

“Secondary” Use of Health Information

1

*Developing a Strategy for Long Term
HIE Financial Sustainability*

Kristen B. Rosati
Coppersmith Schermer & Brockelman, PLC

New Jersey Health Information Technology Commission

March 29, 2011

Agenda



- Potential use cases for secondary use of health information
 - Research
 - Quality improvement activities
 - Accountable Care Organizations
 - Public health
 - Commercial use of indentified information
- For each use case, discuss:
 - The opportunities and benefits
 - Applicable laws
 - Risks and ways of mitigating risks
- Next steps

**THE POTENTIAL OF HIES AS
INFOMEDIARIES**

**JOURNAL OF HEALTHCARE INFORMATION MANAGEMENT,
VOL. 21, NO. 1 (WINTER 2007)**

**HEALTH INFORMATION EXCHANGE:
FROM START UP TO SUSTAINABILITY
EHEALTH INITIATIVE REPORT TO HRSA(MAY 27, 2007)**

New Paradigm for 21st Century Biomedicine Leads to:



Quality

- **Quality care is delivered through ready access to care guidelines and practice plans accessible through decision support systems**



Comparative
Effectiveness

- **Knowledge bases support ongoing assessment of effective interventions informed by individual characteristics including molecular information**



Pharmaco-
Vigilance

- **Access to electronic health information at point of care permits ongoing assessment of safety of approved interventions in real world settings**



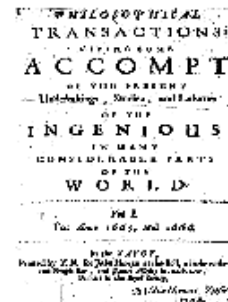
Biomedical
Research

- **Biomedical research effectively leverages health observations and rapidly feeds back approved interventions into a care setting**

Information and Community Fragmentation Blocks this Paradigm

- **Isolated information “islands”**
- **Information dissemination uses models recognizable to Gutenberg and pioneered by London Academy of Science**
 - Write manuscripts
 - “Publish”
 - Exchange information at meetings

17th Century



Royal Society of London

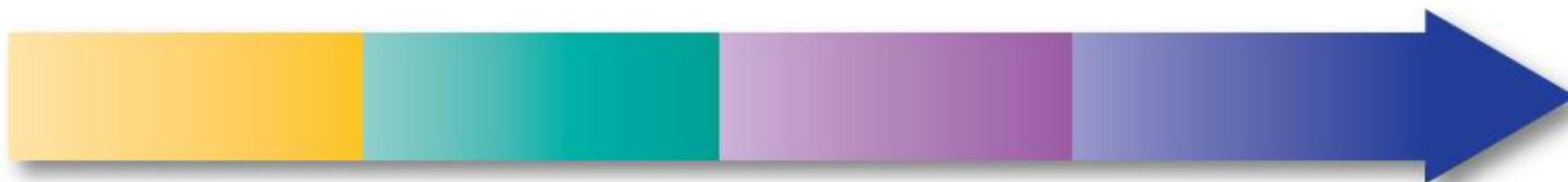
- Oldest learned society (1660)
- Oldest scientific journal (1665)

21st Century



We Still Operate in the 20th Century

Research > Care Paradigm



Discovery

- Biological pathways
- Target identification and validation

Product Development

- Candidate selection and Optimization
- Pre-clinical testing
- Phase I, II, III
- New Drug application and Approval

Clinical Care

- Product launch
- Clinical adoption

Outcomes & Surveillance

- Reporting of serious/fatal ADRs
- Re-labeling (or recall) as needed
- Additional indications as warranted

We Still Operate in the 20th Century

Research > Care Paradigm

Current paradigm is linear, sequential, slow, cost-ineffective, and minimally productive. It does not capture value of clinical data, or leverage knowledge for discovery or clinical impact in a timely way.



Discovery

Issues:

It's difficult to:

- Access clinical outcomes data on relevant populations
- Access biospecimens of high quality with clinical data
- Validate *in silico*

Product Development

Issues:

- Linear, sequential process
- Information is trapped in silos
- Each trial demands re-creation of infrastructure
- No economies of scale
- Failed candidates hard to resuscitate

Clinical Care

Issues:

- Launches and product detailing are costly
- Adoption can be slow
- Traditional physician outreach methods now constrained
- Process is slow and uni-directional

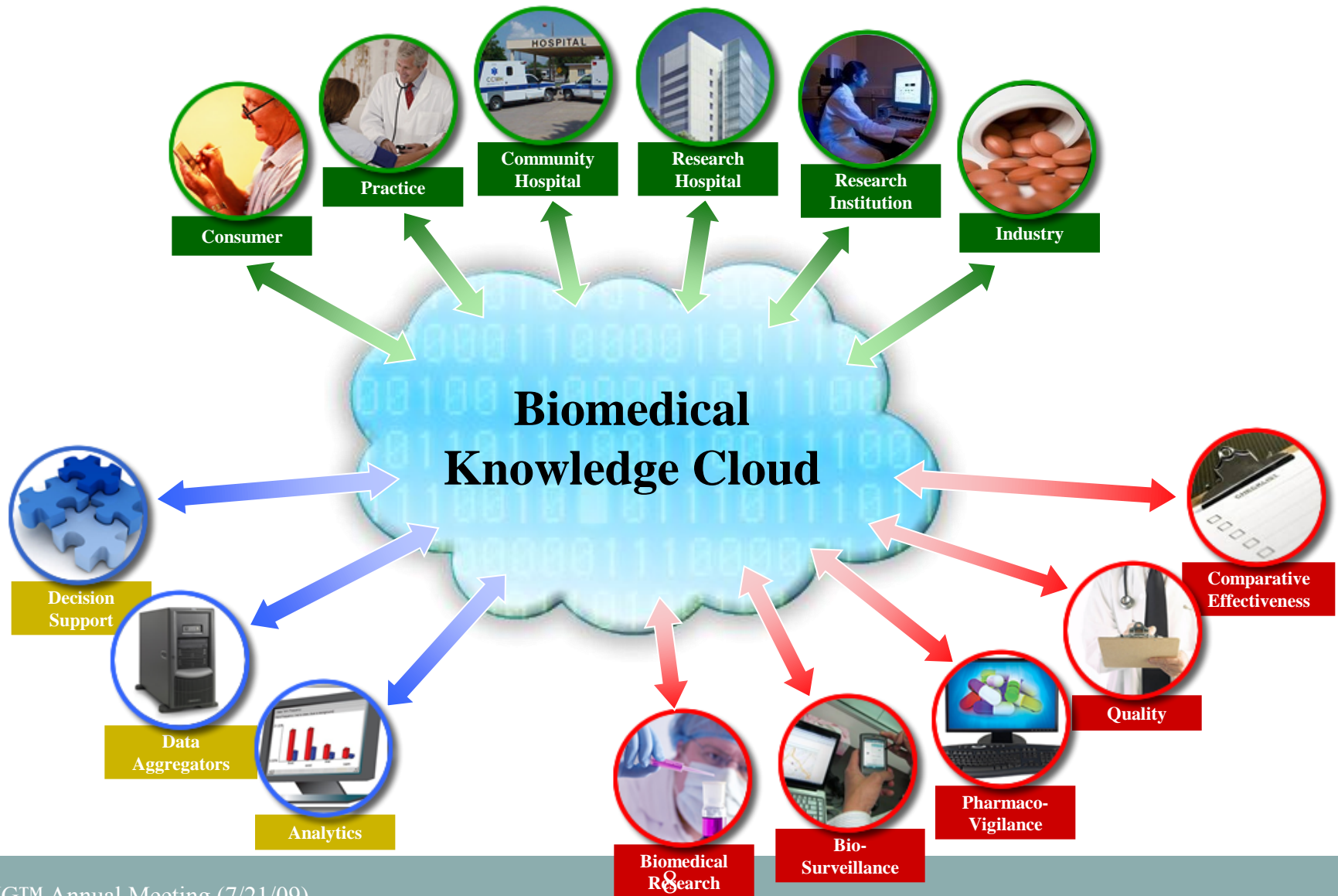
Outcomes & Surveillance

Issues:

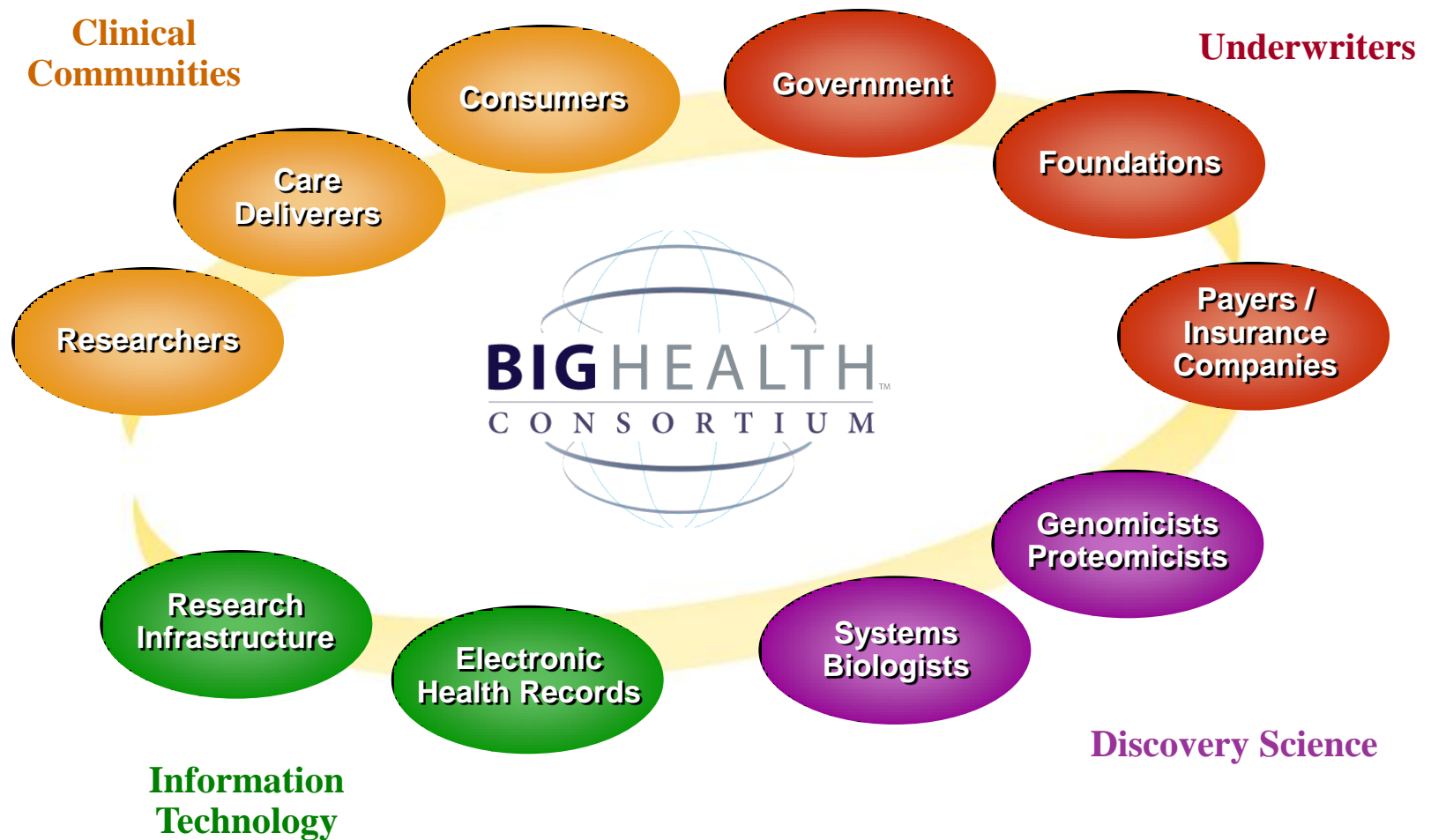
- Ph IV not conducted uniformly or consistently
- Efficacy and ADR patterns are recognized very slowly
- New indications are gained painstakingly from regulators
- Recalls are financially disastrous

Information on clinical experience with products is not captured systematically. Observations are “locked away” or ignored, and little new knowledge is gained or leveraged.

A “Knowledge” Cloud Enables Data Integration to Serve Multiple Purposes



The Knowledge Cloud enables a 21st century biomedical “ecosystem”



Research Opportunities



- Research with the health information itself
 - Health services research
 - ✦ *Example: The High Value Health Care Collaboration with the Mayo Clinic, the Cleveland Clinic, Intermountain Healthcare, Geisinger, Denver Health, Dartmouth-Hitchcock, and the Dartmouth Institute for Health Policy and Clinical Practice*
 - ✦ *Example: The Dartmouth Atlas*
 - ✦ *Example: Regenstrief Institute (Indiana Health Information Exchange)*
 - ✦ *Example: Explorys, Inc.*
 - Epidemiology research
 - ✦ *Example: Arizona HealthQuery*

Research Opportunities



- Research with the health information itself cont...
 - Provision of clinical data for biobanking activities
 - ✦ *Future example: Arizona Biospecimen Consortium*
 - ✦ *Good resource for information: Faster Cures*
- Research support services
 - Identification of cohorts for clinical trials organized by region, community, or provider
 - ✦ *Example: Recombinant Data, Inc.*
 - Creation of patient registries: patient-provided data for research and notification of patients of relevant clinical trials
 - ✦ *Example: EmergeMD and its “Communities for Care” platform*

Laws Related to Use of Health Information for Research



- HIPAA
 - Applies to HIPAA covered entities (and soon to their business associates)
- The Common Rule (HHS rules regarding human subject research)
 - Applies to federally-funded research and research conducted by institutions that have a broad “Federalwide Assurance” in place
- Federal substance abuse treatment regulations
 - Applies to federally-supported substance abuse treatment programs and to some recipients of information from those programs
- State law
 - Application varies

HIPAA Privacy Rule and Research



- The HIPAA Privacy Rule applies when a “covered entity” internally accesses or externally discloses protected health information (PHI) (see 45 CFR Part 164, Subpart E)
- The HITECH Act applies HIPAA to business associates (which will be enforceable six months after the effective date of the final rule amending HIPAA)
 - Proposed HHS Office for Civil Rights (OCR) rule published on July 14 (see 75 Fed. Reg. 40868)
- HIPAA basics: only one rule must be satisfied for use or disclosure of PHI for research

HIPAA Privacy Rule and Research



- The research involves only de-identified data
- The research uses or discloses a “Limited Data Set” and the recipient signs a “Data Use Agreement”
- The research subject has signed an authorization
- An Institutional Review Board (IRB) has waived the requirement for authorization
- The activities are just to prepare for research
- The use or disclosure is for patient recruitment purposes
- The research involves only the information of decedents
- The disclosure of the PHI is required by law
- The research is “grandfathered” under the HIPAA rules

HIPAA Option 1: De-Identify Data



- Remove or code the “identifiers” (if code is not derived from identifiers), including:
 - Name;
 - Geographic location information (unless only the first three digits of the zip code are used and the area has more than 20,000 residents);
 - Dates (except year) directly related to an individual, such as birth date, admission date, discharge date, dates of service, or date of death;
 - Age if over 89 (unless aggregated into a single category of age 90 and older);
 - Numbers related to the patient (SSN, etc.);
 - Biometric identifiers, such as fingerprints
 - Full-face photographs and any comparable images; or
 - Any other unique identifying number, characteristic, or code

HIPAA Option 1: De-Identify Data



- Get a certification from a qualified statistician that there is a “very small” likelihood of determining identity
- Comparison with Common Rule:
 - Information is considered “de-identified” if investigator cannot reasonably determine identity
 - Additional rules for coding:
 - ✦ Destroy key to code before research begins
 - ✦ Investigators and holder of key enter into agreement prohibiting release of key to investigators until individuals are deceased
 - ✦ Have IRB approve written policies and procedures for a repository or data management center that prohibit the release of the key to investigators until individuals are deceased or
 - ✦ Determine that other legal requirements exist that prohibit release of key to investigators

HIPAA Option 2: Use a Limited Data Set



- Partially de-identified PHI: remove all identifiers except dates related to individual and geographic designations (above street level)
- Must have “Data Use Agreement” in place with recipient
- Comparison with Common Rule: a Limited Data Set likely will not be “identifiable” under the Common Rule (i.e., investigator likely will not be able to readily ascertain the identity of the subjects)

HIPAA Option 3: Subject Authorization



- Numerous requirements for authorization forms
- Challenges for seeking authorization in advance:
 - (1) HIPAA authorization may not seek permission to use or disclose PHI for future unspecified research—authorization must be protocol specific or must be for storage in a research repository only
 - (2) Cannot combine HIPAA authorization with informed consent, if informed consent seeks permission to use the PHI for future unspecified research (“compound” authorization)
- In its proposed rule, OCR seeks public comment on changing these requirements

HIPAA Option 4: IRB Waiver of Authorization



- Use or disclosure of PHI involves no more than minimal risk to individuals' privacy, based on:
 - An adequate plan to protect PHI from improper use and disclosure;
 - An adequate plan to destroy PHI at the earliest opportunity consistent with conduct of the research (unless there is a health or research justification for retention or if retention is required by law);
 - Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the study, or for other research permitted by the rules; and...

HIPAA Option 4: IRB Waiver of Authorization



- The research could not practicably be conducted without the waiver or alteration of authorization; and
- The research could not practicably be conducted without access to and use of information identifying the subjects
- Partial waiver option
 - Example: IRB waiver of authorization (and informed consent) to create a research registry and to use the registry to identify potential clinical trial participants; IRB approval to contact potential participants for a particular clinical trial; authorization (and informed consent) to participate in clinical trial

HIPAA Option 5: Activities to Prepare for Research



- Representations from researcher that will use of PHI solely to prepare for research, the PHI is necessary for research, and the PHI will not be removed from premises
What activities are to prepare for research?
 - Developing protocol, identifying research cohorts, identifying potential participants...What constitutes removal from premises?
 - Remote access okay if no printing, copying, saving or electronically faxing
- Comparison with the Common Rule: Access to identifiable patient information is “human subject research” that requires IRB review and waiver of informed consent

HIPAA Option 6: Subject Recruitment



- Covered entity may use own PHI to recruit patients under HIPAA rules for “treatment” or “health care operations”
- Third party may use PHI to recruit patients if has a business associate agreement in place with the covered entity
- Comparison with the Common Rule: Access to identifiable patient information is “human subject research” that requires IRB review and waiver of informed consent

Creating a Clinical Data Warehouse



- Providing PHI to populate a clinical data warehouse (CDW) is itself a health care operation, if the CDW will be used for health care operations activities (such as quality assurance)
- Providing PHI to populate a CDW to be used for research, is itself research and should follow one of the HIPAA rules regulating use or disclosure of PHI for research
 - If existing CDW (created for health care operations) will be used for research purposes, should comply with HIPAA research rules before convert use of CDW to research

Creating a Clinical Data Warehouse



- Creating a CDW with integrated, aggregated data from multiple covered entities is permitted by HIPAA
 - HIPAA doesn't regulate how PHI is stored (except for requiring a business associate agreement and HIPAA Security Rule compliance)
 - HIPAA regulates who has access to PHI and for what purpose
- Business associate agreement required with holder of CDW
- Minimum necessary standard
- Patient Protection and Affordable Care Act (PPACA) will encourage greater data integration and collaboration

HIPAA Privacy Rule Challenges Ahead



- Current rule: Covered entity may receive payment for a disclosure of PHI where that disclosure is permitted by the regulations (such as for health care operations or research)
- HITECH (sec. 13405(d)) prohibits indirect or direct receipt of remuneration in exchange for a disclosure of PHI without the individual's authorization (with exceptions)
- OCR proposed amendments to HIPAA Privacy Rule would prohibit indirect or direct remuneration in exchange for a disclosure of PHI without authorization (with exceptions on the next slide) -- will this include non-financial remuneration?

HIPAA Privacy Rule Challenges Ahead



- **Exceptions:**
 - For public health purposes
 - For research, “where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit” the PHI
 - For treatment and payment
 - For the sale, transfer, merger or consolidation of the covered entity and related due diligence
 - To or by a business associate to perform activities for the covered entity, where “the only remuneration provided is by the covered entity to the business associate for the performance of such activities”
 - To an individual for access or accounting
 - Where required by law to disclose PHI
 - Where the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI, or a fee is otherwise expressly permitted by another law

HIPAA Privacy Rule Challenges Ahead

- HITECH Act requires HHS to issue guidance on methods for de-identification of PHI
- OCR solicited stakeholder input from experts with practical technical and policy experience to inform the creation of guidance materials, and collected views regarding de-identification approaches, best practices for implementation and management of the current de-identification standard and potential changes to address policy concerns
- March 2010 2-day conference on de-identification – see http://www.hhs.gov/ocr/privacy/hipaa/understanding/covered_entities/De-identification/deidentificationworkshop2010.html

HIPAA Security Rule

28

- Requires HIPAA covered entities (and soon business associates) to comply with rules to establish administrative, physical and technical safeguards (see 45 CFR Part 164, Subpart C)
 - No special requirements imposed on security for research

HIPAA Breach Reporting Rule

- Any CE (or BA) that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses” unsecured PHI must notify individuals whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed as a result of a breach
- “Unsecured” PHI is not secured per HHS guidance (which will be issued annually)– most recent guidance is in HHS August 24, 2009 guidance (at 74 Fed. Reg. 42740): “secured” PHI is encrypted per NIST guidelines or destroyed
 - Applies to electronic and paper PHI
 - Works as “safe harbor” to reporting requirement

HIPAA Breach Reporting Rule

30

- HHS regulations for breach notification: 45 CFR Part 164, Subpart D (published at 74 Fed Reg. 42740 (Aug. 24, 2009))— enforceable on Sept. 23 (but HHS will exercise “enforcement discretion” until Feb. 22, 2010)
- Applies to CEs and BAs
- Breach: the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI (i.e. which poses a significant risk of financial, reputational, or other harm to an individual)
- Exceptions....

HIPAA Breach Reporting Rule

- Exceptions....
 - Not a breach if the information does not include direct identifiers, date of birth, or zip code
 - ✦ So, if you disclose a Limited Data Set for research (which may include dates related to a patient, and address information above the street level or PO Box), the unauthorized use or disclosure of the Limited Data Set is not reportable only if it does not include date of birth or zip code
 - ✦ Rationale: Date of birth or zip code makes it possible to re-identify an individual when information is paired with publicly available data

HIPAA Breach Reporting Rule

32

- Exceptions continued:
 - Unintentional use of PHI by a workforce member or a person acting under the authority of the CE or BA, if it was in good faith, within scope of authority, and does not result in further use or disclosure that violates HIPAA
 - Inadvertent disclosure to another at the CE or BA (or within an organized health care arrangement), if the recipient is authorized to see PHI and does not result in further use or disclosure that violates HIPAA
 - Good faith belief that recipient would not reasonably have been able to retain the PHI

HIPAA Breach Reporting Rule

33

- CEs must notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired, or disclosed as a result of a breach
- BAs must notify the CE, not the individuals; BA notice must contain information about individuals affected
- Method of notice
 - Individual notice by first class mail (or email if individual agrees)
 - Alternative method if insufficient contact information (if for more than 10 individuals, then website posting or media notice)
 - Notice to “prominent media outlets” if more than 500 residents of the state or jurisdiction are affected
 - Concurrent notice to HHS if more than 500 residents are affected; an annual report to HHS including every breach

HIPAA Breach Reporting Rule

34

- Timing of notice
 - Without unreasonable delay and in no case later than 60 days of discovery of breach by CE or business associate
 - CE learns of breach when it is known to any employee, officer or other agent, other than the person who committed the breach
 - Can delay with law enforcement request that notice will impede a criminal investigation or cause damage to national security

HIPAA Breach Reporting Rule

35

- Content of notice
 - “A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
 - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
 - The steps individuals should take to protect themselves from potential harm resulting from the breach.
 - A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
 - Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.”

The Common Rule



- The Common Rule applies to federally-funded human subject research and if an institution voluntarily extends the scope of its Federalwide Assurance to all human subject research, regardless of source of funding

4. Applicability

(a) This Institution assures that whenever it engages in human subjects research conducted or supported by any federal department or agency that has adopted the ... Common Rule....

(b) Optional: This Institution elects to apply the following to all of its human subjects research regardless of the source of support, except for research that is covered by a separate assurance:

The Common Rule (see section 3 of the Terms of the FWA for Institutions Within the United States for a list of departments and agencies that have adopted the Common Rule and the applicable citations to the Code of Federal Regulations)

The Common Rule and subparts B, C, and D of the HHS regulations at 45 CFR part 46”

The Common Rule



- The Common Rule requires IRB review of “human subject” research (see 45 C.F.R. 46.102)

Research: “a systematic investigation...designed to develop or contribute to generalizable knowledge”

Human subject research: (1) interaction with the individual, or (2) identifiable private information”

Private information: information provided for specific purposes by an individual, which the individual can reasonably expect will not be made public

Identifiable: an individual’s identity is or may be readily ascertained by the investigator

The Common Rule



- When is research exempt from IRB review (see 45 CFR 46.101(b)(4))
 - Collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens; and
 - If these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects
 - Information may not be coded

Who Must Obtain IRB Approval?



- Is the data provider “engaged” in research?
 - Institution is “engaged” in human subjects research if its employees or agents:
 - Obtain for research purposes identifiable private information from any source (even if there is no interaction with the participants)
- Institution is not “engaged” in human subjects research if its employees or agents:
 - Release identifiable private information or identifiable specimens to investigators at another institution
 - Obtain coded information, but have no access to the key

Which IRB Can Review?



- HIPAA permits a covered entity to rely on an “outside” IRB’s waiver of HIPAA authorization; this permits alternative IRB arrangements such as “lead” IRBs or collaborative IRBs
- Reviewing IRB should provide documentation to all covered entities that meets the HIPAA requirements for waiver of authorization
- If the Common Rule applies, it also permits reliance on an outside IRB, if the parties have an IRB authorization agreement in place and the relying institution lists the reviewing IRB on its Federalwide Assurance

Informed Consent



- 45 C.F.R. 46.116(a)(1) requires:
 - Explanation of the purposes of the research
 - Description of the procedures
 - Description of any reasonably foreseeable risks
- OHRP Guidance on “Research Use of Stored Data or Tissues” (1997)
(<http://www.hhs.gov/ohrp/humansubjects/guidance/repository.htm>) requires clear description of:
 - Operation of repository;
 - Specific types of research to be conducted;
 - Conditions under which data will be released to recipient-investigators; and
 - Procedures for protecting privacy of subjects and confidentiality of data

Waiver of Informed Consent



- IRB must determine that:
 - (1) The research involves no more than minimal risk to the patients
 - (2) Waiving informed consent will not adversely affect the rights and welfare of the individuals
 - (3) That the research could not practicably be carried out without the waiver
 - (4) That the researcher will provide additional pertinent information to individuals after participation in the research

Certificates of Confidentiality



- Certificates of Confidentiality available from NIH for “sensitive” research information where disclosure of identifying information could damage subjects’ financial standing, employability, insurability or reputation
- Research collecting information related to genetics, psychological well being, sexual behavior, drug use, criminal activities
- Research where subjects may be involved in litigation related to exposures under study

The “Part 2” Regulations



- 42 CFR Part 2 governs information obtained from a federally-funded substance abuse treatment program, which information identifies an individual as a substance abuser
 - Federally-funded = Medicare or Medicaid participation, or tax-exempt status
 - Program = Holding self (or entity) out to the public as providing substance abuse treatment

The “Part 2” Regulations



- Part 2 permits use of patient identifying information for research if:
 - Informed consent; or
 - Part 2 program director approval (42 CFR § 2.52)
 - ✦ Recipient qualified to conduct the research
 - ✦ Recipient has a research protocol under which the patient identifying information:
 - Will be maintained in accordance with the security requirements of §2.16 of these regulations (or more stringent requirements); and
 - Will not be redisclosed except as permitted; and ...

The “Part 2” Regulations



- Recipient has provided a satisfactory written statement that a group of three or more individuals who are independent of the research project has reviewed the protocol and determined that:
 - ✦ The rights and welfare of patients will be adequately protected; and
 - ✦ The risks in disclosing patient identifying information are outweighed by the potential benefits of the research

- A person conducting research may disclose patient identifying information only back to the program from which that information was obtained and may not identify any individual patient in any report of that research or otherwise disclose patient identities

Risks of Using Health Information for Research



- HIPAA civil and criminal penalties for noncompliance
 - Applies criminal penalties to individuals who without authorization obtain or disclose individually identifiable health information that is maintained by a covered entity (enforceable on 2/18/10)
 - Increases amount of civil penalties from \$100 per violation and a total of \$25,000 per year, to a tiered penalty system that can go to \$50,000 per violation and total penalties of up to \$1,500,000 per year
 - Gives State Attorneys General authority to bring civil action to enjoin a violation, seek statutory damages for individuals and obtain attorneys fees

Risks of Using Health Information for Research



- HHS Office for Human Research Protections (OHRP) enforces the Common Rule
 - No civil penalty enforcement authority
 - Can prevent entity from conducting federally-funded research in the future

Risks of Using Health Information for Research



- HHS Substance Abuse and Mental Health Services Administration (SAMHSA)
 - Criminal penalty: any person who violates the statute or these regulations shall be fined not more than \$500 in the case of a first offense, and not more than \$5,000 in the case of each subsequent offense

Risks of Using Health Information for Research



- HIE contractual compliance (including with the business associate terms in the participation agreements)
 - Each HIE should evaluate their contractual flexibility in using health information for research

Risks of Using Health Information for Research



- Public opinion: Reactions of consumers and legislators

Mitigating Risks



- HIE contract terms that will permit activity, under defined terms and conditions
- Collaborative development of HIE policies to reflect all legal compliance obligations
- Public/ consumer outreach related to use case
- Legislative outreach and development of champions for use case
- Adequate insurance coverage

Quality Improvement Opportunities



- Aggregated data for quality benchmarking
- Reports to specific institutions/physicians using institution's health information
- Multi-institutional quality projects with HIE at the “hub”
 - ✦ *Example: Explorys, Inc.*
 - ✦ *Example: Arizona HealthQuery*

Laws Related to Use of Health Information for Quality Improvement



- **HIPAA**
 - Applies to HIPAA covered entities (and soon to their business associates)
- **Federal substance abuse treatment regulations**
 - Applies to federally-supported substance abuse treatment programs and to some recipients of information from those programs
- **State law**
 - Application varies

HIPAA Privacy Rule and Quality Improvement: Option 1



- PHI can be used or disclosed for the covered entity's treatment, payment, or health care operations (“TPO”) without individual authorization
 - 45 C.F.R. § 164.506(c)(1) (permitting disclosure of PHI for a covered entity's health care operations)
 - 45 C.F.R. § 164.501 (defining health care operations as including quality assurance and improvement activities)
- Participants should have access only to their own PHI– any reports generated for QA and PI should contain only own PHI compared against aggregated views of other participants' PHI
 - HIPAA permits access to other participants' PHI for QA and PI only for shared patients (and for time period during relevant relationship)

HIPAA Option 2: De-Identify Data



- Remove or code the “identifiers” (if code is not derived from identifiers)
- Get a certification from a qualified statistician that there is a “very small” likelihood of determining identity

HIPAA Option 3: Use a Limited Data Set



- Partially de-identified PHI: remove all identifiers except dates related to individual and geographic designations (above street level)
- Must have “Data Use Agreement” in place with recipient

HIPAA Option 4: Authorization



- Numerous requirements for authorization forms

HIPAA Privacy Rule Challenges Ahead



- Current rule: Covered entity may receive payment for a disclosure of PHI where that disclosure is permitted by the regulations (such as for health care operations or research)
- HITECH (sec. 13405(d)) prohibits indirect or direct receipt of remuneration in exchange for a disclosure of PHI without the individual's authorization (with exceptions)
- OCR proposed amendments to HIPAA Privacy Rule would prohibit indirect or direct remuneration in exchange for a disclosure of PHI without authorization (with exceptions on the next slide) -- will this include non-financial remuneration?

HIPAA Privacy Rule Challenges Ahead



- Exceptions:
 - For public health purposes
 - For research, “where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit” the PHI
 - For treatment and payment
 - For the sale, transfer, merger or consolidation of the covered entity and related due diligence
 - To or by a business associate to perform activities for the covered entity, where “the only remuneration provided is by the covered entity to the business associate for the performance of such activities”
 - To an individual for access or accounting
 - Where required by law to disclose PHI
 - Where the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI, or a fee is otherwise expressly permitted by another law

HIPAA Security Rule

61

- Requires HIPAA covered entities (and soon business associates) to comply with rules to establish administrative, physical and technical safeguards (see 45 CFR Part 164, Subpart C)

HIPAA Breach Reporting Rule

62

- Requires covered entity (or business associate) that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses” unsecured PHI must notify individuals whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed as a result of a breach

The “Part 2” Regulations



- 42 CFR Part 2 governs information obtained from a federally-funded substance abuse treatment program, which information identifies an individual as a substance abuser
 - Federally-funded = Medicare or Medicaid participation, or tax-exempt status
 - Program = Holding self (or entity) out to the public as providing substance abuse treatment

The “Part 2” Regulations



- Part 2 permits disclosure of patient identifying information for quality improvement activities:
 - With patient consent; or
 - To a “Qualified Service Organization”:
 - ✦ (a) Provides services to a program, and
 - ✦ (b) Has entered into a written agreement that:
 - (1) Acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from the program, it is fully bound by these regulations; and
 - (2) If necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the Part 2 regulations

Risks of Using Health Information for QI



- HIPAA civil and criminal penalties for noncompliance
 - Applies criminal penalties to individuals who without authorization obtain or disclose individually identifiable health information that is maintained by a covered entity (enforceable on 2/18/10)
 - Increases amount of civil penalties from \$100 per violation and a total of \$25,000 per year, to a tiered penalty system that can go to \$50,000 per violation and total penalties of up to \$1,500,000 per year
 - Gives State Attorneys General authority to bring civil action to enjoin a violation, seek statutory damages for individuals and obtain attorneys fees

Risks of Using Health Information for QI



- HHS Substance Abuse and Mental Health Services Administration (SAMHSA)
 - Criminal penalty: any person who violates the statute or these regulations shall be fined not more than \$500 in the case of a first offense, and not more than \$5,000 in the case of each subsequent offense

Risks of Using Health Information for QI



- HIE contractual compliance (including with the business associate terms in the participation agreements)
 - Each HIE should evaluate their contractual flexibility in using health information for quality improvement activities

Risks of Using Health Information for QI



- Public opinion: Reactions of consumers and legislators

Mitigating Risks



- HIE contract terms that will permit activity, under defined terms and conditions
 - Include QSO contract language to comply with the Part 2 regulations
- Collaborative development of HIE policies to reflect all legal compliance obligations
- Public/ consumer outreach related to use case
- Legislative outreach and development of champions for use case
- Adequate insurance coverage

Accountable Care Organization Opportunities



- HIEs as the “hub”
- See Premier-IBM integrated IT platform for all Premier members’ development of ACOs, at <http://healthsystemcio.com/2011/02/18/premier-releases-aco-roadmap/>

Laws Related to Use of Health Information for ACOs



- **HIPAA**
 - Applies to HIPAA covered entities (and soon to their business associates)
- **Federal substance abuse treatment regulations**
 - Applies to federally-supported substance abuse treatment programs and to some recipients of information from those programs
- **State law**
 - Application varies

HIPAA Privacy Rule and ACOs: Option 1 – TPO



- PHI can be used or disclosed for the covered entity's treatment, payment, or health care operations (“TPO”) without individual authorization
 - 45 C.F.R. § 164.506(c)(1) (permitting disclosure of PHI for a covered entity's health care operations)
 - 45 C.F.R. § 164.501 (defining health care operations as including quality assurance and improvement activities)
- No restrictions on disclosures for treatment
- No restrictions on disclosures for payment (except minimum necessary standard)

HIPAA Privacy Rule and ACOs: Option 1 -- TPO



- Restriction if disclosure is for health care operations: participants should have access only to their own PHI as compared against aggregated views of other participants' PHI
 - HIPAA permits access to other participants' PHI for health care operations only if shared patients (and for time period during relevant relationship)

HIPAA Option 2: De-Identify Data



- Remove or code the “identifiers” (if code is not derived from identifiers)
- Get a certification from a qualified statistician that there is a “very small” likelihood of determining identity

HIPAA Option 3: Use a Limited Data Set



- Partially de-identified PHI: remove all identifiers except dates related to individual and geographic designations (above street level)
- Must have “Data Use Agreement” in place with recipient

HIPAA Option 4: Authorization



- Numerous requirements for authorization forms

HIPAA Privacy Rule Challenges Ahead



- Current rule: Covered entity may receive payment for a disclosure of PHI where that disclosure is permitted by the regulations (such as for health care operations or research)
- HITECH (sec. 13405(d)) prohibits indirect or direct receipt of remuneration in exchange for a disclosure of PHI without the individual's authorization (with exceptions)
- OCR proposed amendments to HIPAA Privacy Rule would prohibit indirect or direct remuneration in exchange for a disclosure of PHI without authorization (with exceptions on the next slide) -- will this include non-financial remuneration?

HIPAA Privacy Rule Challenges Ahead



- **Exceptions:**
 - For public health purposes
 - For research, “where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit” the PHI
 - For treatment and payment
 - For the sale, transfer, merger or consolidation of the covered entity and related due diligence
 - To or by a business associate to perform activities for the covered entity, where “the only remuneration provided is by the covered entity to the business associate for the performance of such activities”
 - To an individual for access or accounting
 - Where required by law to disclose PHI
 - Where the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI, or a fee is otherwise expressly permitted by another law

HIPAA Security Rule

79

- Requires HIPAA covered entities (and soon business associates) to comply with rules to establish administrative, physical and technical safeguards (see 45 CFR Part 164, Subpart C)

HIPAA Breach Reporting Rule

80


- Requires covered entity (or business associate) that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses” unsecured PHI must notify individuals whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed as a result of a breach

The “Part 2” Regulations



- 42 CFR Part 2 governs information obtained from a federally-funded substance abuse treatment program, which information identifies an individual as a substance abuser
 - Federally-funded = Medicare or Medicaid participation, or tax-exempt status
 - Program = Holding self (or entity) out to the public as providing substance abuse treatment

The “Part 2” Regulations



- Part 2 permits disclosure of patient identifying information for quality improvement activities:
 - With patient consent; or
 - To a “Qualified Service Organization”:
 - ✦ (a) Provides services to a program, and
 - ✦ (b) Has entered into a written agreement that:
 - (1) Acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from the program, it is fully bound by these regulations; and
 - (2) If necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the Part 2 regulations

Risks of Using Health Information for ACOs



- HIPAA civil and criminal penalties for noncompliance
 - Applies criminal penalties to individuals who without authorization obtain or disclose individually identifiable health information that is maintained by a covered entity (enforceable on 2/18/10)
 - Increases amount of civil penalties from \$100 per violation and a total of \$25,000 per year, to a tiered penalty system that can go to \$50,000 per violation and total penalties of up to \$1,500,000 per year
 - Gives State Attorneys General authority to bring civil action to enjoin a violation, seek statutory damages for individuals and obtain attorneys fees

Risks of Using Health Information for ACOs



- HHS Substance Abuse and Mental Health Services Administration (SAMHSA)
 - Criminal penalty: any person who violates the statute or these regulations shall be fined not more than \$500 in the case of a first offense, and not more than \$5,000 in the case of each subsequent offense

Risks of Using Health Information for ACOs



- HIE contractual compliance (including with the business associate terms in the participation agreements)
 - Each HIE should evaluate their contractual flexibility in using health information for ACO participation

Risks of Using Health Information for ACO



- Public opinion: Reactions of consumers and legislators

Mitigating Risks



- HIE contract terms that will permit activity, under defined terms and conditions
 - Include QSO contract language to comply with the Part 2 regulations
- Collaborative development of HIE policies to reflect all legal compliance obligations
- Public/ consumer outreach related to use case
- Legislative outreach and development of champions for use case
- Adequate insurance coverage

Public Health Opportunities



- Vital records exchange
- Required disease reporting
- Public health lab order entry and results reporting (newborn screening)
- Immunization registries
- Public health syndromic surveillance (biosurveillance)
- Public health alerts to health care providers
- Managing health care resources in emergencies
- Chronic disease management and prevention

Public Health Opportunities



- Integration of public health data into useful reports and products
- Integration of community public health information into clinical decision-support systems
- Medical product post-marketing drug safety surveillance
 - *Example: The FDA Sentinel Initiative (see <http://www.fda.gov/Safety/FDAsSentinelInitiative/ucm2007250.htm>)*

Laws Related to Use of Health Information for Public Health



- **HIPAA**
 - Applies to HIPAA covered entities (and soon to their business associates)
- **Federal substance abuse treatment regulations**
 - Applies to federally-supported substance abuse treatment programs and to some recipients of information from those programs
- **State law**
 - Application varies

HIPAA Privacy Rule and Public Health: Option 1



- PHI can be disclosed to public health authorities, or to entities acting under contract or under authority of public health authorities

HIPAA Option 2: De-Identify Data



- Remove or code the “identifiers” (if code is not derived from identifiers)
- Get a certification from a qualified statistician that there is a “very small” likelihood of determining identity

HIPAA Option 3: Use a Limited Data Set



- Partially de-identified PHI: remove all identifiers except dates related to individual and geographic designations (above street level)
- Must have “Data Use Agreement” in place with recipient

HIPAA Option 4: Authorization



- Numerous requirements for authorization forms

HIPAA Privacy Rule Challenges Ahead



- Current rule: Covered entity may receive payment for a disclosure of PHI where that disclosure is permitted by the regulations (such as for health care operations or research)
- HITECH (sec. 13405(d)) prohibits indirect or direct receipt of remuneration in exchange for a disclosure of PHI without the individual's authorization (with exceptions)
- OCR proposed amendments to HIPAA Privacy Rule would prohibit indirect or direct remuneration in exchange for a disclosure of PHI without authorization (with exceptions on the next slide) -- will this include non-financial remuneration?

HIPAA Privacy Rule Challenges Ahead



- **Exceptions:**
 - For public health purposes
 - For research, “where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit” the PHI
 - For treatment and payment
 - For the sale, transfer, merger or consolidation of the covered entity and related due diligence
 - To or by a business associate to perform activities for the covered entity, where “the only remuneration provided is by the covered entity to the business associate for the performance of such activities”
 - To an individual for access or accounting
 - Where required by law to disclose PHI
 - Where the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI, or a fee is otherwise expressly permitted by another law

HIPAA Security Rule

97

- Requires HIPAA covered entities (and soon business associates) to comply with rules to establish administrative, physical and technical safeguards (see 45 CFR Part 164, Subpart C)

HIPAA Breach Reporting Rule

98


- Requires covered entity (or business associate) that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses” unsecured PHI must notify individuals whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed as a result of a breach

The “Part 2” Regulations



- 42 CFR Part 2 governs information obtained from a federally-funded substance abuse treatment program, which information identifies an individual as a substance abuser
 - Federally-funded = Medicare or Medicaid participation, or tax-exempt status
 - Program = Holding self (or entity) out to the public as providing substance abuse treatment

The “Part 2” Regulations



- Part 2 permits disclosure of patient identifying information for public health activities:
 - With patient consent; or
 - To a “Qualified Service Organization”:
 - ✦ (a) Provides services to a program, and
 - ✦ (b) Has entered into a written agreement that:
 - (1) Acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from the program, it is fully bound by these regulations; and
 - (2) If necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the Part 2 regulations

Risks of Using Health Information for Public Health



- HIPAA civil and criminal penalties for noncompliance
 - Applies criminal penalties to individuals who without authorization obtain or disclose individually identifiable health information that is maintained by a covered entity (enforceable on 2/18/10)
 - Increases amount of civil penalties from \$100 per violation and a total of \$25,000 per year, to a tiered penalty system that can go to \$50,000 per violation and total penalties of up to \$1,500,000 per year
 - Gives State Attorneys General authority to bring civil action to enjoin a violation, seek statutory damages for individuals and obtain attorneys fees

Risks of Using Health Information for Public Health



- HHS Substance Abuse and Mental Health Services Administration (SAMHSA)
 - Criminal penalty: any person who violates the statute or these regulations shall be fined not more than \$500 in the case of a first offense, and not more than \$5,000 in the case of each subsequent offense

Risks of Using Health Information for Public Health



- HIE contractual compliance (including with the business associate terms in the participation agreements)
 - Each HIE should evaluate their contractual flexibility in using health information for public health activities

Risks of Using Health Information for Public Health



- Public opinion: Reactions of consumers and legislators

Mitigating Risks



- HIE contract terms that will permit activity, under defined terms and conditions
 - Include QSO contract language to comply with the Part 2 regulations
- Collaborative development of HIE policies to reflect all legal compliance obligations
- Public/ consumer outreach related to use case
- Legislative outreach and development of champions for use case
- Adequate insurance coverage

Opportunities for Commercial Use of De-identified Information



- Provision of data to the life sciences industry regarding drugs and devices
- Provision of data to the life sciences industry regarding physician prescribing (but note limit in some states)
- Provision of data to companies for marketing
- Provision of data back to HIE participants for marketing
- Etc.!

HIPAA Rules on De-Identification



- Remove or code the “identifiers” (if code is not derived from identifiers), including:
 - Name;
 - Geographic location information (unless only the first three digits of the zip code are used and the area has more than 20,000 residents);
 - Dates (except year) directly related to an individual, such as birth date, admission date, discharge date, dates of service, or date of death;
 - Age if over 89 (unless aggregated into a single category of age 90 and older);
 - Numbers related to the patient (SSN, etc.);
 - Biometric identifiers, such as fingerprints
 - Full-face photographs and any comparable images; or
 - Any other unique identifying number, characteristic, or code

HIPAA Rules on De-Identification




- Get a certification from a qualified statistician that there is a “very small” likelihood of determining identity

HIPAA Privacy Rule Challenges Ahead

109

- HITECH Act requires HHS to issue guidance on methods for de-identification of PHI
- OCR solicited stakeholder input from experts with practical technical and policy experience to inform the creation of guidance materials, and collected views regarding de-identification approaches, best practices for implementation and management of the current de-identification standard and potential changes to address policy concerns
- March 2010 2-day conference on de-identification – see http://www.hhs.gov/ocr/privacy/hipaa/understanding/covered_entities/De-identification/deidentificationworkshop2010.html

Risks of Using De-Identified Information for Commercial Purposes



- HIE contractual compliance (including with the business associate terms in the participation agreements)
- Public opinion: Reactions of consumers and legislators

By Terry Baynes

NEW YORK, March 11 (Reuters Legal) - A lawsuit filed in California this week accuses national drug-store chain Walgreen Co of unlawfully selling medical information gleaned from patient prescriptions, another front in the battle over personal information.

Unlike suits that focus on patient privacy, the plaintiffs accuse Walgreen of depriving them of the commercial value of their own prescription information.

According to the suit, brought by Todd Murphy on behalf of his two daughters and the rest of the class, Walgreen sells the prescription information to data mining companies who resell it to pharmaceutical companies for marketing purposes. The practice allows drugmakers to target physicians considered high-volume prescribers and those most willing to prescribe new medications, it said.

Courthouse News Service

CVS Faces Suit for Prescription Data Sales

By REUBEN KRAMER

PHILADELPHIA (CN) - CVS Pharmacy raked in millions by selling consumers' confidential prescription information to some of the nation's largest pharmaceutical manufacturers, according to a class action Monday.

"Not content with the receipt of the substantial funds generated from the performance of pharmacy services, defendants instead chose to generate additional sources of revenue from the confidential prescription information entrusted by consumers to defendants," the complaint in Philadelphia County Court states.

Arthur Steinberg and the Philadelphia Federation of Teachers Health and Welfare Fund filed the suit on behalf of other consumers who have received unsolicited communications after CVS allegedly sold customers' private information to Eli Lilly and Co., Merck, AstraZeneca, Bayer, and other drug manufacturers."

Vermont case could jeopardize patient privacy

March 03, 2011 | Molly Merrill, Associate Editor

WASHINGTON – Vermont's appeal to the U.S. Supreme Court to uphold the state's prescription confidentiality law – which allows doctors to block use of their prescribing information, mined from pharmacy records, for marketing purposes – will see its day in court next month.

Last week, Vermont Attorney General William Sorrell filed a brief arguing that Vermont's law is constitutional. But Data mining companies, including IMS Health and PhRMA, a trade organization for the pharmaceutical industry, claim the law violates their First Amendment rights. The case, *Sorrell v. IMS Health Inc.*, will be argued before the Supreme Court on April 26.

...

The Vermont federal district court upheld the law but a divided panel of the Second Circuit Court of Appeals reversed that ruling in November 2010. That decision is now under review by the Supreme Court. The First Circuit Court of Appeals upheld similar laws passed in New Hampshire and Maine.

Mitigating Risks



- HIE contract terms that will permit activity, under defined terms and conditions
- Collaborative development of HIE policies to reflect all legal compliance obligations
- Public/ consumer outreach related to use case
- Legislative outreach and development of champions for use case
- Adequate insurance coverage

Next Steps



- What secondary uses will be pursued?
- In what priority?
- What secondary use cases are appropriately centralized, and what use cases conducted by the HIEs at the local level?
- Should the state develop a common set of messaging to consumers and legislators?

Next Steps



- Should HIE practices be standardized with regard to secondary use?
 - Facilitated discussions with HIE decision-makers
 - Development of governance processes to enable and manage the use of health information for secondary purposes
 - Standardized participation agreements (on this issue)
- Other thoughts?

Questions?

117

Kristen B. Rosati

Coppersmith Schermer & Brockelman PLC

2800 North Central Avenue, Suite 1200

Phoenix, Arizona 85004

tel (602) 381-5464/fax (602) 772-3764

Email: krosati@csblaw.com

www.csblaw.com