Health Law Advisory

March 29, 2013 • Julie A. Knutson, Editor

BAIRD HOLM LLP
ATTORNEYS AT LAW

Data Hosting: A New Venture with New Risks

Hospitals and health care organizations are more frequently hosting data or back-up data at off-site data locations. While segregating data by hosting data off site is generally an advisable risk management strategy, hospitals have also entered arrangements to host data for third parties (including other hospitals). This practice may leave the hosting hospital exposed to unanticipated liability if the third-parties' data is breached, lost or destroyed.

There are many different types of data "hosting" arrangements, including the following:

1. The hosting site leases space at its location to the third party (similar to any other landlord-tenant relationship); the third-party is responsible for securing and maintaining the data stored in the leased space and purchasing and maintaining all equipment.

2. The hosting site leases both the space and the equipment to the third party; there is no co-mingling of data and the third party is responsible for securing and maintaining the data stored in the leased space and maintaining the equipment.

3. The hosting site provides space, equipment and IT consultation to the third party; however data remains independent.

4. The hosting site provides complete managed data hosting, including space, equipment and consultation; data may reside on the same servers or in the same space. All of the above.

When hospitals or other organizations enter any type of hosting arrangement, they need to carefully consider the agreement language and closely examine their insurance policies. First, the parties entering such agreements should spell out the responsibilities of each party in detail. Next, the parties need to consider who is liable if something were to go wrong. For example, what happens if a server goes down or there is

Also in this issue

a utility interruption? What if a virus spreads from the hosting site's data to the third-party data? Who is responsible for backup/recovery services? Last, the parties need to manage these exposures and, when possible, insure against their effects. Accordingly, the agreements should specify how exposures will be managed and the type(s) of insurance each party is obligated to carry.

While the hosting hospital may have cyber liability coverage, generally such cyber coverage will only cover the hospital for loss of its own data. Depending on the nature of the hosting arrangement, the hosting hospital may need to purchase additional technology business insurance, such as a Technology Errors and Omissions (E&O) policy. Technology E&O professional liability insurance protects an organization if the third-party storing data alleges the hosting site is responsible for technological errors, or fails to perform as stated in the agreement.

Technology E&O insurance is often confused with cyber insurance or privacy insurance. While this type of professional liability insurance has previously been reserved for IT companies, when a non-IT company such as a hospital takes on responsibilities such as data hosting, they now become a target for IT related claims. Most general commercial policies or traditional cyber insurance policies will not cover programming errors, security breach of third-party information, or third-party data loss. Technology E&O policies generally cover liability and property loss to a third-party resulting from (1) an act or omission committed in the course of the insureds' performance of services for the third-party or (2) failure of an insured's product to perform as intended or expected. Note that many of these policies will contain stipulations that minimum level of risk controls be in place. Hosting data may provide additional revenue to the organization; however the risk control obligations can create significant challenges to an organization that does not typically perform this type of service.

Not all risks can be covered by insurance. It is important to understand the definitions of products and services in the policy and any exclusions. Exclusions in these types of policies are many and varied, so each party needs to understand both coverage and exclusions. The scope of many insurance agents are unfamiliar with advising insureds about this emerging risk. The parties should seek out expert advisors who will identify the risk issues and knowledgeably compare coverage optims. ■

John Marshall
Torri Criger, JD
Silverstone Group

Commentary on HIPAA Security and Data Hosting Agreements

The decision to enter into an arrangement to have another organization host your data will be driven by a number of factors such as: resource availability, technical considerations, location diversity, and cost. One of the factors which must be considered is the HIPAA Security Rule.

If the hosting arrangement is for backup purposes, it can be the cornerstone of your *data backup, disaster recovery and contingency operations plans,* which are all required to meet the *Contingency plan* HIPAA Security Rule safeguard (45 CFR § 164.308(a)(7)). If the hosting arrangement is for production purposes, then you will be dependent on the policies, procedures, and practices of the host facility in order to meet many of the Security Rule safeguards.

Regardless of whether the hosting arrangement is for backup or production purposes, you will need to update your security *Risk Analysis* (45 CFR § 164.308(a)(1)) to address the hosting arrangement. In addition, you will need to have a written agreement clearly articulating the obligations of the host facility, allocating the risks attendant to the hosting arrangement, and specifying the required insurance coverages for each party as pointed out in the Silverstone article.

Finally, if you enter into a hosting arrangement (including cloud-based), the host facility is your business associate. If the host facility refuses to sign a business associate agreement, do not use it. ■

James E. O'Connor
Technology and Intellectual Property Practice Group

Governmental Hospitals and Section 501(r) Compliance

Over the past few months, we have received a number of calls from representatives of governmental hospitals inquiring about the application of section 501(r) of the Internal Revenue Code to their respective organizations. Some governmental hospitals have assumed that, because they are not obligated to file a Form 990, 501(r) does not apply to them. If a governmental hospital also has 501(c)(3) status, this assumption is inaccurate.

Section 501(r) was added to the Code by the Affordable Care Act and includes five new standards hospitals must satisfy to maintain their tax-exempt status under section 501(c)(3) of the Code. Most notable are the provisions regarding the performance of community health needs assessments, the implementation of financial assistance and collections policies to include specific provisions required by the statute, and the limitation on charges to patients who qualify for assistance under a hospital's financial assistance policy.

When the Act passed, there was some uncertainty as to the application of the Act to governmental hospitals that also maintain separate 501(c)(3) status. These governmental hospitals are known as "dual status" hospitals due to the fact that governmental entities are also exempt from federal income tax under section 115 of the Code. Even though they are exempt from federal income tax, dual status governmental hospitals traditionally elected to obtain separate 501(c)(3) status in order to offer certain employee benefit plans that were historically unavailable to non-501(c)(3) entities.

Notice 2011-52, published by the IRS on July 7, 2011, clarified and confirmed the IRS's position on this point. According to the Notice, the requirements of section 501(r) apply to dual status governmental hospitals. Thus, dual status governmental hospitals are required to comply and should be complying with section 501(r). This includes the timely performance of a community health needs assessment and the establishment of compliant charity care and collections policies.[1]

It remains unclear how the IRS intends to obtain information as to the compliance of dual status governmental hospitals with 501(r). The IRS has indicated that it intends to monitor compliance with 501(r) through desk reviews of filed 990s and potential audit referrals based upon responses to various questions and the contents of the Form. However, traditionally, governmental entities are not required to file 990s with the IRS. Notice 2011-52 further confirmed that, while 501(c)(3) governmental hospitals are subject to section 501(r), section 501(r) did not otherwise change the Form 990 reporting exemption. Thus, those governmental hospitals that are currently exempt from filing 990s continue to enjoy that exemption.

Nonetheless, if a dual status hospital's 501(c)(3) exemption is revoked due to a failure to comply with section 501(r), it could have serious consequences on the hospital's employee benefit plans. Governmental hospitals should first determine whether they maintain separate 501(c)(3) status. If so, the hospital should ensure that it is compliant with the terms and conditions of section 501(r). For hospitals that are unsure whether they have dual status, if you maintain a 403(b) employee benefit plan, you almost certainly have 501(c)(3) status. Doubts may be resolved by calling the IRS exempt organization helpline with your employer identification number. IRS staff should be able to confirm whether your organization has separate 501(c)(3) status.

It is hoped that the IRS may exempt dual status governmental hospitals from the requirements of 501(r), but the IRS has noted that the statute does not provide them with the authority to do so. Unless and until the IRS formulates an acceptable workaround that alleviates some or all of the 501(r) requirements from dual status hospitals, those hospitals should immediately take the steps necessary to comply with the terms and conditions imposed by 501(r). ■

Andrew D. Kloeckner

1 Hospitals should be complying with the financial assistance, collections and limitation on charges provisions of 501(r) at this time. A community health needs assessment must be performed and adopted at least once every three years beginning on the date of the Act's enactment. The community health needs assessment should be performed in accordance with the provisions in Notice 2011-52.

CMS Finalizes Physician Payment Sunshine Regulations

In early February, the Centers for Medicare & Medicaid Services (CMS) issued regulations implementing the Physician Payments Sunshine Act, one of several Affordable Care Act mandates intended to create additional transparency in the health care market.

The Sunshine Act requires manufacturers of drugs, devices, biological, and medical supplies covered by Medicare, Medicaid, or the Children's Health Insurance Program (CHIP) to report payments or other transfers of value made to physicians and teaching hospitals. CMS will post this data on a publicly accessible website. Manufacturers and group purchasing organizations (GPOs) are also required to disclose certain ownership and investment information to CMS.

The final rule establishes procedures for submitting annual reports to CMS and incorporates a delay in the implementation schedule in order to give manufacturers and GPOs additional time to prepare for required disclosures. Entities covered by the Sunshine Act must begin collecting data by August 1, 2013, and will report data for August through December 2013 to CMS by March 31, 2014. The agency must release data by September 30, 2014.

Outside of certain narrow circumstances, drug and device manufacturers operating in the United States generally must report all transfers of value to physicians and teaching hospitals, including transfers unrelated to covered products. Failure to report as required by the Sunshine Act subjects the violator to civil monetary penalties of up to $150,000 annually, or up to $1 million annually for intentional violations.

CMS defines a "covered product" as one for which payment is available under Medicare, Medicaid, or CHIP and which requires a prescription or premarket approval by or notice to the Food and Drug Administration (FDA). Payment is considered "available" whether made individually for the specific item or as part of bundled payment—e.g. the hospital inpatient prospective payment system. Over-the-counter prescription drugs and medical devices that do not require premarket approval or notification to the FDA are excluded from this definition.

"Covered recipients" include any teaching hospital that receives Medicare payments for indirect medical education (IME), direct graduate medical education, or psychiatric hospital IME, as well as doctors of medicine and osteopathy, dentists, podiatrists, optometrists, and chiropractors. Physician residents and bona fide employees of drug or device manufacturers are not covered.

Manufacturers are not required to report transfers of items valued at less than $10, so long as the aggregate amount transferred to a given covered recipient does not exceed $100 annually. Items worth $10 or less which are provided at events open to the public are exempt from disclosure and do not need to be tracked. Any item worth more than $10, however, must be tracked.

Educational materials that directly benefit patients or are intended for patient use are exempt from reporting. CMS indicated in the final rule that while this category is meant to be interpreted broadly, it is not without limits. Wall hangings and anatomical models which are intended to be used with patients are not subject to disclosure; journals and textbooks meant for physician use are not included, even though such use may eventually benefit patients.

Other items excluded from reporting are discounts and rebates; in-kind items provided for charity care; product samples; certain short-term loans of covered devices; and items or services provided as part of a contractual warranty.

Although the Sunshine Act does not place a reporting obligation on health care providers, the greater transparency it creates may expose providers and hospitals to increased risk under fraud and abuse laws, federal regulations on conflicts in clinical research, and patient injury lawsuits involving medical device or drug safety. Providers who are covered recipients should prepare to respond to manufacturers and GPOs to confirm receipt of payments, transfers of value, and ownership and investment interests. In addition, covered recipients should review their internal compliance policies to ensure that existing procedures identify impermissible conflicts of interest and adequately manage conflicts. ■

Whitney C. West

Upcoming Speaking Engagements

Barbara Person will present at the NHIMA Annual Convention in Kearney, NE, "Stage II Meaningful Use," April 18, 2013.

John R. Holdenried will present during the AHLA Fair Market Value Bootcamp Webinar and Roundtable Discussion on April 24, 2013.

Vickie B. Ahlers will present at several Meetings and Conferences this spring:

- IMGMA Spring Conference, "HITECH Final Regulations and Enforcement," May 9, 2013
- ISHA Spring Conference, "The Next Decade of HIPAA: Understanding and Implementing the Omnibus Final Rule," May 14, 2013
- Nebraska HIMSS Spring Meeting, "HIPAA Privacy Update," May 21, 2013
- Nebraska Hospital Association Mid-Year Meeting, "Scary Situations: Protecting Your Hospital from Violent Patients, Employees or Visitors," May 23, 2013 (co-presenting with Heidi Guttau-Fox)
- Nebraska IT Symposium, "The Cloud...and Its Legal Linings," May 23, 2013 (co-presenting with James E. O'Connor)

Julie A. Knutson and Michael W. Chase will present at the Nebraska MGMA Spring Meeting, "It Can Happen in Your Office: How to Prepare for and Respond to Investigations and Audits," May 10, 2013. ■

Health Care Group

Vickie Brady Ahlers
402.636.8230
vahlers@bairdholm.com

Michael W. Chase
402.636.8326
mchase@bairdholm.com

Alex (Kelly) M. Clarke
402.636.8204
kclarke@bairdholm.com

John R. Holdenried
402.636.8201
jholdenried@bairdholm.com

Andrew D. Kloeckner
402.636.8222
akloeckner@bairdholm.com

Julie A. Knutson
402.636.8327
jknutson@bairdholm.com

Barbara E. Person
402.636.8224
bperson@bairdholm.com

Whitney C. West
402.636.8353
wwest@bairdholm.com

All attorneys are admitted to practice in Nebraska and Iowa unless otherwise noted.

Health Law Advisory is intended for distribution to our clients and to others who have asked to be on our distribution list. If you wish to be removed from the distribution list, please notify healthupdate@bairdholm.com.

Baird Holm

1700 Farnam St
Suite 1500
Omaha, NE 68102

402.344.0500
402.344.0588

www.bairdholm.com