and hospitals participating in a network, changes in benefits, or benefits available under various plan options



# Marketing Exclusions (Con't)

- **(Targeted) communications made to an individual:**
  - To describe a health-related product or service provided by, or included in a plan of benefits of, the covered entity making the communication
  - **For treatment of the individual**

A physician recommends a specific foot care product to a diabetic patient



# Marketing Exclusions (Con't)

- **(Targeted) communications made to an individual:**
  - To describe a health-related product or service provided by, or included in a plan of benefits of, the covered entity making the communication
  - For treatment of the individual
  - **For care coordination or case management** (which includes disease management programs)

A disease management case worker provides a list of smoking cessation programs to a pulmonary patient



# Marketing Exclusions (Con't)

- **(Targeted) communications made to an individual:**
  - To describe a health-related product or service provided by, or included in a plan of benefits of, the covered entity making the communication
  - For treatment of the individual
  - For care coordination or case management
  - **To direct or recommend alternative treatments, therapies, health care providers, or care settings**

A health plan promotes a new weight reduction program for obese patients not having success with their current programs



# So What is HIPAA Marketing?

- To make a communication about a product or service to encourage recipients of the communication to purchase or use the product or service except:
  - A face-to-face communication made by a covered entity to an individual or
  - A promotional gift of nominal value given by the covered entity
- An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, for remuneration, for the other entity or its affiliate to make a communication about its own product or service to encourage its purchase or use



# Discussion Deferred

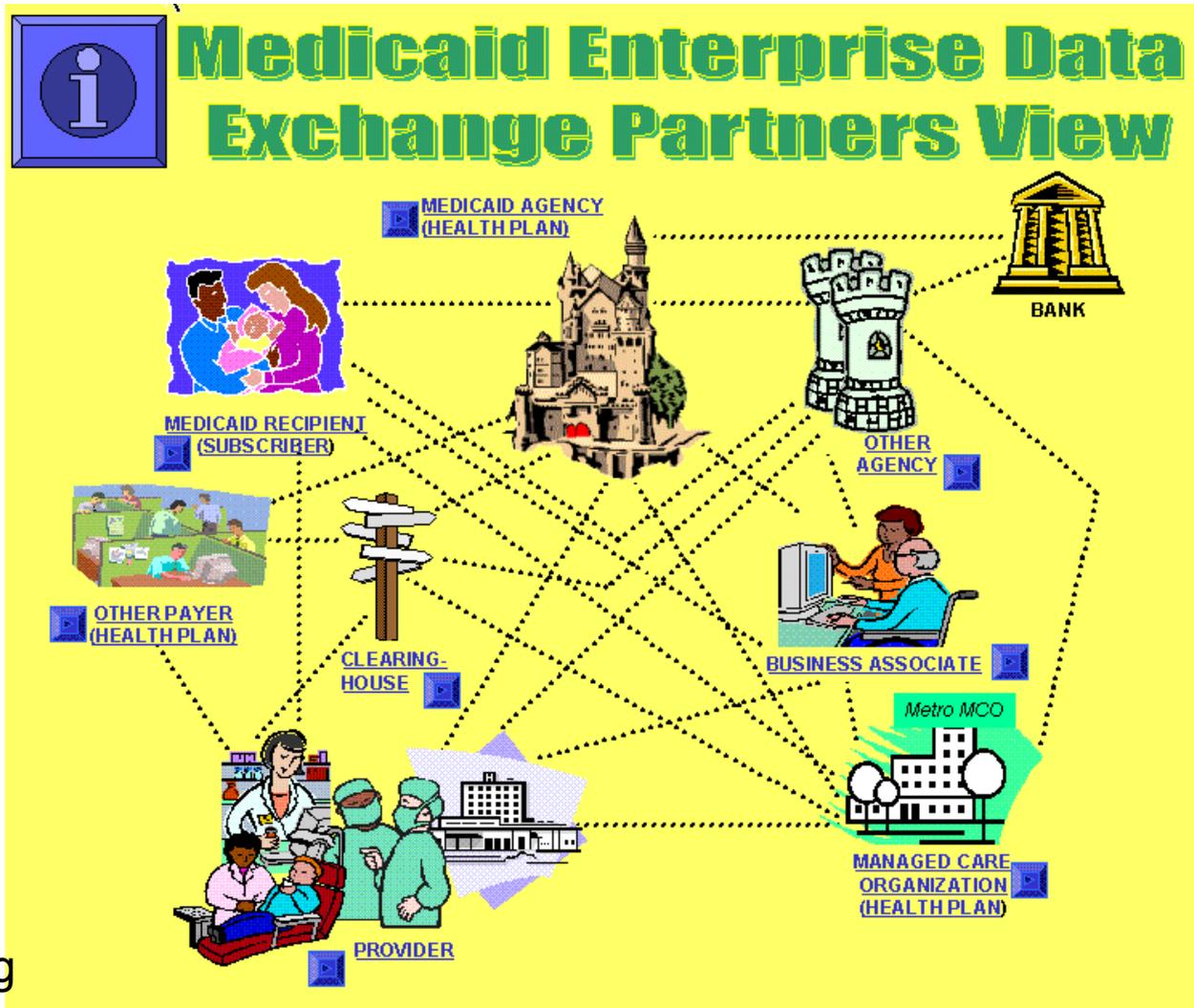
- Under certain conditions, health plans may use PHI:
  - For research
  - In limited data sets
- Both more commonly involve disclosure to a third party, and therefore discussion will be deferred until disclosures are addressed



# Disclosures of PHI by Medicaid Agencies



# A Complex Web of Inter-relationships



[www.mhccm.org](http://www.mhccm.org)



# Accounting of Disclosures

- Individuals are entitled to a written 6-year accounting of disclosures of their PHI by a covered entity (to who, when, what PHI, purpose). Excluded are disclosures:
  - To carry out TPO
  - To individuals of PHI about themselves
  - Incidental to an otherwise permitted or required disclosure
  - Pursuant to an authorization
  - For a facility directory or to persons involved in the individual's care or other notification purposes
  - For national security or intelligence purposes
  - To correctional institutions or law enforcement officials in certain custodial situations
  - As part of a limited data set
  - That occurred prior to the compliance date



# Disclosures to Business Associates

- A business associate is a person or entity that, on behalf of the covered entity--
  - Performs or assists with a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, UR, QA, billing, benefit management, practice management, and repricing, or any function or activity regulated by the Privacy Rule
  - Performs legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation and financial services involving the disclosure of PHI
- By definition, these disclosures are part of TPO (no consent/auth needed; no accounting required)



# Typical Business Associates

- Agents who receive claims and encounters and send remittance advices
- Clearinghouses
- Enrollment contractors
- Prior authorization service companies
- Pharmacy Benefit Management companies
- Fraud and abuse contractors
- Data warehouse contractors
- Shredding services
- Lawyers, accountants and consultants
- Etc., etc., etc.



# Business Associates (con't)

- Business associates do not include:
  - Members of the covered entity's workforce:
    - ✓ Employees
    - ✓ Volunteers
    - ✓ Trainees
    - ✓ Others under the entity's direct control
  - Persons/entities having only incidental contact with PHI:
    - ✓ Cleaning services
    - ✓ Couriers
    - ✓ Etc.



# Business Associates (con't)

- Necessary Provisions in Business Associate (BA) Contracts:
  - Establish the permitted and required uses and disclosures of PHI
  - Preclude use or further disclose of PHI other than as provided by the contract or as required by law
  - Require use of appropriate safeguards to prevent impermissible uses and disclosures
  - Require a report to the covered entity on any improper use or disclosure of PHI
  - Require application of the same restrictions to subcontractors and agents



# Business Associates (con't)

- Required Provisions (Con't):
  - Require BA to make PHI available to individuals when appropriate
  - Require BA to make PHI available for amendment when appropriate
  - Require BA to make accounting of disclosures available
  - Require BA to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of HHS
  - Require BA to return or destroy all PHI at the termination of the contract (if feasible)



# Disclosures to Providers & Other Plans

- Routine disclosures to providers and other health plans will almost invariably be part of TPO (no consent/auth needed; no accounting required)
  - Information exchanges with providers regarding services to be provided, actually provided, and/or billed for
  - Information exchanges with other health plans for purposes of COB and ensuring that Medicaid is payer of last resort



# Disclosures to the Subject of the PHI

- An individual has the right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for:
  - Psychotherapy notes
  - Information compiled in anticipation of a civil, criminal, or administrative action or proceeding
  - Laboratory-related PHI to which access is prohibited by law
- Plan's designated record set: the enrollment, payment, claims adjudication, and case or medical record systems, plus any other records used in whole or part to make decisions about individuals
- Accounting of disclosures is not required



# Disclosures to the Subject of the PHI (con't)

- May require that a request for access be in writing, provided that the individual is informed of such a requirement
- Must act on a request for access no later than 30 days after receipt of the request (60 days if information is not on-site)
- May extend the time period by no more than 30 days, one time only, provided that the individual is timely given a written statement of the reason for the delay and the date by which action on the request will be completed
- If the plan denies the request, in whole or in part, it must provide the individual with a written denial
- If access is denied due to danger of harm, an individual must be given the right to have the denial reviewed by another licensed health care professional, except in very limited situations



# Disclosures to Personal Representatives

- A health plan must treat a personal representative (e.g., parent of minor, executor, guardian) as the individual, with the same rights of access to the individual's PHI, unless it determines, in the exercise of professional judgment, that doing so is not in the best interests of the individual (e.g., domestic violence and abuse situations)
- State law determines when a person qualifies as the personal representative of another
- While a parent is normally the personal representative of an unemancipated minor, that is not the case for PHI when the minor may lawfully obtain the health care service without the consent of the parent or the parent assents to an agreement of confidentiality between the minor and a provider



# Uses/Disclosures Required by Law

- A health plan may use or disclose PHI without consent/auth to the extent that such use or disclosure is required by law and is limited to the relevant requirements of such law.
- If applicable, the requirements of other more specific sections of the Privacy Rule must also be met:
  - Disclosures about victims of abuse, neglect or domestic violence
  - Disclosures for judicial and administrative proceedings
  - Disclosures for law enforcement purposes
- Accounting of disclosures is required



# Disclosures for Public Health Activities

- A health plan may disclose PHI without consent/auth as follows:
  - To a public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability (e.g., reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance and investigations)
  - To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect
  - To a person subject to the jurisdiction of FDA with respect to an FDA-regulated product or activity, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity



# Disclosures for Public Health (con't)

- A health plan may also disclose PHI without consent/auth as follows:
  - To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation
- Accounting of disclosures is required



# Disclosures about Victims of Abuse, etc.

- In addition to disclosures required by law, a health plan may disclose PHI about an individual whom it reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority without consent/auth if:
  - The individual agrees to the disclosure or
  - The disclosure is expressly authorized by statute or regulation and the plan believes the disclosure is necessary to prevent serious harm to the individual or if the individual is unable to agree and the information is required for immediate enforcement activity



# Disclosures about Victims (con't)

- If a health plan makes a disclosure to a government authority about an individual's victim status, it must promptly inform the individual that such a report has been or will be made, except if:
  - Such knowledge would endanger the individual or
  - Such information would be disclosed to a personal representative who is reasonably believed to be responsible for the abuse, neglect, or domestic violence
- Accounting of disclosures is required (presumably subject to above exception)



# Disclosures for Health Oversight

- Without consent/auth, a health plan may disclose PHI to a health oversight agency for oversight activities authorized by law (e.g., audits, investigations, inspections, licensure or disciplinary actions, and other activities needed for oversight of the health care system, government health benefits program, and entities subject to regulatory programs or civil rights laws where health information is necessary for determining compliance)
- Health oversight activities do not include an investigation or other activity in which the individual is the subject of the investigation or activity
- Accounting of disclosures is required, subject to suspension



# Suspension of Accounting of Disclosures

- A health plan must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if the agency or official provides a written statement that an accounting would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required
- If the agency or official statement is made orally, the plan must:
  - Document the statement
  - Temporarily suspend the individual's right to an accounting and
  - Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.



# Disclosure for Judicial/Admin Proceedings

- Without consent/auth, a health plan may disclose PHI in the course of any judicial or administrative proceeding:
  - In response to an order of a court or administrative tribunal, but only to the extent authorized by the order or
  - In response to a subpoena, discovery request, or other lawful process not accompanied by an order if:
    - ✓ It receives satisfactory assurances that reasonable efforts have been made to notify the individual of the request or
    - ✓ It receives satisfactory assurances that reasonable efforts have been made to secure a protective order or stipulation that prohibits the parties from using or disclosing the PHI for any purpose other than the purpose requested and requires that all PHI be destroyed at the end of the litigation or proceeding



# Judicial/Admin Disclosures (con't)

- ✓ If a health plan does not receive satisfactory assurances under one of the two situations set forth above, it may nonetheless make the disclosure if it makes its own reasonable efforts to provide notice to the individual or seeks a qualified protective order
- ✓ Criteria for satisfactory assurances is quite detailed
- Accounting of disclosures is required



# Disclosures for Law Enforcement

- Without consent/auth, a health plan may disclose PHI for a law enforcement purpose to a law enforcement official in the following circumstances:
  - Pursuant to process and as otherwise required by law
  - About victims of crime (not covered in earlier discussions), if the individual agrees, or is incapacitated or in emergency situation and:
    - ✓ The official represents the the PHI is needed to determine whether a crime has occurred, that it won't be used against the victim, and that law enforcement would be materially adversely affected by delay until the individual can agree and
    - ✓ The plan believes that disclosure is in the best interests of the individual



# Disclosures for Law Enforcement (con't)

- For purposes of identifying or locating a suspect, fugitive, material witness or missing person (only limited information—e.g., no DNA or dental records)
- About decedents for the purpose of alerting authorities to a death the plan suspects to have resulted from criminal conduct
- PHI that the plan believes to be evidence of a crime on its premises
- Accounting of disclosures is required, subject to suspension



# Disclosures re: Decedents & for Donations

- A health plan may disclose PHI without consent/auth:
  - To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law
  - To funeral directors, as legal and required to carry out their duties, including disclosing PHI prior to and in reasonable anticipation of the individual's death
  - To organ procurement and similar entities for the purpose of facilitating organ, eye or tissue donation and transplantation
- Accounting of disclosures is required



# Uses & Disclosures for Research Purposes

- If the participants have authorized the research, no accounting is required
- A health plan may use and disclose PHI for research purposes without consent/auth in the following three situations:
  - An alteration to or waiver of, in whole or in part, the Privacy Rule's requirement for authorization has been approved by either an Institutional Review Board (IRB) or comparable privacy board (after finding that the research could not practicably be conducted without the PHI and without the alteration or waiver, and that the use or disclosure of the PHI involves no more than a minimal risk to the privacy of the individuals)



# Research Uses & Disclosures (con't)

- The researcher represents all of the following:
  - ✓ Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research
  - ✓ No PHI is to be removed from the entity
  - ✓ The PHI for which use or access is sought is necessary for the research
- The health plan obtains from the researcher:
  - ✓ Representation that the use or disclosure sought is solely for research on the PHI of decedents
  - ✓ Documentation, at the request of the plan, of the death of such individuals and
  - ✓ Representation that the PHI for which use or disclosure is sought is necessary for the research



# Research Uses & Disclosures (con't)

- Absent authorization, accounting of disclosures is required
- If during the accounting period the plan has made PHI disclosures for a particular research purpose for 50+ individuals, potentially including the subject of the accounting, the plan may provide:
  - The name, and a description of, the protocol or other research activity
  - A description of the type of PHI that was disclosed
  - The period of time during which such disclosures occurred
  - The name, address, and telephone number of the entity that sponsored the research and of the researcher
  - Statement that the subject's PHI may have been disclosed
- If the plan provides such an accounting for research, and if it is reasonably likely that the PHI of the individual was disclosed, the plan must, upon request, assist in contacting the entity that sponsored the research and the researcher



# Limited Data Sets

- A health plan may, without any consents/auths, use or disclose a limited data set for the purposes of research, public health, or health care operations
- A limited data set may not include any of the following direct identifiers of the individual or of relatives, employers, or household members of the individual :
  - Name or street address
  - Telephone, fax or e-mail address
  - SSN or health plan, medical record, account, or certificate/license numbers
  - Vehicle or device identifiers
  - URLs or IP address numbers
  - Biometric identifiers or full face photograph



# Limited Data Sets (con't)

- Examples of data elements that can be included in a limited data set include:
  - Dates of admission and discharge
  - Dates of birth and death
  - Zip code or other geographic subdivision (not including street address)
  - Diagnosis, treatment plan, medical history, and prognosis
- May use or disclose a limited data set only if a data use agreement (akin to business associate agreement) restricts the use and disclosure of the PHI
- Accounting of disclosures is not required



# Averting Threats to Health & Safety

- A health plan may disclose PHI without consent/auth when it believes in good faith that the disclosure:
  - Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or public and is to a person or persons reasonably able to prevent or lessen the threat or
  - Is necessary for law enforcement authorities to identify or apprehend an individual who has admitted participation in a violent crime that the plan believes to have caused serious physical harm to the victim or who appears to have escaped from a correctional institution or lawful custody
- Accounting of disclosures is required



# National Security and Intelligence

- A health plan may disclose PHI to authorized federal officials without consent/auth:
  - For the conduct of lawful intelligence, counter-intelligence and other national security activities
  - For the provision of protective services to the President, foreign heads of state and other dignitaries, and for the conduct of related investigations
- Accounting of disclosures is not required



# Special Rules for Government Programs

- Without consent/auth, a health plan that is a government program providing public benefits may disclose to another agency administering a similar program:
  - PHI relating to eligibility or enrollment, if such sharing of information or the maintenance of such information in a database accessible to all such agencies is required or authorized by statute or regulation
  - PHI relating to the program if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the programs or improve the administration and management of the programs
- Accounting of disclosures is required



# Disclosures for Worker's Compensation

- Without consent/auth, a health plan may disclose PHI as authorized by, and to the extent necessary to comply with, laws relating to worker's compensation or other similar programs
- Accounting of disclosures is required



# Opportunity to Agree or Object

- Provided that the individual agrees, or does not express an objection when given the opportunity, a health plan may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care
- Accounting of disclosures is not required



# Opportunity to Agree or Object (con't)

- A health plan may use or disclose PHI to notify, or assist in notifying, a family member, personal representative, or another person involved in the individual's care, of the individual's location, general condition or death if:
  - The individual agrees, or does not express an objection when given the opportunity
  - The individual is not present or an opportunity to agree/object cannot practicably be provided (emergency, incapacity) if plan determines, in exercise of professional judgment, that doing so is in the individual's best interests
  - Includes disclosures to entities authorized to assist in disaster relief efforts
- Accounting of disclosures is not required





**CGI**

**25**  
YEARS  
OF COMMITMENT

# Questions and Discussion



# Contact Information

**Michael J. Mahoney**

**Director of Regulatory Affairs and Counsel**

**CGI Information Systems & Management  
Consultants, Inc.**

**1301 East 9<sup>th</sup> Street, Suite 3000**

**Cleveland, OH 44114-1800**

**Office: 216-416-6413**

**Fax: 216-687-1488**

**[michael.mahoney@cgi.com](mailto:michael.mahoney@cgi.com)**

