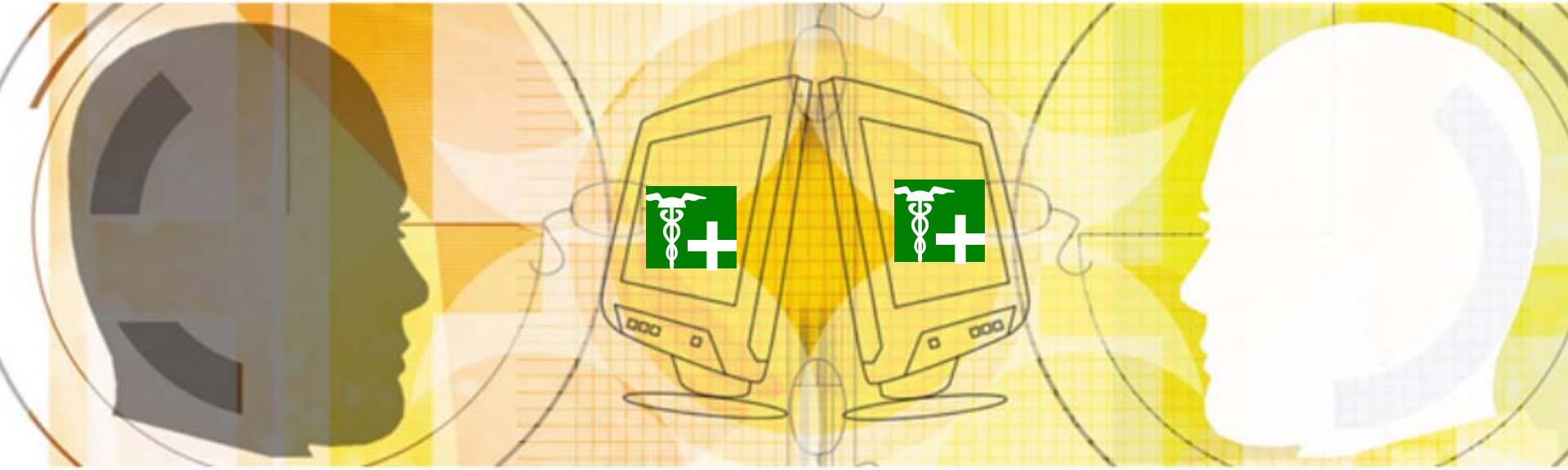


Electronic Health Records:

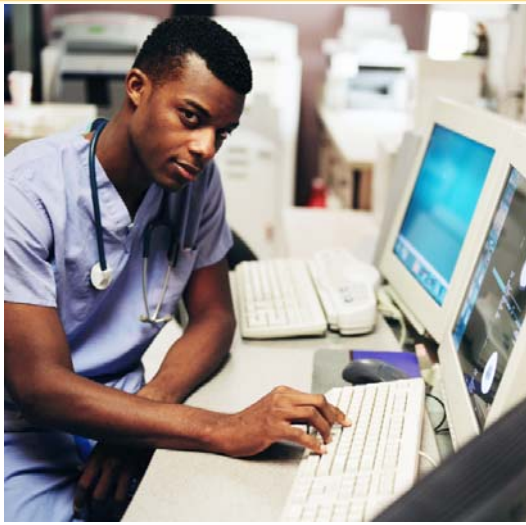
How to Implement Your Electronic Health Record and Share It Without Getting a HIPAA Headache

Tenth National HIPAA Summit **April 7, 2005**

Sarah E. Coyne
608-283-2435
sec@quarles.com

Quarles & Brady LLP
1 South Pinckney Street, Suite 600
Madison, WI 53703

What I An Electronic Health Recor



- Real time health record with evidence-based decision support tools to aid clinicians in decision making.
- Can support collection of non-clinical data such as billing, quality assurance, etc.
- Interoperable = many participants, all sharing records (clinic/hospital = mini-model).
- Some of the participants will be covered entities under HIPAA, some will not.

Two Levels of Difficulty

- Today's Difficulty: Internal EHR or 2 participant.
- Tomorrow's Difficulty: Interoperable EHR between multiple entities.

The Interoperable EHR Buz

- On April 27, 2004, President Bush called for widespread adoption of interoperable EHR within ten years.
- May 6, 2004, Then DHHS Secretary Tommy Thompson appointed David J. Brailer, M.D., Ph.D. to serve in this new position.

- Executive Order 13335 requires the National Health Information Technology Coordinator (NCHIT) to report (within 90 days of operation) on the development and implementation of a strategic plan to guide nationwide implementation of NCHIT in the public and private sectors.
- EO 13335 specifically requires National Coordinator to ensure that patients' IIHI is secure and protected.

DHHS Specified Goals

- Inform clinical practice.
- Interconnect clinicians.
- Personalize care.
- Improve population health.

Regional Health Information Organization

- Hot term of the day: RHIO.
- An organization facilitating electronic health records within a region, state or other designated area.
- An actual organized entity with a board and governing bylaws.
- Charged with overseeing and implementing a secure health information exchange among the participating providers within that region.
- Unclear at this point which organizations will be RHIOs.

National Health Information Infrastructure

- National EHR Interoperability – ideally, RHIOs exchanging information with each other.
- A workable authentication process for that giant web.
- A workable access process.
- Security safeguards.

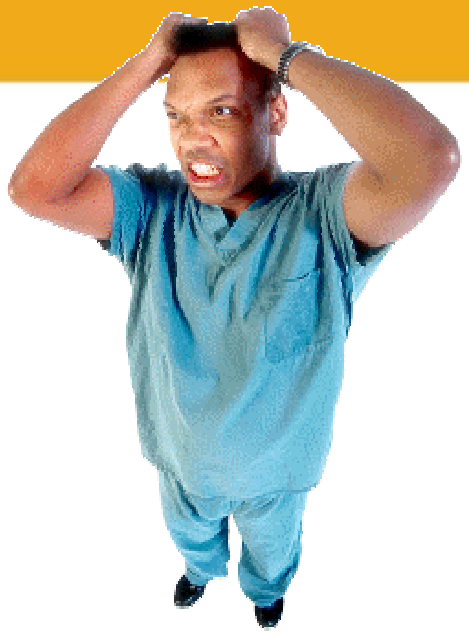
I Lie

- There are going to be headaches from HIPAA with interoperable EHRs.
- Let's try to figure out the best medicine to treat those headaches.

Some Headaches

- Patient authorization.
- Disclosures permitted without authorization (TPO, etc.).
- Patient rights.
  - Notice of privacy practices.
  - Requesting amendments.
  - Restricting modes of communication.
  - Accounting.
  - Access to designated record set.
  - Requested restrictions on disclosures.
- Business associate requirements.

More Headaches



- Security Rule Authentication is a 3 aspirin headache.
- Security Rule Joint Risk Analysis.
- Security Rule Implementation Specifications – Especially Those Pesky Addressable Ones!
- Minimum Necessary Requirements.

HIPAA Headache #1
State Law Issues/ Preemption

- State laws add layer of complexity to every single headache.

- Headaches intensify with “special” records where state protections are often more stringent than HIPAA (HIV/AIDS, mental health, AODA, STDs, child abuse).

HIPAA Headache #2: The Minimum Necessary Standard

- Each CE in the RHIO may use or disclose only the minimum necessary amount of PHI.
- Helpful points:
  - Exception for Treatment.
  - May rely on requests as minimum necessary from other CEs.
- Same old problem: if you get into the EHR and see a bunch of unrelated stuff, is that a violation of the MNS or is it incidental?

HIPAA Headache #3: Business Associate Requirements

- If participating entities perform functions or provide services involving exchange of PHI, RHIO can be structured to include BA provisions.
- If the RHIO is an OHCA, providers within the OHCA do not need BAAs.
- RHIO itself is likely a BA.

HIPAA Headache #4
What Is A Disclosure?

- Internal EHR – the question is going to be appropriate use, not disclosure (*e.g.* HIV test results).
- Interoperable EHR – is every piece of ePHI in the RHIO disclosed with each cross-entity access?
  - Need RHIO-wide agreement on this point.
  - Consider levels of access (greatest access for treatment, HCO etc.).

HIPAA Headache #5
Patient Authorizatio

- The patchwork of state laws vary as to which disclosures are permitted without patient authorization – greater preemption would help!
- Work with IT folks for electronic tracking of patient authorization for each participating provider in the interoperable system.
- Consider whether viewing of extraneous ePHI can legitimately be categorized as incidental disclosures.
- To keep claims down, education (of patients AND workforce) is key.
- Another key: electronic functionality to achieve tracking of patient authorization.

HIPAA Headache #6: TPO and Other Permitted Disclosure

- Where do the RHIO's activities fit in?
  - Healthcare operations: QA, business management, general administrative activities.
  - TPO exception provides broad latitude to move ePHI within the interoperable record.

- Legitimate use for treatment but what about all the incidental disclosures (and internally, uses).

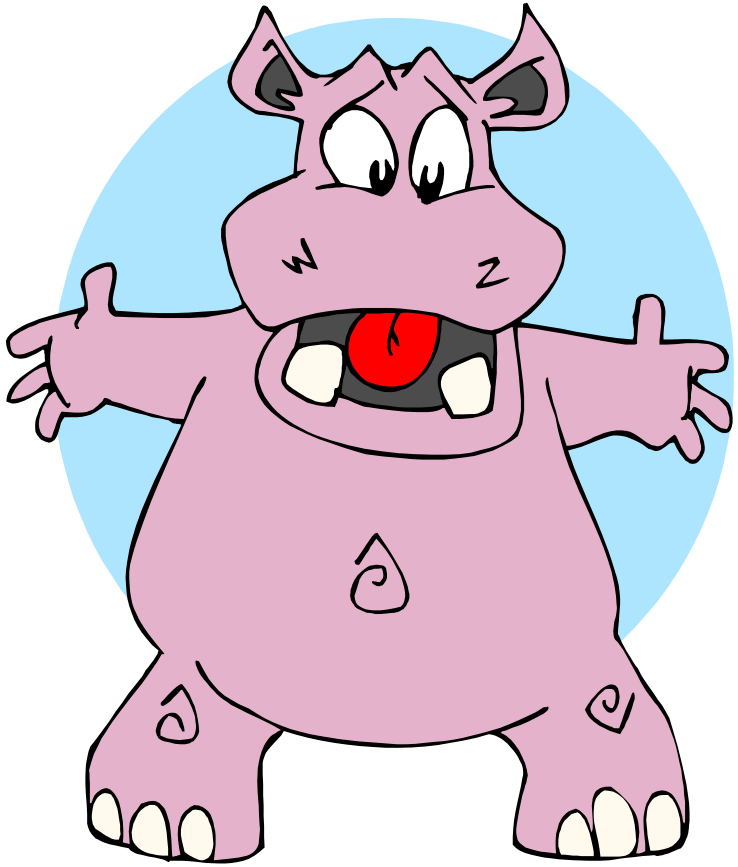
- The OHCA concept may help.
  - Clinically integrated care setting in which individuals typically receive health care from more than one health care provider (but is that always true?)
  - Organized system of health care in which more than one CE participates and in which participants hold themselves out to the public as a joint arrangement doing utilization review, QA, or payment activities with risk sharing.

HIPAA Headache #1
Notice Of Privacy Practices

- If RHIO = OHCA, Joint NPP permissible. (How's that for alphabet soup!)
- Even then, need uniformity of uses and disclosures within the RHIO.

HIPAA Headache #8: Patient Right t Alternative Modes of Communicatio

- Need RHIO-wide electronic system for patient designation of preferred communication of PHI.



HIPAA Headache #9
Patient Acces

- Patient has right of access to PHI in a designated record set (DRS) (and non-duplicative PHI held by BAs).
- Need RHIO-wide patient access system and this implicates the Security Rule authentication and audit trail headaches.
  - How will access to RHIO be managed?
  - Who gets to be the gatekeeper?
  - What is the DRS for that patient, in the context of the interoperable EHR?

HIPAA Headache #10: Patien Restrictions on Disclosure

- Patients may request restrictions on disclosure of their PHI
- CE is not obligated to agree, but there is a documentation process for reviewing and responding.
- Need centralized RHIO manager for this process.

HIPAA Headache #1
Accounting for Disclosures

- Accounting is already an administrative headache.
- Interoperable EHR could serve as exponential headache multiplier.
- Need automated electronic system for managing RHIO-wide accounting.

HIPAA Headache #12 Requests to Amend

- Patient has the right to request amendment of PHI in the DRS.
- CE not obligated to acquiesce but process for evaluating and denying.
- Need RHIO-wide system for managing such requests and ensuring that if request is granted, PHI is amended on a RHIO-wide basis.

HIPAA Headache #13 Research

- RHIO-wide privacy board?
- RHIO-wide waivers of authorization?
- One simplifying factor: QA studies are HCO, not research.

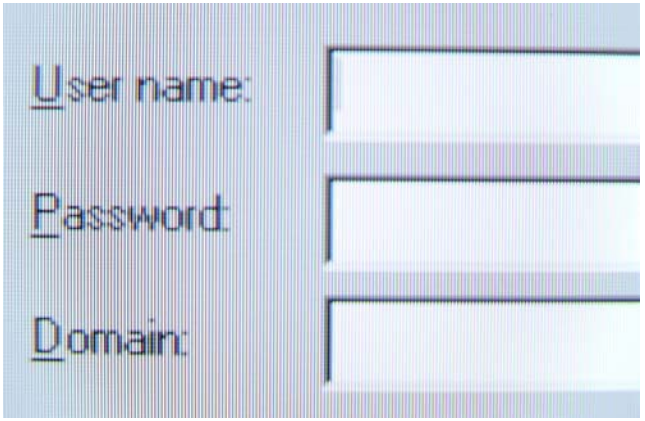
HIPAA Headache #14: Securit Rule Risk Assessmen

- How do the participating entities measure their risk of participating in a RHIO?
- One solution: uniform minimum security practices for all RHIO participants and thus uniform risk analysis.

HIPAA Headache #15: Addressabl Implementation Specification

- Each RHIO participant must decide whether each addressable implementation specification is reasonable and appropriate for the RHIO, the shared EHR.
- If not, each participant must evaluate the options and document a common solution.
- How will each of these work in an interoperable setting?
  - authorization/supervision of those who work with ePHI.
  - method for clearing given members of workforce to specified levels of ePHI access.
  - termination of access to ePHI when workforce members leave.

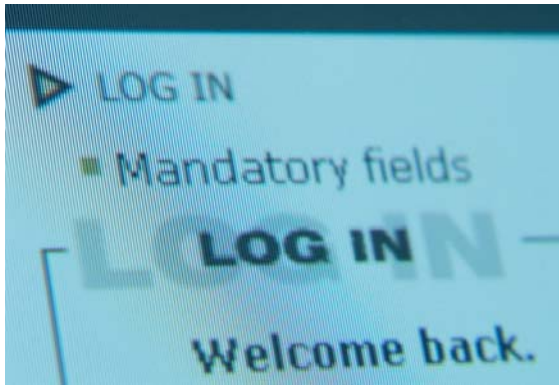
- periodic security updates to workforce of all RHIO CEs.
- virus protection.
- monitoring log-ins.
- password management.
- periodic testing and revision of contingency plans.
- automatic log-off after periods of inactivity.
- encryption/decryption.
- mechanism to authenticate ePHI.
- integrity controls.



HIPAA Headache #16: Required Implementation Specification

- Risk analysis – separate analysis for the RHIO?
- Reasonable and appropriate risk management – need specified manager for RHIO.
- Sanction policy (perhaps best managed on an entity-by-entity basis?)
- Information system activity review.
- Reporting of security incidents (takes on larger proportions with the interoperable EHR).
- Contingency planning for data back up, disaster recovery, emergency mode operation.
- Final disposal of ePHI.

- Removal of ePHI from media that will be re-used (disks etc.).
- Unique user ID!
- Access to ePHI during emergency.
- Person/entity identification.



- Policies/procedures/documentation (on a RHIO-wide basis: should each covered entity have a policy specifically addressing participation in the RHIO?)
- 6 year retention – managed on an entity-by-entity basis? What about information stored solely in electronic form?
- Don't lose sight of requirement to update – centralized function in RHIO should coordinate.

HIPAA Headache # 17
Privacy and Security Officer

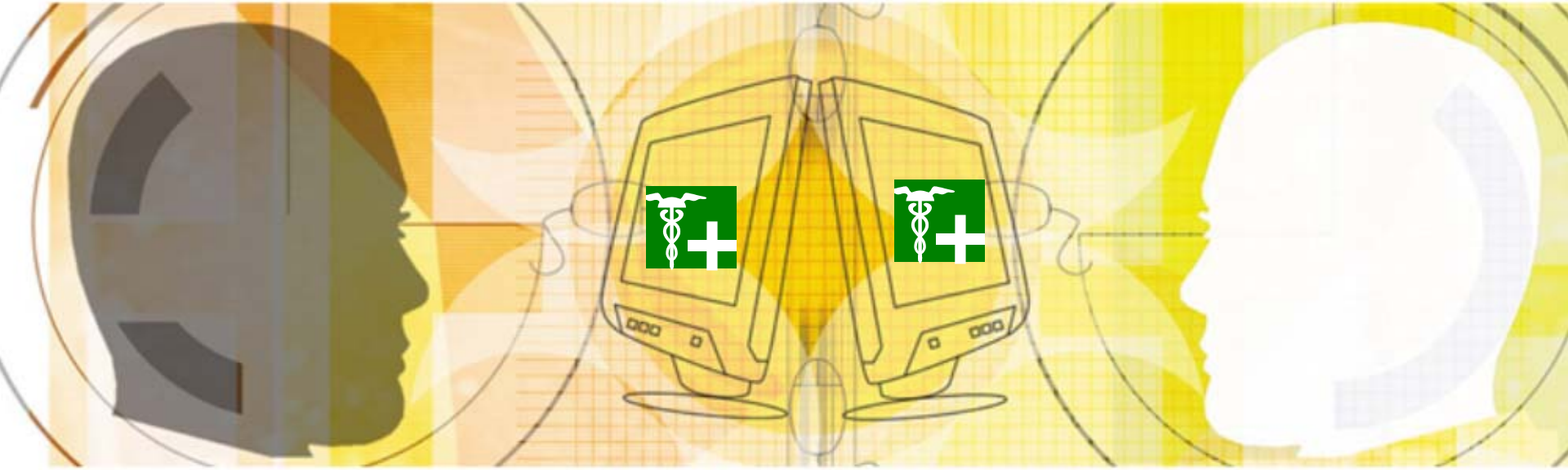
- Security officer.
  - Required for each covered entity.
  - Should there be a centralized position for the RHIO?
  - Additional points addressing the interoperable EHR in the entity SO description?
- Same analysis for Privacy officer.

The Best Medicine

- Sounds trite, but every participant in the RHIO should be strategically on the same page.
- Some sort of uniform patient identification system
- Don’t forget about state law! Some RHIOs will cross state lines.
- If possible, start with an existing structure/ organization.
- Have a lot of money. ☺
- Another one that sounds trite: trust.

- Leader to initiate and oversee.
- Commitment: If you're in, you're in.
- Some system of measurement: How is it working?
- Joint accountability for success.
- Everything on the table: No hidden agenda.
- Neutral meeting ground for organizational efforts.

- Interface with:
  - State officials (include the Governor!)
  - Local academic medical centers
  - Local hospitals
  - Local health plans
  - Local employers
  - Local professional societies and associations
  - Consultants and vendors (don't forget the lawyers!)
  - QIOs



Electronic Health Records:

How to Implement Your Electronic Health Record and Share It Without Getting a HIPAA Headache

Tenth National HIPAA Summit **April 7, 2005**

Sarah E. Coyne
608-283-2435
sec@quarles.com

Quarles & Brady LLP
1 South Pinckney Street, Suite 600
Madison, WI 53703