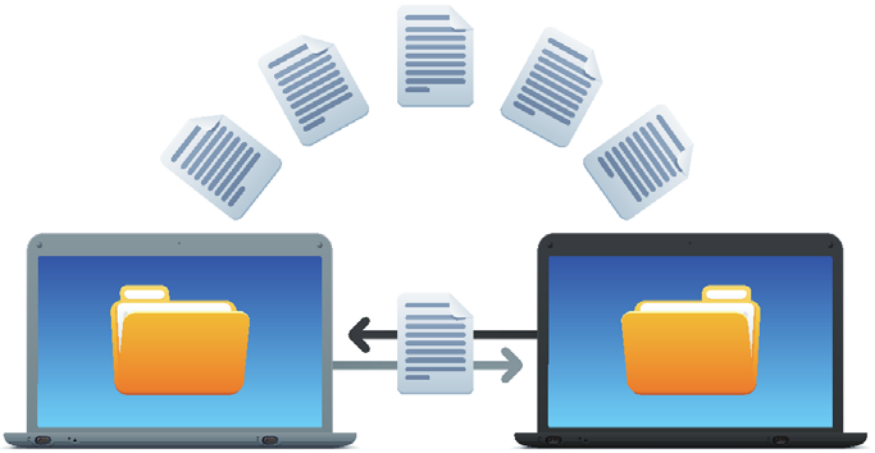
BY DANIEL F. SHAY, ESQ. AND ALICE G. GOSFIELD, ESQ.

# EHR data control: a practical primer

**EVERY OTHER MONTH, DERMATOLOGY WORLD** covers legal issues in "Legally Speaking." This month's authors, attorneys Daniel F. Shay, Esq. and Alice G. Gosfield, Esq., are health care attorneys at Alice G. Gosfield and Associates, P.C.



There are a range of concerns when selecting and implementing an electronic health records (EHR) system: choosing the right one, considering its impact on practice productivity in the short and long term, and return on investment, to name a few.

There is also the negotiation process and the review of the end-user license agreement (or "EULA"), which may delay implementation as the practice and the vendor negotiate contract terms. However, the review of the EULA is an important early step in EHR implementation. It is at this stage that critical issues, such as those of data control and ownership, should be addressed. For a more general overview of evaluating EHR software, as well as common EULA terms and an analysis of the Medicare EHR incentive program, see the section of the Academy's "HIT Kit" on EHR implementation, located at www.aad.org/member-tools-and-benefits/practice-management-resources/hit-kit/ehr-implementation.

## DATA CONTROL: THE BASICS

What is "data control?" In a very basic sense, "data control" applies to the question of who owns, has access to, and has the ability to manipulate or otherwise use data which populates the EHR. To what "data" does the concept refer? Put simply, the "data" in question is the information generated by the practice's use of software. This may be granular, specific bits of information, such as a patient's name, address, age, etc. It may include larger blocs of data, such as progress notes, orders for laboratory studies, or prescription orders. It may also apply to data drawn from information practice personnel enter, as well as data that is de-identified, aggregated, and collated for further use, such as prescribing habits for certain demographic blocs, frequency of billed services, etc.

Not surprisingly, this information can have independent commercial value, as well as value from a practice compliance perspective. (We discuss this in depth on our website at www.gosfield.com/PDF/Ch5Shay.pdf .) For example, pharmaceutical companies will pay to know

a physician's prescribing habits. The billing records of the practice — and billing patterns derived from them — may prove essential in responding to insurer audits or investigations, or in addressing potential overpayments. Vendors often want access to this data, specifically because of its commercial value when de-identified and aggregated.

## STRUCTURAL CONSIDERATIONS

Depending on the nature of the software involved, actual control over and access to the data may vary. For example, with Web-based software, the data (or at least a copy of it) is likely not stored on the practice's computers, especially when the software includes a remotely provided practice management component, such as data storage, billing, or computerized order entry. Because it needs access to the data to provide these services, the vendor will retain the data on its servers.

By contrast, if the software is resident on the practice's computers, the vendor will likely lack direct access to the data. The vendor may still, however, be able to access the data indirectly or remotely. For example, software resident on a practice's computer might still require an internet connection (similar to how Microsoft Windows requires such a connection to activate the software and push updates to the software). With such a connection, a vendor might be able to access the data through a built-in "back door" in the software itself.

The major benefit of the data being resident on the practice's computers, however, is that the practice has more ability to retain its data, and restrict vendor access if it chooses to. Moreover, the vendor has far less ability to "hold the data hostage" in the event of a contractual dispute. There may be tradeoffs, however. The software may offer limited options for remote access, which may mean the loss of access to the software from home, or may require a separate copy to be installed on a home computer (which can increase the cost of the software). A Web-based system suffers no such restrictions; access can be had from any computer with a compatible Web browser. In addition, the practice may lose the benefit of additional vendor services, if data is stored locally and the vendor has no access to it.

## POINTS OF CONFLICT AND CONTRACT ISSUES

Three common areas of conflict may present themselves with respect to data control and ownership: (1) vendor use of practice data, (2) vendor audits of practice data, and (3) post-termination access to records. The best time to address these issues is during the negotiation process, before signing the EULA.

*1. Vendor use*

As noted above, vendors often want access to practice data, due to its commercial value. If the vendor intends to use the data, the EULA should specifically state as much. Such use of the data should also be only in a form rendering it "de-identified" within the definition of the HIPAA regulations. Moreover, the practice should receive something for the vendor's use of its data. This may be a value-added service, such as the vendor using de-identified data to create clinical decision-making tools within the software, or it may take the form of a price decrease (or, more likely, a price increase if you refuse the vendor access to the data).

Assuming the matter is addressed in the EULA, the language may read something like this:

> *Practice grants Vendor a nonexclusive license to use the Practice Data, in de-identified format in accordance with the definition of "de-identified" under 42 CFR 164.514. In exchange, Vendor shall grant Practice use of Vendor's Clinical Quality Decision-Making Database ("CQDM Database") described in Exhibit C, attached hereto and incorporated by reference herein. Practice may refuse to grant Vendor access to such data, but Vendor shall not grant Practice the use of the CQDM Database.*

In this case, the language means that the vendor has the right to use de-identified practice data. The practice can refuse, but it will lose access to the vendor's clinical decision-making tools. Note that the language above does not describe the specific use of the data. Practices may want to inquire how their data — even if de-identified — may be used. Even if a practice has no objections to permitting the vendor to use such data, it may want to use the data for similar purposes. Without knowing how the vendor intends to use the data, the practice could find itself in competition with the vendor in the commercialization of its own data.

An alternative, more practice-friendly approach to data usage and ownership would look as follows:

> *All business data obtained or created by Practice is the property of Practice, including patient clinical, financial, and insurance-related information. Vendor may, in the fulfillment of its duties, access Practice's data. At no time shall Vendor copy or otherwise use any data obtained or created by Practice, without Practice's explicit consent. Vendor shall maintain the exclusive ownership of all rights, title, and interest in and to the Software, Documentation, and other material provided by Vendor to Practice under this Agreement, and this Agreement does not provide Practice with title or ownership of the Software, Documentation, or other materials provided by Vendor to Practice hereunder.*

In this case, the vendor can only use the practice's data with the practice's explicit permission. This gives the practice leverage. This type of language, however, is far less common.

*2. Vendor audit*

In some cases, vendors may either offer auditing services/software functions, or demand that the practice permit the vendor to audit the practice's records. The latter is more likely to be seen when dealing with an arrangement such as a health information exchange (HIE) or an organized health care arrangement (OHCA). These concepts involve otherwise disparate health care providers who may treat the same patient population, and therefore share electronic health records across a network. For example, a hospital system may provide EHR software to practices treating patients within the hospital's system, thereby facilitating the sharing of records and improving continuity of care. A EULA for such an arrangement may include language such as:

> *Corporation reserves the right to audit, remotely or otherwise, use of the System by the Practice and its Authorized Personnel. Such audits will be conducted to ensure compliance with the provisions of this Agreement and Confidentiality Agreements. Suspected breaches, including without limitation any unauthorized use of the System, will be investigated promptly, and the Practice shall cooperate fully in connection with any such investigation.*

The organizing entity is acting as the business associate of all of the various providers to which it gives the EHR software. Thus, it must ensure the privacy and security of those providers' records. This, in turn, may require the organizing entity to periodically audit providers' records to ensure no unauthorized access has occurred. Such audits are, in theory, beneficial to the provider, and should not be viewed as a "hostile" audit (such as a government audit of billing records). The goal here is to ensure that the practice's records are protected, and that those with access to the software are using it properly.

In other cases, a software vendor may offer auditing services to assist the practice, or may tout the auditing functions offered by its software. This does not necessarily mean that the vendor will audit without the practice's permission, nor should it. When the vendor is providing data storage and/or other practice management services, the vendor is, again, acting as the business associate of the practice. Unless the practice otherwise authorizes it, the vendor should therefore not audit practice records of its own volition.

*3. Post-termination use*

The last, and possibly most important, aspect of data control relates to handling of post-termination data. When a software license agreement terminates, the practice will usually be required to return the software (if it was installed on practice computers) or will simply lose access to the software. When this happens, the practice's data will need to be returned and may need to be converted to a format readable outside of the software. The EULA should address this. For example:

> *At any time during the Term upon written request by the Practice and without request upon termination or expiration of this Agreement, within thirty (30) days of receipt by Vendor of a payment of a $XXX fee, Vendor shall send the Practice an electronic file of the Practice Data in a commercially reasonable flat file format on commercially reasonable media. After the thirty (30) day period commencing on the date of termination or expiration of this Agreement, Vendor shall have no obligation to maintain any copies of or provide any copies of the Practice data, except as otherwise required by law.*

The language in this section includes a common feature of EULAs: a cost for data conversion. This is not unreasonable. "Flat file format" is industry jargon for a neutral, basic text format; in some cases, practices may request a specific file format (such as a searchable PDF) for the data, but that may come with additional charges. As a practical matter, the vendor likely will want to rid itself of the practice's data (and free up server space) as soon as possible, but may be bound by the terms of a HIPAA business associate agreement to maintain the data. Bear in mind that state laws often require practices to maintain records for a specific number of years, so practices have a legal duty to obtain copies of the data even after termination.

Another consideration is what happens if there is a dispute about fees owed by the practice, and the vendor refuses to release the data. This poses a practical problem for practice owners: do they fight the dispute out in court, or pay what the vendor demands? As distasteful as it may be, in some cases the smart move is to pay what the vendor demands, simply because doing so may ultimately be less expensive than litigating, and will almost certainly achieve faster results. In any case, the EULA should clearly address the process by which data will be converted and returned to the practice.

As discussed above, the right time to address these issues is during the negotiation process following a practice's review of the EULA. It is far easier to plan for the future than it is to resolve a dispute in the present when the EULA itself is imprecise. The EULA can provide a roadmap for how to handle issues of data control and data ownership, and when precisely drafted, can do so in a way that benefits — or at least identifies disadvantages to — the practice. ***dw***