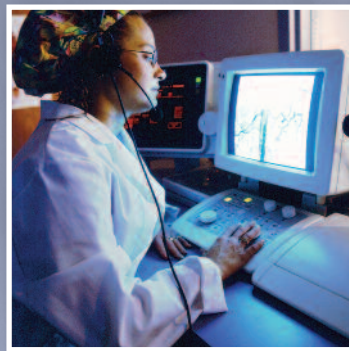
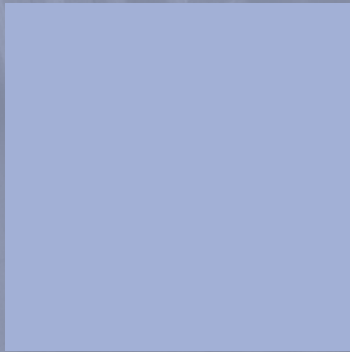


Contracting for Electronic Health Records: Guidelines for Hospitals



2011



American Hospital
Association

Using the Guidelines

The American Recovery and Reinvestment Act of 2009 (ARRA) authorized incentive payments under Medicare and Medicaid to “meaningful users” of certified electronic health records (EHRs) beginning in fiscal year (FY) 2011. Beginning in FY 2015, ARRA also phases in penalties for those who fail to meet “meaningful use.” To be eligible for these incentives and to avoid future penalties, hospitals and physicians must use EHRs that have been certified through a new federal certification process established by the Office of the National Coordinator for Health Information Technology (ONC).

To assist hospitals in working with health information technology (IT) vendors to achieve meaningful use, the American Hospital Association (AHA) has developed the following guidelines for EHR contracting. These guidelines address the most common issues for hospitals that license EHR software applications and/or obtain related products and services from a vendor.

The guidelines are intended to help hospitals, especially smaller hospitals and those just beginning to implement IT, identify and address critical concerns involved in establishing EHR vendor relationships. **They are NOT intended to, and cannot, substitute for responsible legal advice.** Working closely with appropriate legal counsel, hospitals should examine and carefully evaluate how to use the guidelines as part of their efforts to establish appropriate vendor relationships to address their particular technology needs.

The guidelines provide a checklist of general topics that hospitals need to consider when establishing a vendor contract. They identify some of the specific questions to be addressed in each area and, where appropriate, suggest options for addressing a particular question.

The guidelines focus on licensing for software applications and are applicable primarily to the scenario where a hospital will license the applications to be run on the hospital’s servers. Remotely hosted applications (i.e., cloud computing solutions) raise a series of additional issues, primarily due to the hospital’s loss of control over the hardware, software and its data. Hospitals that are considering a remotely hosted application, for example, will need to give consideration to:

- *Availability:* If access to the vendor’s cloud computing solution is interrupted, what procedures and remedies are in place to minimize the impact on the hospital and ensure a prompt resolution?
- *Data control:* Who owns the data processed on the system, and what rights will the vendor claim to use such data? Will the hospital be able to readily access its data at any time and in a mutually agreed upon format?
- *Privacy:* Where will the data be stored (i.e., jurisdiction) and how will this impact the applicable privacy regulations?
- *Data security:* What is the vendor doing to address confidentiality, theft, data corruption and data loss of the hospital’s data stored and processed on the vendor’s servers?
- *Data breach:* The parties need to address data breach notification laws and allocate responsibility and cost between the vendor and the hospital when a data breach is caused by the vendor.

An in-depth consideration of these additional issues, however, is beyond the scope of these particular guidelines.

Contracting for Electronic Health Records: Guidelines for Hospitals

These guidelines are designed to address some of the most common issues that arise when a hospital licenses electronic health records (EHR) software applications and obtains related products and services from a vendor. They are most applicable to the scenario where the hospital will license an application to be run on the hospital's servers. Issues raised by remotely hosted applications (i.e., cloud computing solutions) are beyond the scope of this checklist.

DEVELOPMENT

Does the application require custom development, enhancements or modifications prior to use by the hospital? If so, consider the following:

- *Custom development issues generally:* If the application requires custom development, enhancements or modifications prior to use by the hospital, consider the specific needs related to that custom development.
- *Specifications:* The vendor should perform the custom development in accordance with mutually agreed upon specifications that should be detailed in an exhibit or incorporated by reference into the agreement. The agreement should include a process to manage changes to the specifications.
- *Schedule:* The agreement should include a detailed development schedule, including milestones.
- *Cost of development:* For any custom development work, specify whether the fee for custom development services will be charged at a fixed price, on a time and materials basis, or already is incorporated in the license fee structure. Also, consider whether custom development will impact the cost of maintenance and support services.
- *Other potential issues to consider:* The hospital may want to consider whether there are other standards that it would like to see included in the EHR specifications. For example, a hospital may want to consider custom development such as compatibility with HL7 interoperability standards, FDA Part 11 rules for electronic records in clinical trials and other types of standards.

SCOPE of LICENSE

The hospital will want to understand the scope of the license it obtains from the vendor. Consider:

- *Scope of license:* Review the scope of license rights to ensure that the scope is broad enough to cover all of the hospital's anticipated needs.
- *Licensed subject matter:* Address whether the hospital needs source code, object code, user documentation, internal documentation and/or updates of the application. If the hospital will receive source code, it also should receive all materials needed to use the source code effectively. Note that, prior to obtaining rights to modify the application's source code, the hospital should consider the implications and potential liabilities, including any impact on the application's performance, compliance with regulatory standards, etc.
- *Licensed rights:* Address whether the license is exclusive or non-exclusive. Include, as applicable, rights to use, copy, modify, distribute and display. Include the right to sublicense the foregoing rights if applicable.
- *Users and equipment:* Determine who can use the application and where the application will reside. Consider types of licenses: network, CPU, seat, concurrent user, named users, server, site or enterprise. Also consider whether the application must be used in conjunction with specified hardware or software. Will the hospital need the right for affiliates, contractors, independent physician practices or other third parties to use the application? If applicable, specify the scope of sites and facilities where the hospital needs to use the application. Can a third-party service provider operate the application for the benefit of the hospital?
- *Hosted environment:* Will the hospital have the right to deploy the application in a hosted environment or will any of the components of the application be accessible to the hospital's users through the Internet?
- *Territory:* If the vendor imposes any geographic limitation of use (e.g., limiting use to the U.S.), consider whether those limitations are problematic for the hospital's proposed scope of use.

RESTRICTIONS on LICENSE GRANT

Understand the implications of any restrictions on the license for the application that are imposed by the vendor to ensure that the license restrictions remain consistent with the hospital's intended use and other business objectives. Consider:

- *Restrictions on copying the application and documentation:* Consider the need of the hospital to copy the application for archival and backup purposes and copy the documentation for training and distribution.
- *Restrictions on using or modifying the application:* Carefully read the license restrictions in light of business objectives, such as limitations on how the application can be used, or prohibitions on modifying the application.
- *Sublicense flowdown requirements:* Where the hospital will sublicense the application to third parties, carefully review any provisions that the vendor requires the hospital to include in the hospital's agreements with the third parties.

CERTIFIED EHR TECHNOLOGY STANDARDS

Carefully review contract provisions that specify the vendor's obligations to meet the certification requirements set by the federal government to support meaningful use. Consider:

- *Warranties regarding compliance with regulatory standards:* Carefully review the representation and warranty by the vendor that the application currently complies in all material respects with the Stage 1 requirements necessary for eligible hospitals to successfully demonstrate meaningful use of certified EHR technology and receive the associated incentive payments. Address whether the application will continue to meet or exceed Stage 1 requirements throughout the term of the contract.
- *Alternative language:* If software is not intended to meet all of the meaningful use Stage 1 specifications (for example, because the hospital is purchasing various EHR Modules rather than a Complete EHR), include a representation and warranty that the application currently complies with the specific capabilities applicable to the EHR Module.

- *Meaningful use Stage 2 and 3 requirements:* The vendor should agree that the application will be updated to meet the Complete EHR (or EHR Module, as appropriate) standards that will be mandated for eligible hospitals to meet the requirements for incentive payments in Stages 2 and 3.
- *Manner of providing updates:* The vendor could provide updates by providing replacement third-party or vendor software that meets the Stage 2 and/or 3 requirements.
- *Timeframe:* Updates should be provided sufficiently in advance to allow for a testing period prior to the effective date.
- *Remedies:* Address the available remedies for the vendor's failure to update the application to meet Stage 2 or 3 requirements by the effective date of the applicable requirements. Examples of remedies may include: termination right without penalty; source code escrow release; service credits (such as savings on ongoing support fees while not in compliance); damages in the amount of meaningful use incentive payments not received by the hospital or in the amount of payment reductions imposed on the hospital in 2015 or later.
- *Ongoing obligation to maintain certification:* Consider obligating the vendor to agree to maintain certification of the application over the course of agreement, for a particular version or all versions of the application.
- *Remedies for failure to maintain certification:* Consider possible remedies where the vendor fails to maintain such a certification, such as costs to change vendors (or some period of time in which costs of changing vendors will be covered), and/or any lost Medicare/Medicaid incentive payments.
- *Agreement to seek certification as applicable certification standards are updated or modified:* Consider seeking a representation from the vendor that it will seek the appropriate certifications as new applicable certification criteria are required. This may be an alternative to requiring that a vendor warrant that it will meet certification criteria established in the future, instead requiring the vendor to agree to engage in the certification process.

DELIVERY and IMPLEMENTATION

Spell out the obligations related to the delivery and implementation of the application. Consider:

- *Delivery:* Specify when and how the application will be delivered and/or accessed (such as being delivered to the hospital and installed on hardware, or accessed via the Internet). When establishing an application delivery date, consider the hospital's timing for going live with the application and possible contingencies that may delay the process.
- *Penalties for late delivery:* Consider including late delivery consequences to incentivize on-time delivery.
- *Installation and integration:* Address whether the vendor will install the application. Clarify which party is responsible for integrating the application with the hospital's existing systems. Will the vendor be responsible for developing programming interfaces between the hospital's existing systems and the application? For complex implementations, the hospital should ensure there is a robust project management structure and clearly defined procedures in place to guide the implementation. Plans for more complex implementations typically include detailed project timelines, identifying internal and external resource requirements and specific responsibilities of the parties involved. In certain instances, the hospital may find that an "off-the-shelf" implementation plan provided by the vendor is not sufficient to address the hospital's unique internal processes and requirements. Depending upon the complexity of the task, the parties may address implementation services through a separate agreement or addendum.
- *Data conversion:* Address whether the vendor will provide data conversion services and the associated fees.

HARDWARE and EQUIPMENT

Establish the responsibilities and obligations of each party to ensure that the appropriate hardware and other equipment are in place for the application to operate. Consider:

- *Equipment and facilities:* Address any hardware, third-party software, content and/or network requirements for the application to operate and specify which party is responsible for obtaining any such hardware, software, content and network requirements. When evaluating these types of requirements, consider compatibility issues with the hospital's existing information technology infrastructure.
- *Hardware:* If purchasing hardware from the vendor, address: (1) schedule for delivery; (2) title transfer and risk of loss; (3) responsibility for installation; (4) the hospital's obligation to meet minimum requirements for the installation site (such as power supply, Internet connectivity and temperature/humidity controls); and (5) hardware maintenance obligations.
- *Hardware purchase vs. lease:* Consider implications to the hospital of leasing instead of purchasing certain hardware, including any restrictions placed on use of leased hardware.

TRAINING

Outline the respective responsibilities of the parties for training hospital staff and others to use the application. Consider:

- *Training and materials:* Address whether the vendor will provide training services and, if so, the timeframe to roll out training for hospital personnel. Specify whether the vendor will be responsible for developing and/or delivering training materials for use by the hospital. What level of training is included without a separate charge?
- *Location:* Will training be conducted at the hospital's facilities, will the hospital need to send employees to the vendor's central training facilities or will training be conducted remotely?
- *Audience:* Will the vendor provide comprehensive training for users throughout the hospital or will the vendor "train the trainer," whereby key hospital employees will be trained to use the application and then be responsible for training other end users?

TESTING and ACCEPTANCE

Address how the application will be tested to ensure it meets product specifications and clearly outline criteria and procedures for final acceptance of the application by the hospital. Consider:

- *Testing:* The hospital should have the right to review, inspect and test the application before the purchase is final, particularly if the hospital is acquiring a custom product which has not gone through the rigorous product testing processes of off-the-shelf software. It is advisable to ensure participation in the testing process by the types of individuals within the organization that will actually be using the application in the future.
- *Acceptance criteria:* These criteria should be detailed and in writing. The criteria should include conformance of the application with the product specifications. Such specifications should be sufficiently detailed.
- *Mechanism for rejection, fixing, retesting, etc.:* These provisions also should be detailed in writing and should address time periods for each party to comply. At some point in the process, if the application still fails to meet the specifications, the hospital should be able to return the application for a complete refund.
- *Payment holdback:* In order to maintain sufficient leverage to ensure the vendor adequately addresses issues identified during the acceptance testing process, consider structuring the hospital's payment schedule to retain a meaningful payment holdback until after final acceptance.

MAINTENANCE and SUPPORT

Consider the vendor's obligations to support and maintain the application over time:

- *Provision of support:* The vendor should typically provide maintenance and support services unless the hospital receives source code and intends to handle all maintenance and support in-house.
- *Help desk support:* Consider whether the hospital needs continuous all-hours support or only support during defined business hours. Support should include correcting defects, "bug" fixes, updates and upgrades (and such terms should be clearly defined in the agreement). Address whether support will be available to all employees or only designated contacts.
- *Problem resolution procedures:* Define problem severity levels (such as, application non-operational vs. "minor" bug), response times by the vendor, escalation procedures (such as the level of involvement of vendor management) and resolution efforts (such as continuous work until resolution versus effort only during business hours). Establish a minimum service level commitment with set standards.
- *Application upgrade obligations:* If the vendor requires the hospital to install all Application upgrades, address whether the hospital can comply. Consider requiring the vendor to support current and previous versions of the application for a certain period of time. The hospital should clearly understand what updates are included without charge as part of maintenance and support services and what categories of upgrades may require additional license fees. Are updates to reflect government-mandated changes included as part of maintenance and support services?

REGULATORY COMPLIANCE

Establish vendor's obligations to meet all relevant regulatory requirements. Consider:

- *Compliance with laws:* Require vendor compliance with all applicable laws, including but not limited to applicable laws and regulations promulgated by the U.S. Department of Health and Human Services, the U.S. Food and Drug Administration, and federal and state laws governing the privacy of health information, including the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), and the *Health Information Technology for Economic and Clinical Health Act* (HITECH).

Because the exchange of health information in the hospital setting is subject to a wide range of compliance requirements, it will be important to consider a representation that the application is compatible with those requirements, such as HIPAA, as well as that the vendor itself is in compliance with those laws.

HIPAA REQUIREMENTS, INCLUDING BUSINESS ASSOCIATE OBLIGATIONS

Because the application will use, process and store patients' personal medical information, the application will need to be compatible with all HIPAA privacy and security requirements, including the business associate requirements, if the vendor will access patient data as part of its technical support for the application. Consider:

- *Representations regarding HIPAA:* Include representation and warranty that the application is compatible with all requirements of the HIPAA Privacy and Security Rules.
- *Business associate activities:* If the vendor is accessing data as part of the vendor's technical support for the application, or if the application is accessed remotely to provide services, consider whether the vendor is a business associate under HIPAA. If so, the hospital and the vendor also should sign a business associate agreement.

PRICING and PAYMENT

Pricing and payment obligations are core elements of the vendor agreement. Consider:

- *License fee structure:* Examples of license fee structures include: (1) up-front, one time lump sum payment; (2) monthly, quarterly or annual license or subscription fees; and (3) transaction-based fees.
- *Application maintenance fee timing:* Negotiate whether the application maintenance fees start immediately upon execution of the agreement, upon delivery of the application, upon final acceptance of the application by the hospital or following the end of the initial performance warranty period.
- *Other services (such as installation, training, data conversion):* If the hospital obtains optional services, address whether the fees for such services are fixed at a certain amount, at then-current rates or on a time and materials basis.
- *Application license fee increases:* Negotiate up front how license fees will increase over time. It may be preferable to lock in the application license fee perpetually, or to at least set the fees for a certain number of years. After the years elapse, try to establish a cap on fee increases. If the hospital has sufficient negotiating leverage, a most favored pricing clause may be helpful to ensure preferred pricing in the future.
- *Application maintenance fee increases:* If the hospital is unable to lock in the annual maintenance fees for a period of years, then provide that the maintenance fees may increase annually by no more than a certain fixed percentage (or, alternatively, limit increases to changes in the consumer price index).
- *Future changes to hospital's size and requirements:* Once the hospital commits to a particular EHR application vendor, the cost to change vendors in the future can be significant. Therefore, consider building in protections to ensure equitable pricing as the hospital grows and its needs evolve. For example, if the license fees are based on number of users, consider locking in future user fees at a discounted rate.
- *Expense reimbursement:* Include the hospital's standard policies and requirements for reimbursing vendor expenses. Limit reimbursement to reasonable and documented expenses and if appropriate, request a cap on total out-of-pocket expenses.
- *Due date:* Establish a set due date for payments to the vendor, such as 30 days after receipt of invoice or as otherwise required for business reasons.

TERM and TERMINATION

Consider the time period covered by the agreement as well as the specific conditions for terminating the agreement, including early termination. Consider:

- *Term of license:* Consider the business implications of the time period set for the software license, such as agreeing to a perpetual vs. term license, with automatic renewal or a fixed term, taking into account issues such as locking in fee arrangements for a specific period of time, and being required to use software that may become outdated during the term of the license. Address when the license and maintenance periods commence, such as on the effective date of the agreement or upon acceptance by the hospital. Commencement may trigger payment obligations.
- *Termination by vendor:* Limit the vendor's ability to terminate the contract to avoid disruption to the hospital's business. If the vendor can terminate at any time, the hospital may want the vendor to agree to provide maintenance for a certain period of time and/or obtain a right to continue using the application for a certain period of time following termination.
- *Termination by hospital for convenience:* Consider whether the hospital needs the right to terminate the contract for convenience. Where possible, eliminate early termination fees or tie the penalty to specified performance criteria.
- *Termination for breach:* The hospital should have at least 30 days to correct a material breach of the agreement before the vendor may terminate the license. It is standard for this to be mutual.
- *Termination for failure to comply with meaningful use requirements:* Consider whether the hospital wants the right to terminate the contract for failure of the application to meet Stage 1 and/or Stage 2 or 3 meaningful use criteria (see "Certified EHR Technology Standards" on page 3) and/or certification criteria.
- *Effect of termination:* If the vendor will require the hospital to stop using and return or destroy the application, then address whether the hospital will need to keep an archival copy. Each party should return or destroy (at the other party's instruction) the other party's confidential information. Understand whether the hospital's data processed through the application is stored in a universal or proprietary format, since this will impact the ease by which the hospital can transition to another system. Also consider requesting a commitment from the vendor for transition assistance to another application provider following termination.

PROPRIETARY RIGHTS

Consider the ownership rights of the parties to the software application as well as the data held in the EHR:

- *Title to standard software:* In general, the vendor will retain all ownership rights in its application, subject to the license rights granted to the hospital.
- *Title to customized software:* Consider whether the hospital wants to obtain from the vendor ownership rights in certain customizations or other work product developed pursuant to the agreement.
- *Third-party software:* Does the application include any third-party software? If so, the hospital should ensure it has appropriate and sufficient rights to such third-party software. In these cases, the agreement will typically include an attachment with any applicable and relevant licensing terms and restrictions for the third-party software and/or include links to access the relevant licensing terms online. Be aware of any third-party licensing terms and restrictions that may be updated by the third-party provider from time to time and the hospital's obligation to periodically review any changes to the terms.
- *Open source software:* Understand whether the application includes open source software and whether any part of the application is provided pursuant to separate terms of an open source license.
- *Hospital data:* To the extent the vendor will have access to any data input in the application, clarify that the hospital owns all rights in such data and the vendor is limited to using such data as necessary to provide services under the agreement. Depending on the level of vendor access to the data, consider whether the vendor is a HIPAA business associate, which would require the establishment of a compliance business associate relationship (see "HIPAA Requirements" on page 6).

WARRANTIES

Carefully review the guarantees made by the vendor to ensure the application performs as expected, and the vendor's obligations if it does not. Consider:

- *Warranty of performance:* The vendor should warrant that the application will perform substantially in accordance with its written specifications. The duration of this warranty is usually negotiable, often ranging between 30 – 180 days.
- *Specifications:* Performance is generally warranted against the contracted specifications. Make sure these specifications are detailed enough so that when a problem arises with the application, the hospital has a clear standard against which to measure application performance. Alternatively, the information may be contained in the “documentation.”
- *Remedies for breach of warranty of performance:* The vendor may try to limit remedies to replacement, repair or refund. If so, make sure the refund option is included.
- *Warranty regarding rights:* The vendor should warrant that it has the rights necessary to enter into the agreement and that licenses granted and use of the application as contemplated will not infringe any third-party rights. This is less critical if the vendor grants a broad intellectual property indemnity as necessary to protect the hospital (see “Indemnity” on this page).
- *Systems integration:* If there may be compatibility issues regarding integration of the application into the hospital's systems, have the vendor warrant systems integration. If the vendor refuses, make sure specifications adequately address compatibility requirements.
- *Services warranties:* The vendor should warrant that all services provided under the agreement are performed in a professional manner in accordance with industry standards.
- *Third-party warranties:* To the extent the vendor is the beneficiary of any warranties for any third-party software or hardware it provides to the hospital under the agreement, require the vendor to pass through the benefit of those warranties to the hospital.
- *Hospital warranties:* While it is important for the vendor to offer sufficiently robust warranties to make the hospital comfortable licensing the application, the hospital (as the customer) should avoid providing significant warranties. This will help to reduce the hospital's risk of contractual liability from breaching those warranties.

INDEMNITY

Consider obligating the vendor to hold the hospital harmless for certain vendor behaviors, including potential infringement of third-party intellectual property rights and vendor negligence or willful misconduct:

- *Intellectual property infringement indemnity:* The vendor should indemnify the hospital for third-party claims that the application infringes any patent, copyright, trade secret or other proprietary right.
- *Other indemnities:* Depending on the hospital's standard policies regarding indemnification, consider indemnification for injury or damage caused by the negligence or willful misconduct of the vendor.

LIMITATIONS OF LIABILITY

Consider the limitations on the liability of the respective parties for damages related to the application or the agreement:

- *Exclusion of certain types of damages:* The hospital (or alternatively, neither party) should be liable for indirect, incidental, consequential or special damages relating to the agreement or the application. The exception to this general exclusion for the vendor would be for damages in the amount of meaningful use incentive payments not received by the hospital or in the amount of payment reductions imposed on the hospital in 2015 or beyond.
- *Liability cap:* Typically, vendors will limit their liability for direct damages to the amount of fees received for the application and related products and services under the agreement. Sometimes the damages are limited to the amount of fees received in the prior year. The hospital can try to: (1) eliminate the cap; (2) negotiate a mutual cap; or (3) try to raise the cap. **Be sure to exclude the vendor's indemnification obligations and the confidentiality/nondisclosure obligations from the liability cap and exclusion of damages.**
- *Limitations on liability:* Carefully consider efforts by the vendor to limit liability related to meaningful use and related certification.

SOURCE CODE ESCROW

The hospital should consider requiring deposit of the software source code with a third-party escrow agent to ensure that it has access to the source code when the maintenance of the software cannot otherwise be assured by the vendor.

- *Source code escrow:* The hospital should consider requiring the vendor to place the source code for the application in escrow with a third-party escrow provider. The agreement should, at a minimum, specify: (1) the conditions for release of the source code; (2) the vendor's obligation to regularly update the escrow materials throughout the term; and (3) the scope of the hospital's license rights following release. Potential source code release conditions include the vendor's bankruptcy, the vendor ceasing to provide maintenance and support for the application, and the vendor's failure to meet certain critical service level thresholds. The agreement also should specify which party is responsible for the costs of the third-party escrow provider. Note that the vendor already may have a relationship with a source code escrow provider for the benefit of its other customers and, if so, the cost to add the hospital as another beneficiary is usually not significant.
- *Meaningful use:* Consider also including failure of the application to remain compliant with the meaningful use criteria as a condition for releasing the source code.

OTHER ISSUES

Contracts for EHRs also may address additional topics, such as:

- *Confidentiality:* Include standard hospital confidentiality protections.
- *Insurance:* Include the hospital's standard insurance requirements for vendors providing services of this scope.
- *Customer reference/publicity/trademark license:* Include the hospital's standard protections, if any, against the vendor's use of the hospital's name and trademarks for publicity purposes.
- *Miscellaneous provisions:* Include the hospital's other standard contractual provisions, including governing law, dispute resolution, notice, assignment (e.g., consider whether the hospital needs the ability to assign its rights under the agreement following a merger or sale of assets), non-waiver, severability, integration, etc.
- *Arbitration:* Consider whether arbitration is the preferred method for resolving disputes about damages resulting from application's failure to meet meaningful use criteria (see "Certified EHR Technology Standards" on page 3 and "Limitations of Liability" on page 8).



**American Hospital
Association**

155 N. Wacker Dr.
Chicago, Illinois 60606
(312) 422-3000

325 7th Street, N.W.
Washington, DC 20004-2802
(202) 638-1100