

Legal Issues in Implementation of an Electronic Health Record System

Presented by:
Barry S. Herrin, JD, CHPS, FACHE
Smith Moore Leatherwood LLP
Atlanta GA
404-962-1027
barry.herrin@smithmoorelaw.com

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Overview

- Top Myths About EHR Contracts
- The “Do Not” List
- Important Contract Provisions
- Implementation Issues
- Other Practical Considerations



Top Myths About EHR Contracts

- Everybody signs the vendor's standard form
- The standard form is non-negotiable
- If you miss the signing deadline, pricing goes up dramatically
- The vendor's form protects your facility as well as the vendor



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Top Myths About EHR Contracts

- The vendor's form tells you exactly what the technology can do
- The vendor knows better than you do what features your facility needs
- You can hammer out some of those details after you sign the contract



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

The “Do Not” List

- Do not sign vendor’s online contract (where you click the “agree” button)
- Do not agree to solely calendar-based payments



 SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

The “Do Not” List

- Do not sign contract without getting sound legal and consulting advice from professionals experienced in EHR contracting
- Do not contract with a vendor with whom you can’t agree on key points—the relationship will not get better after you sign the contract

 SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Licensing
 - Anticipate growth when determining structure/number of licenses
 - Seek reduced fees for non-full-time users
- Staffing
 - Restrict vendor's ability to remove good/key people from the project
 - Be sure you can add or remove personnel if needed



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Payment terms
 - Include performance milestones; do not base solely on calendar
 - Down payment of no more than 30% (20% is preferred)
 - Final payment at project completion or end of testing
 - Cap annual price increases or tie to CPI
 - Provide incentives for both parties
 - What about custom work?



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Testing and Acceptance
 - Detailed criteria in writing
 - Include users and key departments in testing
 - Consider robust RFP process to specify needed performance



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Preserve Access to Data
 - When you need it and in required format
 - Address return of data upon termination of contracts, including format and cost to transition data
 - Source code escrow



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Training
 - Specify frequency, length, cost
 - Have recourse for poor training (money back or retraining)



 SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Upgrades
 - How frequent? How long has current version been in effect? What about previous version? How long will vendor support old versions?
 - Will any near-time upgrades be included in original purchase price?
 - Automatic upgrades for changes in law?

 SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Confidentiality/Security
 - Address issues related to breaches
- Warranties
 - IP
 - Service warranty
 - Compliance with law
- Insurance
 - General liability, workers' compensation, professional liability (E&O)
 - Cybersecurity



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Support Services
 - Tiered response times?
 - 24/7? If not, what happens in case of emergency?
 - Escalation of issues



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Statements of Work
 - Include deadlines and specify responsibilities
 - Include deliverables and acceptance criteria
 - SOWs should enhance and clarify contract and be consistent with terms of the agreement, not conflicting



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Remedies
 - Money back → seek total amount you've paid out
 - Return/replacement of software if it doesn't work
- Liability
 - Vendor will try to limit significantly
 - Try to avoid liability caps, especially for vendor's errors or omissions
 - Carve out HIPAA breaches from any caps
 - The "learned intermediary" doctrine



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Important Contract Provisions

- Termination
 - Transition period/services
 - Ensure you can terminate for cause
- Dispute Resolution
 - Defined process
 - Avoid arbitration



SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Implementation Issues

- Defining the “Legal” HER
- The “Source-Output Gap”
- HITECH and Permissible Sharing of ePHI
- Penalties for Breach



SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Defining the “Legal” EHR

- Legal Health Record
 - The record that is generated **at or for** a healthcare organization as a *business record* that documents the clinical activity respecting a patient and is the record that will be disclosed upon request
- Electronic Health Record
 - Health information recorded on any digital medium that is evidence of transactions or events that (1) has legal or business value and (2) indicates an intention to be memorialized



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Defining the “Legal” EHR

- Legal Electronic Health Record
 - Which aspects of these 2 definitions do we pick?
 - Is it the legal health record created and maintained in an electronic format, or is it the electronic health record further defined to make it “legal”?
 - It is not a distinction without a difference



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Definitional Problems

- Cannot begin with “anything that has business value,” because that means ALMOST EVERYTHING
- Cannot begin with “what is discoverable,” because that means EVERYTHING
- Don’t forget the “H” in EHR



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Much Ado About Nothing?

- You already know what you **MUST** have in a patient’s health record, don’t you?
- Are you focusing more on the **FORMAT** or on the **CONTENT**?



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Much Ado About Nothing?

- What's in your Designated Record Set?
 - Clinical vs. Financial Records
 - What process did you use to define the DRS?
- Do you really want to keep in electronic form all of the things you currently create in paper form?



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

ZITS/ by Jerry Scott and Jim Borgman



ROCKY MOUNTAIN NEWS, 10/9/2006

“Old School” Record Issues

- Post-it® Notes
- Telephone message slips
- Your “miscellaneous” tab
- Stuff that isn’t supposed to be in the chart to start with
- “Volunteered” records
- Throwing stuff away



 SMITH MOORE
LEATHERWOOD.

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

The “Real” Problem with the Legal EHR Definition

- EHRs don’t necessarily preserve data content (NOT format) when converting from SOURCE (point of data entry) to OUTPUT (later reproduction for care or ROI)
- Analogize this to a “scanned” paper record – SOURCE data and OUTPUT data are IDENTICAL

 SMITH MOORE
LEATHERWOOD.

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

The “Real” Problem with the Legal EHR Definition

- If the data the clinician sees on the floor when treating the patient (SOURCE) cannot be reproduced exactly in the same detail at a later time (OUTPUT), then the SOURCE data, and NOT the OUTPUT data, is the “legal” EHR
- In defining the “legal” EHR, address the SOURCE/OUTPUT gap – there may be categories of electronic (OR PAPER) data that may have to be kept in a “human perceivable” form outside of the EHR if the EHR system cannot manage the SOURCE/OUTPUT conversion with integrity



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH and the Permissible Sharing of ePHI

- HITECH (part of ARRA) expanded the coverage of HIPAA to business associates
- Also included the concept of “unsecured PHI”
 - ANY paper PHI
 - Electronic PHI (ePHI) not protected in a manner specified in NIST criteria (basically unencrypted)
- Impermissible use, access, disclosure, acquisition of “unsecured PHI” is a “breach” requiring notice to patients, the government, and in some cases the media



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH and the Permissible Sharing of ePHI

- HITECH contains three narrowly construed exceptions
- If an acquisition, access, use, or disclosure fits within an exception, it is not a breach, **even if** information was unsecured PHI and the disclosure is not permitted under HIPAA



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.



HITECH Exceptions

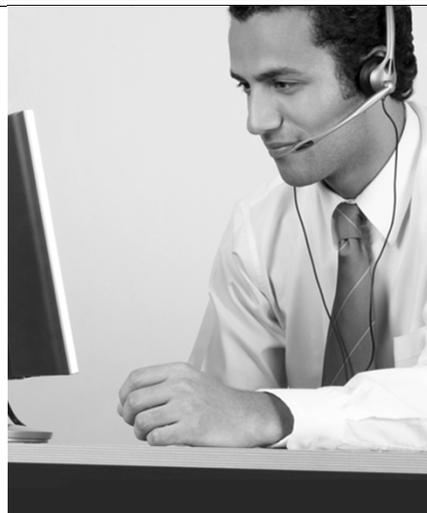
- Exception 1: Unintentional access to, or acquisition or use of, PHI:
 - By a workforce member for the covered entity or BA
 - Acting in good faith
 - Within the course and scope of duties
 - If the access, acquisition, or use does not result in any further use or disclosure in a manner not permitted by HIPAA



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Example: Billing employee receives and opens an e-mail containing patient's PHI that was mistakenly sent to her. Billing employee notifies the sender of the error, and then deletes the e-mail without further using or disclosing the information. **Exception applies – no breach.**



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Example: Receptionist, who is not authorized to access PHI, decides to browse through patient files to find out information about a friend's treatment.

Exception does not apply –breach.



SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Example: A physician on the medical staff, who is authorized to access PHI, looks through the medical records of patients she has not treated and whose cases she has not been asked to consult.

Exception does not apply –breach.



SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Exception 2: Inadvertent disclosure of PHI
 - From one workforce member at the covered entity or BA to another at the same covered entity or BA
 - Where both workforce members are authorized to access the information
 - If the access, acquisition, or use does not result in any further use or disclosure in a manner not permitted by HIPAA



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Example: Inadvertent disclosure by a member of the hospital medical staff, even if she is not a hospital employee, to a hospital employee who is authorized to receive PHI, provided that the employee does not subsequently inappropriately use or disclose the information. **Exception applies – no breach.**



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Example: A member of the medical staff deliberately discloses information to another member of the medical staff regarding a patient for whom the receiving medical staff member has no treatment or consultation responsibilities. **Exception does not apply –breach.**



 SMITH MOORE
LEATHERWOOD.

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Exception 3: Unauthorized disclosure to an unauthorized person of PHI:
 - Where there is a reasonable good faith belief
 - That the unauthorized recipient would not reasonably have been able to retain the information

 SMITH MOORE
LEATHERWOOD.

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Example: A nurse mistakenly hands Patient A the discharge instructions for Patient B. The nurse immediately recognizes his error and retrieves the document before Patient A has a chance to review the information. **Exception applies – no breach.**



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

HITECH Exceptions

- Example: The billing office, due to a lack of reasonable safeguards, send a number of patient statements to the wrong individuals. Some of the statements are returned unopened, marked “undeliverable.” **Exception applies – no breach.** The other statements that were sent to the wrong addresses, however, are not returned. **Exception does not apply – breach.**



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Why You Should Care

- Four new penalty tiers have been implemented, effective November 30, 2009
- For violations occurring on or after **February 18, 2010**:
 - CMPs ranging from \$100 to \$50,000 per violation, up to \$1.5 million for identical violations occurring during a calendar year, where the entity did not and, by exercising reasonable diligence, would not have known that a violation occurred;



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Breach Penalties

- CMPs ranging from \$1,000 to \$50,000 per violation, up to \$1.5 million for identical violations occurring during a calendar year, where the violation was due to “reasonable cause” and not willful neglect (reasonable cause = “circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply”);



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Breach Penalties

- CMPs ranging from \$10,000 to \$50,000 per violation, up to \$1.5 million for identical violations occurring during a calendar year, where the violation was due to willful neglect and was corrected during the 30 day period following the date the covered entity knew or should have known the violation occurred



 SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Breach Penalties

- CMPs of at least \$50,000 per violation, up to \$1.5 million for identical violations occurring during a calendar year, where the violation was due to willful neglect and was not corrected during the 30 day period following the date the covered entity knew or should have known the violation occurred



 SMITH MOORE
LEATHERWOOD

© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Breach Penalties

- Penalties may be avoided if the entity can demonstrate:
 - Violation is the result of a knowing, criminal act by an individual that is punishable under 42 U.S.C. § 1320d-6; or
 - Violation is not due to willful neglect and was corrected within the 30 days following discovery or such additional period as the Secretary deems appropriate



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Breach Penalties

- Secretary may waive an imposed CMP if the CMP would be excessive if the violation was due to “reasonable cause,” even where the violation was not corrected during the 30 day period following discovery or other period deemed appropriate by the Secretary.



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Other Practical Considerations

- Does your EHR system capture your institutional knowledge and best practices regarding record use, maintenance, and disclosure?
- Does/will HIM have a seat at the “adult table” when systems are selected?



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Other Practical Considerations

- Who is going to be the guardian of information after the system is implemented?
- Will the system eliminate “silos”?
- Is the tail wagging the dog?
- Space Shuttles and Roman Chariots



© 2011 Smith Moore Leatherwood LLP. ALL RIGHTS RESERVED.

Contact

Barry S. Herrin, JD, CHPS, FACHE

404-962-1027

877-404-7466 x1027

barry.herrin@smithmoorelaw.com



www.legalhimformation.com

Find us on Facebook - legalhimformation