AMERICAN BANKRUPTCY INSTITUTE

2018 Mid-Atlantic Bankruptcy Workshop

Fallout of Health Care Consolidation: Who Will Be the Winners and Losers?

Suzanne A. Koenig, Moderator
SAK Management Services, LLC; Northfield, Ill.

Hon. Paul M. Black
U.S. Bankruptcy Court (W.D. Va.); Roanoke

Peter C. Chadwick
Berkeley Research Group, LLC; Washington, D.C.

David N. Crapo
Gibbons P.C.; Newark, N.J.

Warren J. Martin, Jr.
Porzio, Bromberg & Newman, P.C.; Morristown, N.J.

CONCURRENT SESSION

2018

HIPAA, HIPAA BREACHES AND THE REORGANIZATION OF THE HEALTHCARE DEBTOR

David N. Crapo
Gibbons P.C.
Newark, New Jersey

Introduction. The past twenty years has witnessed an exponential increase in consolidations of all types—whether by merger or acquisition—among healthcare providers and insurers. Some commentators opine that consolidation will lead to greater efficiency in the delivery of healthcare. However, other commentators fret over increasing healthcare costs and limits on the availability of necessary treatment they resulting from those consolidations.

Bankruptcy has functioned effectively as a tool for healthcare consolidations. In New Jersey, for example, bankruptcy has been utilized to facilitate the consolidation of five hospitals to other entities during the last eleven years by means of § 363 sales. Most recently (2016), Prime Healthcare Services acquired St. Michael's Medical Center in Newark. Previously, Christ Hospital in Jersey City (2013), Hoboken University Hospital (2011) and Bayonne Medical Center (2008) had been acquired through § 363 sales and are now owned by CarePoint Health. In 2007, St. Mary's Hospital Passaic (which was acquired by Prime Healthcare Services and renamed St. Mary's General Hospital in 2014) acquired PBI Regional Medical Center (which had resulted from a merger of Passaic Beth Israel Hospital and General Hospital Center at Passaic in 2004) through the latter's bankruptcy case.

It appears that healthcare provider consolidations will continue. Bankruptcy has been and will continue to be a useful tool to facilitate those consolidations. In point of fact, the Bankruptcy Code expressly contemplates the reorganization of a debtor through consolidation with another entity, whether by sale, merger or some other means. 11 U.S.C. § 1123(b)(5)(B) and (C). Laws regulating health care providers and insurers, however significantly impact the reorganization of healthcare debtors. One of those health laws is the Health Insurance Portability and Accounting Act of 1996, as it has been amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (hereafter, as so amended, "HIPAA"). This article will address recent developments concerning the impact of HIPAA on the reorganization of the healthcare debtor. More particularly, this article will address the impact of a significant HIPAA data privacy and security breach on a healthcare debtor's bankruptcy as well as HIPAA's impact

on the consolidation of a healthcare debtor (or, more accurately, divisions and operating units of such a debtor) with one or more entities through a bankruptcy sale process.

HIPAA Applies in Bankruptcy. Bankruptcy practitioners—and even bankruptcy judges—often assume that bankruptcy law takes precedence over other areas of the law. However, appellate courts, including the Supreme Court, have repeatedly held in various contexts that that is not always the case. Indeed, trustees in bankruptcy and debtors-in-possession must conduct the debtor's operations in accordance with applicable non-bankruptcy law.[1] For example, it is now well established that debtors and trustees must comply with environmental laws, even if they can avoid paying in full the related monetary claims. Similarly debtors and trustees must comply with HIPAA and protect the privacy and security of the individually identifiable health-related information protected by HIPAA (hereafter, "PHI").[2] For that reason, HIPAA can, and sometimes does, significantly impact the manner by which a healthcare debtor can reorganize, including any proposed consolidation of the debtor-healthcare debtor with another entity by sale, merger or another method

HIPAA Data Breaches. HIPAA's impact on the reorganization of healthcare debtors should come as no surprise and is likely to become even more important with the increase in data security breaches at healthcare providers and other participants in the healthcare industry. Indeed, it is common knowledge that: (i) PHI is valuable, even more valuable than easily replaceable credit card information; (ii) the value of PHI makes healthcare providers (and healthcare insurers) tempting targets for hackers; and (iii) healthcare providers still remain relatively unprepared to thwart hacking attacks. The explosion in the use of mobile electronic devices like smartphones by healthcare personnel in providing healthcare and the connection of smart medical devices (*e.g.*, infusion pumps, defibrillators or pacemakers) to healthcare providers' information systems, other medical devices, the internet and patients' smartphones have only increased the vulnerability of participants in the healthcare industry to hacking.[3] As if

---

[1] 28 U.S.C. § 959(b).

[2] It can never be overemphasized that, in addition to information of an indisputably medical nature, PHI also includes related demographic and financial information (e.g., addresses, social security numbers and credit card information) concerning an individual. *See* 45 CFR § 164.514(b)(2)(i) (listing identifiers the removal of which will "de-identify" PHI).

[3] In 2017, for example, the FDA determined that radio frequency enabled implantable cardiac pacemakers manufactured by St. Jude Medical, which allowed for the device to be monitored or controlled over the internet,

the vulnerability to hacking was not enough, the actions of negligent (but often well-meaning),[4] poorly trained (*e.g.*, the employee who clicks on a link and facilitates a phishing attack) or rogue[5] employees can lead to either a cyberattack by a hacker or some other unauthorized use or disclosure of PHI.

Numerous healthcare providers—and even large, well-financed and sophisticated insurers—have, in fact, suffered data privacy and security breaches—including the well-publicized cyberattacks—in the last few years, impacting substantial—even eye-popping—numbers of individuals. For example, 2015 has been called the year of the healthcare cyberattack. During that year the most significant healthcare data privacy and security breaches to date occurred or, more accurately, were discovered. Those breaches include:

- **Anthem, Inc.,** the largest U.S. health insurer: almost 79 million people impacted;
- **Premera Blue Cross**: approximately 11 million people impacted;
- **Excellus Blue Cross Blue Shield**: 7 million people impacted;
- **UCLA Health System**: approximately 4.5 million people impacted;
- **Medical Informatics Engineering**, a provider of medical data sharing and transmission services: approximately 3.9 million people impacted; and
- **CareFirst Blue Cross Blue Shield:** approximately 1.1 million people impacted.

More disruptive to healthcare operations than cyberattacks by which the perpetrators seek information are ransomware attacks where data is encrypted and held for ransom. A ransomware attack can shut down the operations of a modern hospital, putting the health, lives and safety of patients at risk. In large part because patient health and safety concerns incent

---

were vulnerable to cybersecurity intrusions or exploits. *See* https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (retrieved on June 2, 2018).

[4] For example, in a well-meaning but misguided attempt to improve healthcare, resident physicians at St. Elizabeth's Medical Center in Brighton, MA used an internet site to share files, thereby exposing PHI to unauthorized viewers. *See* the Resolution Agreement and the Corrective Action Plan at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html (retrieved on June 2, 2018).

[5] *See, e.g.*, Snell, Elizabeth, "Healthcare Data Breach Leads to Identity Theft Guilty Plea," *Health IT Security: Patient Privacy Security News* (March 30, 2018) at https://healthitsecurity.com/news/healthcare-data-breach-leads-to-identity-theft-guilty-plea (retrieved on June 2, 2018) (former hospital employee participated in conspiracy to steal PHI as part of an identity theft racket).

hospitals and other healthcare providers to pay ransoms to hackers, healthcare providers have become the most attractive targets for ransomware attacks.[6]

In one of the earliest reported ransomware attacks on a major U.S. healthcare provider, Hollywood Presbyterian Medical Center suffered a ransomware attack in February, 2016 and paid a ransom of $17,000 to regain access to its records. A month later, MedStar Health suffered a ransomware attack impacting its facilities in the Washington, D.C. metropolitan area. The attack forced MedStar Health's ten hospitals and more than 250 outpatient centers to shut down their computers and email.[7] At that time, the system employed more than 30,000 people and treated hundreds of thousands of patients in the Washington region.[8] Clinicians were forced to resort to paper records until electronic records were recovered or recreated.

Ransomware and similar attacks on healthcare providers and other participants in the healthcare industry continued unabated through 2017 and into 2018. Nuance, a major provider of voice and language tools to the healthcare industry, was knocked offline by the Petya virus.[9] Although masked as ransomware, the purpose of the virus is the disruption and destruction of data.[10] In response to the attack, Nuance offered alternative products to its customers.[11] Pharmaceutical giant Merck also suffered an attack of the Petya virus during 2017.[12] Starting January 18, 2018, the services of Allscripts, the electronic health record giant, were shut down for a week by the SamSam ransomware attack. The shutdown at Allscripts prevented Allscripts clients, including numerous healthcare providers, from accessing PHI and was followed a week

---

[6] *See, e.g.*, Donovan, Fred, "Healthcare Industry Takes Brunt of Ransomware Attacks," *Health IT Security: Cybersecurity News*, May 3, 2018 at https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks (retrieved on June 2, 2018).

[7] Cox, John Woodrow, "MedStar Health Turns Away Patients after a Likely Cyberattack," *The Washington Post* (March 29, 2016) https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html?utm_term=.c02162dd82f1 (retrieved on June 1, 2018).

[8] *Id.*

[9] Davis, Jessica, "Nuance Knocked Offline by Ransomware Attacking Europe," *Healthcare IT News* (June 28, 2017) at http://www.healthcareitnews.com/news/nuance-knocked-offline-ransomware-attacking-europe (retrieved on June 2, 2018)

[10] Davis, Jessica, "Nuance Still Down after Petya Cyberattack, Offers Customers Alternative Tools," *Healthcare IT News* (June 29, 2017) at http://www.healthcareitnews.com/news/nuance-still-down-after-petya-cyberattack-offers-customers-alternative-tools (Retrieved June 2, 2018).

[11] *Id.*

[12] Shabban, Hamza and Nakashima, Ellen, "Pharmaceutical Giant Rocked by Ransomware Attack," *The Washington Post* (June 27, 2017) at https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/?noredirect=on&utm_term=.954a42822783 (retrieved June 2, 2018)

later by litigation against Allscripts by clients for damages they allegedly suffered from the disruption of their businesses.[13]

In January of 2018, Hancock Health, which is based in Greenfield, Indiana, suffered a ransomware attack, resulting in the shutdown of its entire network.[14] According to a hospital official, the attack was sophisticated and did not result from an employee clicking on an infected e-mail, and appears to have aimed at restricting access to certain parts of Hancock Health's information technology system.[15] In other words according to Hancock Health's CEO, Steve Long, "[t]his [cyberattack] was not a 15-year-old kid sitting in his mother's basement."[16]

HIPAA Settlements and Penalties. Significant HIPAA breaches can result in substantial civil monetary penalties, ranging up to a minimum of $50,000 per violation (with a cap of $1.5 million for identical violations during a calendar year) for violations resulting from willful neglect that remains uncorrected after discovery.[17] Between January 1, 2015 and February 18, 2018, a little over three years, $52,691,000 in civil monetary penalties or (more commonly) settlement payments had been imposed by the Office of Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") on HIPAA-covered entities.[18] HIPAA-covered entities include: (i) covered entities (*i.e.*, health care providers, health plans, and healthcare clearinghouses), (ii) business associates of covered entities; and (iii) the subcontractors of business associates.[19]

To date, the most significant HIPAA settlement payments and civil monetary penalties assessed by OCR have been the following:

---

[13] David, Jessica, "Allscripts Sued over Ransomware Attack, Accused of Wanton Disragard" *Healthcare IT News* (Jan. 26, 2018) at https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/?noredirect=on&utm_term=.954a42822783 (retrieved June 2, 2018).
[14] Davis, Jessica, "Ransomware Attack on Hancock Health Drives Providers to Pen and Paper," *Healthcare IT News* (Jan. 15, 2018) at http://www.healthcareitnews.com/news/ransomware-attack-hancock-health-drives-providers-pen-and-paper (retrieved on June 2, 2018).
[15] *Id.*
[16] *Id.*
[17] *See* 45 CFR § 160.404(b) (setting out the tiered HIPAA civil monetary penalty schedule).
[18] Compliancy Group, "HIPAA Fines Listed by Year," (March, 2018) at https://compliancy-group.com/hipaa-fines-directory-year/ (retrieved on June 1, 2018).
[19] *See* 45 CFR §§ 160.103, 164.104(b) (defining "covered entities" and "business associates").

- **Advocate Health** paid $5.55 million for failing to encrypt laptops and enter into a HIPAA-compliant business associate agreement before disclosing PHI to the business associate;
- **Memorial Healthcare** paid $5 million for impermissibly disclosing PHI to an affiliated medical practice over several years;
- **NY Presbyterian Hospital and Columbia University** paid $4.8 million to settle a claim arising from a physician's deactivation of a server that exposed PHI on the internet;
- **Cignet Health** paid a $4.3 million fine for failing to provide patients with ***access*** to their PHI as required by HIPAA;
- **Children's Med Center of Dallas** paid $3.2 million for theft of unencrypted devices containing PHI;
- **Cardio Net** paid $2.5 million for failing to conduct a sufficient data security risk analysis and implement final HIPAA policies which led to a breach of PHI arising out of a stolen laptop;
- **Memorial Herman** paid $2.4 million for disclosure of ***one*** individual's PHI through a press release; and
- **NY Presbyterian** paid $2.2 million for the disclosure of one individual's PHI (which included visual images of the individual) by allowing a TV crew to film, without the permission of the individual or his family the unsuccessful treatment and death of the individual.

The largest "penalty" for a healthcare-related data security breach did not result from government enforcement, however. In 2017, Anthem, Inc. agreed to pay $115 million to settle litigation resulting from the 2015 breach that had exposed the PHI of almost 79 million people.[20]

HIPAA Liabilities and Bankruptcy: *21st Century Oncology*. Especially considering the attractiveness of healthcare providers to hackers as targets and the significant consequences of a HIPAA breach, the impact of a HIPAA data privacy and security breach on a debtor healthcare provider's reorganization should be of no surprise. It is not beyond the realm of possibility that civil monetary penalties imposed by OCR or a substantial adverse judgment in

[20] Pierson, Brendan, "Anthem to Pay Record $115 Million to Settle US Lawsuits Over Data Breach," *Reuters* (June 23, 2017) at https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML (retrieved on June 1, 2018).

data breach litigation could trigger a healthcare debtor's bankruptcy filing. The dollar amount of a healthcare debtor's HIPAA monetary liabilities (pre- or post-petition) and any related non-monetary obligations or penalties imposed on the debtor could preclude reorganization in any form. Even if the extent of a healthcare debtor's HIPAA-related liabilities does not preclude a reorganization, it certainly could significantly impact the form of such a reorganization.

An example of a case in which substantial HIPAA liabilities were a trigger to a bankruptcy filing and impacted the debtor's reorganization strategy was *In re 21st Century Oncology Holdings, Inc., et al.* (Bankr. S.D.N.Y. Case No. 17-22770 (RDD)). In fact, together with other healthcare laws, HIPAA took center stage in that case. Twenty-First Century Oncology, Inc. ("21CO") suffered a cyberattack in 2015, resulting in the breach of the PHI of 2,213,597 patients. Following an investigation, the OCR concluded that 21CO had violated HIPAA and the HIPAA Privacy and Security Rules by failing to adequately protect, and impermissibly disclosing PHI. OCR asserted claims (collectively, "HIPAA Claims") against 21CO as a result of those breaches exceeding $2.3 million.

Five months before 21CO's bankruptcy filing in 2017, a data breach class action alleging that 21CO had failed to adequately secure PHI under its control was filed against 21CO.[21] Following 2010's bankruptcy filing, data breach claimants filed six class claims aggregating $123.2 million and 180 individual claims (collectively, "Data Breach Claims"). The Data Breach Claims dwarfed in amount the other claims filed against 21CO and its co-debtors (collectively "21CO Debtors"). The 21CO Debtors sought the dismissal of the class claims and valuation of the individual claims at $0 for plan confirmation purposes. In response, the plaintiffs in the class action cases sought either class certification pursuant to Bankruptcy Rule 7023 or, alternatively, for relief from the automatic stay to permit the pre-petition data breach litigation to proceed—albeit with recovery limited to insurance proceeds. Under the circumstances, the 21CO Debtors were facing substantial litigation concerning the Data Breach Claims that could significantly delay or even disrupt their reorganization.

Resolution of the HIPAA and Data Breach Claims was crucial to the 21CO Debtors' successful reorganization. Such a resolution was, in fact, a condition to *both* the consummation

[21] HIPAA does not provide a private cause of action. However, relying on other data privacy and security laws that do provide causes of action, asserting the defendants' HIPAA violations as the factual basis of the claim.

of the 21CO Debtors' Chapter 11 plan[22] *and* the obligation of third parties to backstop a rights-offering for which the plan provided.[23] Resolution of the HIPAA Claims was also necessary to avoid the uncertainty of litigating issues that have not yet been tested by in bankruptcy courts and to obtain significant concessions by OCR on the amount and payment of those claims that would ensure the 21CO Debtors' post-confirmation liquidity . Resolution of the Data Breach Claims was a necessary condition to a meaningful distribution on the claims of other unsecured creditors and required either a substantial reduction in the amount of those claims or for the claims to be channeling to a source of payment, like insurance proceeds, other than the 21CO Debtors' bankruptcy case. Resolution of the Data Breach Claims also allowed the 21CO Debtors to avoid the risks and expense inherent in defending against a class action.

The HIPAA Claims were resolved by means of a Resolution Agreement and a two-year Corrective Action Plan ("CAP").[24] The resolution fixes the 21CO Debtors' monetary liability at $2.3 million settlement, with that amount to be paid directly by the 21CO Debtors' insurer. OCR agreed to release its pre-petition HIPAA Claims upon receipt of the $2.3 million payment and to release its post-petition HIPAA Claims upon 21CO's satisfaction of its obligations under the CAP. Full satisfaction of the 21CO Debtors' obligations under the CAP will result in OCR's waiver of any civil monetary penalty arising out of the HIPAA Claims. The CAP imposes several ongoing obligations on 21CO to ensure HIPAA compliance including, *inter alia*: (i) the review of and revisions to HIPAA policies and procedures and the development of new policies and procedures where necessary; (ii) developing and implementing a program to internally monitor its compliance with the CAP; (iii) retention of an external assessor (at 21CO's expense) to monitor 21CO's compliance with the CAP, with the authority to make unannounced visits to the 21CO facilities; and (iv) annual reporting requirements (with reports attested to by officers of 21CO).

Pursuant to the Data Breach Claim settlement, the holders of Data Breach Claims retain the right to litigate the Data Breach Claims, but agree to look only to certain insurance proceeds

---

[22] *In re 21st Century Oncology Holdings, Inc., et al.* (Bankr. S.D.N.Y. Case No. 17-22770 (RDD), ECF Docket No. 915-1, §9.1(q).
[23] Id., ECF Docket No. 434, §8.1(t).
[24] *In re 21st Century Oncology Holdings, Inc., et al.* (Bankr. S.D.N.Y. Case No. 17-22770 (RDD)), ECF Docket No. 825-1, pp. 5-19. Copies of the Resolution Agreement and CAP can be viewed at and retrieved from https://www.hhs.gov/sites/default/files/21co-ra_cap.pdf .

for recovery and waive any recovery from the Debtors' bankruptcy estates.[25] Upon the approval of the Data Breach Claim settlement, they agreed not to oppose confirmation of the 21CO Debtors' plan.[26]

The 21CO Debtors settled the HIPAA and the Data Breach Claims before the confirmation of their Plan. The bankruptcy court approved the settlements by Orders dated December 11, 2017.[27] The 21CO Debtors' plan was confirmed on January 9, 2018.[28]

21st Century Oncology provides a stark example of the challenges that HIPAA and, more importantly, significant HIPAA data privacy and security breach liabilities can present to the reorganization of a healthcare debtor. Indeed, those liabilities were a significant trigger to the bankruptcy filing. Once the 21CO Debtors had entered bankruptcy, it became clear that the HIPAA and Data Breach Claims had to be resolved if there was to be a reorganization. Luckily for the 21CO Debtors, they had available tools for such a resolution and the case stands as a guide to other healthcare debtors in the same or similar to facing and resolving HIPAA liabilities in bankruptcy.

HIPAA and Bankruptcy Sales: *Medlab* and the HIPAA Privacy Rule. More directly relevant to the impact of HIPAA on the consolidation of healthcare debtors with other entities is the *MedLab* case, which did involve the sale of a debtor. The sale of healthcare providers like MedLab, necessarily includes the sale or transfer of PHI to the purchaser. However, the HIPAA Privacy Rule[29] generally conditions the sale of PHI on the prior written authorization of each patient (or the patient's personal representative) whose PHI is being sold.[30] Obviously, a blanket application of the provisions of the HIPAA Privacy Rule governing the sales of PHI to the sale of a covered entity, or even a unit or division thereof, would effectively preclude such sales. Obtaining authorizations from all of a covered entity's patients—or even the patients of a

[25] *In re 21st* Century *Oncology Holdings, Inc., et al.* (Bankr. S.D.N.Y. Case No. 17-22770 (RDD)) ECF Docket Nol 753.
[26] *Id.*
[27] *Id.*, ECF Docket Nos. 823 and 824.
[28] *In re 21st* Century *Oncology Holdings, Inc., et al.* (Bankr. S.D.N.Y. Case No. 17-22770 (RDD)), ECF Docket No. 915.
[29] 45 C.F.R. §§ 164.500, *et seq.*
[30] 45 CFR § 164.508(a)(4).

division of the covered entity—would be impossible, particularly because HIPAA's protection of PHI extends for fifty years after the patient's death.[31]

To facilitate the sales of covered entities, the HIPAA Privacy Rule excludes from the definition of "sale" the disclosure of PHI "[f]or the sale, transfer, merger, or consolidation of all or part ***of a covered entity*** and for related due diligence as described in . . . the definition ***health care operations***" contained in the HIPAA Privacy Rule.[32] For purposes of the HIPAA Privacy Rule, "health care operations" includes:

> [t]he sale, transfer, merger or consolidation of all or part of the covered entity ***with another covered entity, or with an entity that following such activity will become a covered entity*** and the due diligence related to such activity.[33]

In sum, the HIPAA Privacy Rule expressly facilitates the sale of all or a part of a covered entity (but not a pure asset sale) to either another covered entity or an entity that will become a covered entity following the sale. It follows that the HIPAA Privacy Rule thereby facilitates "reorganizations" by sale and, therefore, the consolidation of healthcare debtors with other entities. However, the HIPAA Privacy Rule's facilitation of the sales of debtors in bankruptcy is subject to some limitations.

Laboratory Partners, Inc., a clinical laboratory network, and several subsidiaries (collectively, "MedLab") filed Chapter 11 petitions with the United States Bankruptcy Court for the District of Delaware on October 25, 2013.[34] At that time MedLab provided clinical laboratory and anatomic pathology services to: (i) a number of skilled nursing facilities ("Long-Term Care Division"); (ii) physicians, physician offices and medical groups; and (iii) Union Hospital, Inc. in Terre Haute and Clinton, Indiana. As health care providers, some or all of the MedLab debtors constitute "covered entities" for purposes HIPAA and the HIPAA Privacy Rule.[35] MedLab proposed to "reorganize," in part, by selling, *inter alia*, its Long-Term Care Division.[36] To that end, on October 30, 2013, MedLab filed a motion for authority to, *inter alia*,

---

[31] *See* 45 CFR § 164.502(f).
[32] 45 CFR § 164.502(a)(5)(ii)(A)(2)(iv) (emphasis added).
[33] 45 CFR 164.501 (paragraph (6)(iv) of the definition of "health care operations).
[34] *In re Laboratory Partners, Inc., et al.*, U.S.B.C. D. Del. Case No. 13-12769-PJW.
[35] *See* the definition of "covered entity" contained in 45 CFR § 160.403.
[36] Id., ECF Docket No. 46, ¶ 6.

sell the Long-Term Care Division ("MedLab Sale Motion").[37] In the MedLab Sale Motion, MedLab acknowledged that, although several potential buyers had expressed interest in purchasing the Long Term Care Division, none of them agreed to be a stalking horse bidder.[38] In sum, the Sale Motion did not identify a specific purchaser of the Long Term Care Division, but proposed the Long Term Care Division be sold at auction.

The proposed form of Asset Purchase Agreement attached as Exhibit B to the Sale Motion provided for the sale of, *inter alia*, "all customer lists, machinery and equipment records, mailing lists, quality control records and procedures, employment and personnel records . . . and display materials" related to the Long-Term Care Division.[39] It is beyond dispute that the customer lists (as well as some of the other assets listed in ¶ 1.1(f)) include PHI.

On December 18, 2013, the United States Department of Health and Human Services ("HHS") filed its Protective Objection to [MedLab] Debtors' Motion for Sale of Substantially All of the Debtors' Assets ("Protective Objection").[40] In the Protective Objection, HHS objected to what it characterized as "an authorized sale of their customer's [PHI] that violates federal law."[41] HHS specifically objected to the sale of customer lists which, according to HHS, "almost certainly contain [PHI]."[42] HHS surmised that MedLab had not obtained authorizations from all patients of the Long Term Care Division before filing the Sale Motion.[43] HHS's primary concern arose out of MedLab's failure to identify a purchaser of the Long Term Care Division.[44] HHS acknowledged that if the Long Term Care Division were sold to a covered entity, HIPAA and the HIPAA Privacy Rule would likely permit the sale of the customer lists.[45] *Id.* In sum, absent being able to identify a purchaser, MedLab could not, as of December 18, 2013, provide HHS the assurance it sought that the purchaser of the Long Term Care Division would be a covered entity—although it would be unlikely that an entity that was not a covered entity would have purchased the Division.

---

[37] *Id.*, ECF Docket No. 46.
[38] *Id.*, ¶ 6.
[39] *In re Laboratory Partners, Inc., et al.*, U.S.B.C. D. Del. Case No. 13-12769-PJW ECF Docket No. 46, Exh. B, ¶ 1.1(f).
[40] *Id.*, ECF Docket No. 216
[41] *Id.*, p.2.
[42] *Id.* p. 3.
[43] *Id.*, p. 4.
[44] *Id.*
[45] *Id.*

The hearing on the sale of the Long-Term Division was adjourned without date and, ultimately, HHS's objection to the sale was resolved. Nevertheless, HHS's objection to the sale of the Long Term Care Division raises questions concerning the potential impact of HIPAA and the HIPAA Privacy Rule on bankruptcy sales. The provisions of the HIPAA Privacy Rule, including the provisions governing sales, are complex. They lend themselves to careful parsing by creative counsel. In that regard, HHS's interpretation of the sale provisions of the HIPAA Privacy Rule seems to require an identified stalking horse bidder that is or will become a covered entity as a result of the purchase of all or a portion of a debtor "covered entity." Such an interpretation effectively precludes straight auction sales—such as that contemplated in the MedLab Sale Motion of all or a portion of a "covered entity" in bankruptcy where the identity of the purchaser cannot be known until a successful bid has been made.[46]

The crucial goals of HIPAA and the HIPAA Privacy Rule, however, can be achieved in straight auction sales without resorting to a hyperliteral reading of the definition of "sale" in the HIPAA Privacy Rule. Debtors (or bankruptcy trustees when appointed) should simply include in the bidding procedures for the sale a requirement that the bidder either be a covered entity or become one as a result of the sale. The bidding procedures should also obligate any bidder receiving PHI in connection with pre-auction due diligence to comply with all relevant obligations undertaken by a business associate under a business associate agreement, and should, at the very least, expressly: (i) require the bidder to protect the privacy and security of any PHI as required by HIPAA and the HIPAA Privacy and Security Rules; (ii) prohibit any use or disclosure of PHI obtained from the debtor in connection with pre-sale due diligence for any purpose other than conducting due diligence; (iii) prohibit the bidder from disclosing PHI to a subcontractor retained to assist in due diligence until that subcontractor has agreed in writing to comply with the obligations of a business associate under a business associate agreement which the bidder itself has agreed to comply in connection with the PHI disclosed; (iv) obligate the bidder to return or destroy the PHI as required by HIPAA and the HIPAA Privacy and Security Rules. Objections should be lodged to bidding procedures that do not contain such requirements. In addition to including the foregoing provisions in the bidding procedures, the debtor (or a

[46] *See* 45 CFR § 164.502(a)(5)(ii)(A)(2)(iv) and 45 CFR 164.501 (paragraph (6)(iv) of the definition of "health care operations) cited above, which clearly contemplate the sale or merger of a specifically identified covered entity with another specifically identified covered entity in a transaction that, it is contemplated will close.

bankruptcy trustee if one has been appointed) should require bidders to execute confidentiality or non-disclosure agreements imposing the applicable obligations of a business associate under a business associate on the bidder, including, at the very least, those set forth above, as a condition to receiving PHI in connection with due diligence. In all circumstances, debtors (or bankruptcy trustees) should limit the disclosure of PHI to a bidder to the minimum amount necessary to conduct due diligence. If the foregoing recommendations are implemented, bankruptcy can remain a useful tool for transferring healthcare business to more viable owners and still ensuring that the crucial policies underlying HIPAA and the HIPAA Privacy Rule are effectuated. In sum, HIPAA and the HIPAA Privacy Rule need not stand in the way of the sale, merger or consummation of the debtor.

Conclusion. Healthcare consolidations are will likely proceed apace for the near future. Bankruptcy can be a useful tool in effectuating consolidations. HIPAA, particularly if the debtor has suffered a HIPAA data privacy and security breach can pose challenges to a healthcare reorganization. Cyberattacks on healthcare entities are not likely to abate in the near future. For that reason, HIPAA will likely increasingly impact healthcare reorganizations. However, *21st Century Oncology* and *MedLab* demonstrate some of the tools available to meet HIPAA's challenges to a healthcare debtor reorganization.

Due Diligence and HIPAA: Issues Pertaining to Complete Disclosure and the Limitations Imposed to Protect Privacy Considerations

Patrick D. Souter
Jenny G. Givens
Gray Reed & McGraw PC
Dallas, TX

Whether it is a stock or asset purchase, merger, joint venture, or other type of transaction, the main precursor to the parties of a transaction entering into binding agreements pertains to the due diligence disclosures made by the parties. Due diligence allows for the parties to exchange and review the information necessary to provide a level of assurance that the parties' expectations and understandings are supported by tangible information. It also allows for each party to verify to their satisfaction whether the other parties to the transaction have the ability to satisfy any representations and warranties or other underlying terms contained in the transaction's definitive documents. Accordingly, its scope is generally customized to the transaction and the parties' needs.

In non-health care transactions, the scope of due diligence may be straightforward and the disclosure of information and documentation to the other parties sufficiently protected by a confidentiality and nondisclosure agreement. However, in health care transactions, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and, in particular, the HIPAA Privacy Rule,[1] imposes impediments to the disclosure of certain patient-related information.

This article describes when HIPAA allows for certain due diligence disclosures and the circumstances when there is not clear guidance on how due diligence may be carried out. Although outside the scope of this article, it also should be noted that there are instances where parties providing due diligence information to competitors as part of a transaction may risk compliance issues under other laws and regulations, such as those governing antitrust.[2]

The Scope of Due Diligence in Health Care Transactions

Due diligence is of utmost importance to health care transactions due to the significant regulatory risks that a party may incur as a result of the previous actions of the other party to the transaction. The areas of information privacy and security, fraud and abuse, billing compliance, antitrust, and licensing and certification are some of the areas of concern to any parties to the transaction. Therefore, due diligence sought in a health care transaction commonly encompasses not only the business information requested in non-health care transactions but also the more expansive information that may address these additional areas of concern.

However, this expansive approach to due diligence may trigger HIPAA compliance concerns.[3] The parties may need to exchange financial information (e.g., including accounts receivable and claims for services rendered), as well as information regarding operational and patient matters such as complaints, adverse events, possible claims or litigation, and compliance matters.

In all of these instances, it may be necessary to disclose patient information that falls within the definition of "Individually Identifiable Health Information" (IIHI)[4] or "Protected Health Information" (PHI).[5] As a general matter, the HIPAA Privacy Rule requires that in the absence of patient authorization for such disclosure, the disclosing "Covered Entity"[6] must establish sufficient safeguards to protect PHI and establishes limits as to what PHI may be disclosed and when.[7]

Due Diligence and Permissible Disclosure Under "Health Care Operations"

In addition to establishing restrictions on the transfer of PHI, the HIPAA Privacy Rule also recognizes the need in certain instances for the Covered Entity to be able to transfer PHI to other parties in the normal course of business. A Covered Entity may disclose PHI without patient authorization in certain instances where it is needed for treatment, payment, or health care operations.[8] Even then, however, the Covered Entity must take sufficient steps to restrict the PHI to be disclosed to what is "minimally necessary" to satisfy the request.[9] Yet, the definition of "Health Care Operations" specifically allows disclosure for:

> "Business management and general administrative activities of the entity, including, but not limited to, … (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity."[10]

Do You Need an Article?

Would an article on a corporate law issue be interesting to you, but you don't have time to write it? Well, we hear from people who want to write articles, but need topics. Contact Vice Chair of Publications Susan Zinder at szinder@zinderlaw.com or (646) 380-6715 with your ideas, and we'll see if we can get something published on it.

In the preamble to the modifications to the HIPAA Privacy Rule adopted in August 2002,[11] the U.S. Department of Health and Human Services (HHS) expressly stated that the aforementioned definition of Health Care Operations includes not only PHI shared during due diligence but also the physical transferring of such information upon the conclusion of the transaction.

Significantly, HHS also imposed a limitation on transaction-related disclosures. In particular, HHS stated:

> "Under the final definition of "health care operation", a covered entity may use or disclose protected health information in connection with a sale or transfer of assets to, or a consolidation or merger with, *an entity that is or will be a covered entity upon completion of the transaction*; and to conduct due diligence in connection with such transaction. The modification makes clear it is also a health care operation to transfer records containing protected health information as part of the transaction."[12] (*emphasis added*).

As noted in the emphasized text, HHS limits the definition to the sharing or transferring of PHI to an entity that is or will be a Covered Entity upon completion of the transaction. The example that HHS utilizes to demonstrate the scope of this authority involves a pharmacy that is a Covered Entity buying another pharmacy, which also is a Covered Entity. Under that scenario, PHI may be exchanged between the entities in due diligence and transfer of such records may be made to the new owner upon the completion of the transaction.[13] This authority also allows a Covered Entity to disclose PHI to a party that is not a Covered Entity if it will become a Covered Entity upon consummation of the transaction.[14] The new owner may then use that PHI because it continues to be protected under the HIPAA Privacy Rule as it was prior to the transfer.[15]

The preamble issued by HHS is helpful in some respects, however, this example is very simplistic and leaves many aspects of the due diligence process in a typical health care transaction open for debate. At present, there is little guidance on whether such disclosure fits within the definition of Health Care Operations if in fact the transaction is not consummated or the receiving party is not a Covered Entity and will not be one at the conclusion of the transaction.

Areas of Uncertainty Involving Disclosure of PHI in Due Diligence

In its pharmacy transaction example, HHS addresses only the disclosure of PHI between two Covered Entities and a Covered Entity's disclosure of information to an acquiring entity that will become a Covered Entity at the conclusion of the transaction. This approach assumes that the transaction will essentially be seamless and that the protections required by the HIPAA Privacy Rule have been maintained during diligence. However, many questions remain. For example, would a disclosure comply with the HIPAA Privacy Rule if:

- The PHI is disclosed to a non-Covered Entity that is a party to the transaction but the transaction is not consummated.
- A Covered Entity provides information to multiple non-Covered Entity suitors as part of a Request for Proposal or other type of bidding process with only one or no successful bidders.
- The PHI is provided directly or indirectly to financial, professional, or other advisors associated with the acquiring party.
- The PHI is provided to a non-Covered Entity party that upon closing will become an owner in the acquiring Covered Entity but remain a non-Covered Entity.

In these four examples, there is no clear answer on what steps should be taken to satisfy the HIPAA Privacy Rule.

As to the first example, it is arguable that the definition of "Health Care Operations" provides legal authority to disclose PHI, even if the transaction is not consummated. However, HHS' statement as to due diligence and the pharmacy transaction example in the August 2002 preamble do not provide clear guidance as to the authority derived from Health Care Operations.

The other three examples are more problematic. If a Covered Entity tenders PHI to multiple bidding entities, only one of which will ultimately be party to the transaction, the guidance does not address how the PHI may be protected. In this instance the disclosing Covered Entity should take proactive steps to attempt to satisfy the HIPAA Privacy Rule. For example, the information should be redacted so there is no individually identifiable health information provided to the recipients. If it is necessary to provide PHI in a non-redacted format, the disclosing Covered Entity should enter into a separate agreement meeting those elements of a Business Associate Agreement but specifically tailored to fit the disclosure.

Can We Publish Your Article?

What have you worked on recently? Is it interesting? Why not tell us about it? The BLG PG needs volunteers to draft newsletter articles, Executive Summaries, and Member Briefings for PG members. We are currently especially interested in governance-related topics. Contact Vice Chair of Publications Susan Zinder at szinder@zinderlaw.com or (646) 380-6715 for more information about how we can convert your recent work into an informative publication for your colleagues.

If the PHI is going to be disclosed to the acquiring party's financial, professional, or other advisors, the disclosing Covered Entity should never disclose directly to these third parties. Rather, the PHI should be disclosed to the acquiring party who then may share the PHI with its advisors, subject to the ultimate recipient executing a Business Associate Agreement with the receiving party. If the PHI is disclosed to a non-Covered Entity party who ultimately upon closing is an owner in the acquiring Covered Entity, it does not give that owner any right to PHI after the transaction is consummated. Rather, the owner's right to access and use terminates upon closing. Any post-closing rights to PHI would require that such access or disclosure fall within the scope of payment, treatment, and operations; be permitted by an authorization; or fall within some other permitted use.

Considerations Prior to Disclosing PHI in Due Diligence

Whether it is permissible under the definition of "Health Care Operations" or falls within the areas of uncertainty, there are issues that should be addressed prior to disclosing PHI in connection with a transaction.

- It is advisable that the disclosing Covered Entity's Notice of Privacy Practices (NPP)[16] contain a provision whereby the patient allows for the sharing of PHI in the event of a sale, merger, or other similar transaction involving the Covered Entity. Therefore, by signing the NPP, the patient will have acknowledged the ability of the Covered Entity to disclose the information in due diligence.
- Prior to moving into the disclosing phase of due diligence, the parties should negotiate what information will be needed, in what format it is needed, what components of the information may be redacted, and which parties and advisors will have access to the information. The parties should then reduce this understanding into a Letter Agreement, Confidentiality Agreement, or Non-Disclosure Agreement that incorporates the parties' respective rights and obligations under the HIPAA Privacy Rule.
- The disclosing party should provide only the minimum PHI necessary to satisfy the due diligence request. It is not uncommon for a due diligence checklist to be overly broad and request information in terms of general categories. The disclosing party should seek clarification on exactly what the receiving party needs to satisfy its due diligence requirements. PHI and IIHI that is not absolutely required, as part of the requesting party's due diligence activities, should be redacted.
- The parties should include within the Non-Disclosure or other Confidentiality Agreement how the information will be handled in the event the transaction is not consummated so as to ensure prompt return and/or destruction of the information, and the maintenance (without use) of any information that cannot be returned or destroyed.
- The disclosing party should require that its Business Associate Agreement be used by the receiving party or that it has the opportunity to review and accept the receiving party's Business Associate Agreement should it disclose the information to an outside party. However, Business Associate Agreements are general in their terms, so it is imperative that the agreement entered into by the parties specifically reference the contemplated transaction. The parties should negotiate what additional terms should be included in the Business Associate Agreement and set forth in its recitals a description of the circumstances for the disclosure. As there is uncertainty regarding disclosure, indemnification language in favor of the disclosing Covered Entity should be included in the negotiated Business Associate Agreement. This proactive step will ensure that the PHI is protected to the satisfaction of the disclosing party, and the disclosing party is adequately protected in event of a breach.
- Ascertain if there are any state confidentiality or privacy laws that may restrict or otherwise limit disclosure.

By taking these steps prior to assembling and disclosing any type of due diligence, it will ensure that the disclosure of PHI has been contemplated and planned for in advance by the disclosing party.

1 *See* Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

2 *For examples of other concerns, see* Krul, S., & Joseph, A. "Navigating due diligence: Sensitive information and pitfalls." *Compliance Today*, 69-75 (April 2015).

3 The American Health Lawyers Association Business Law and Governance Practice Group has created due diligence checklists based upon the type of transaction in its Due Diligence Checklist Toolkit. This information may be found at www.healthlawyers.org/Members/PracticeGroups/blg/Toolkits/Pages/DueDiligenceToolkit.aspx.

4 "Individually Identifiable Health Information" is information that is a subset of health information, including demographic information collected from an individual, and:

Dealmakers Needed

The Transactions AG is seeking dealmakers to share their experiences with their colleagues. We need volunteers to share their knowledge by writing email alerts, Executive Summaries, and Member Briefings on hot, newsworthy business transactions or transaction-related topics throughout the year. We also need people who are interested in leading educational sessions. Interested? Please contact Transactions AG Co-Chairs Judy Mayer at mayej@ihn.org or (856) 853-2115 or Joel Rush at jrush@mwe.com or (202) 756-8659, and we'll work together to share your wisdom with your colleagues.

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

5 Pursuant to 45 C.F.R. § 160.103, Protected Health Information is defined as individually identifiable health information that is: (a) transmitted by electronic media; (b) maintained in electronic media; or (c) transmitted or maintained in any other form or medium but does not include individually identifiable health information: (w) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (x) in records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); (y) in employment records held by a covered entity in its role as employer; and (z) regarding a person who has been deceased for more than 50 years.

6 Pursuant to 45 C.F.R. § 160.103, "*covered entity*" means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

7 *See* Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

8 45 C.F.R. § 164.502(a).

9 *Id.* at § 164.502(b).

10 *Id.* at § 164.501.

11 Standards for Privacy of Individually Identifiable Health Information, Final Rule, 67 Fed. Reg. 53182 (Aug. 14, 2002).

12 *Id.* at 53190.

13 *Id.* at 53190 – 53191.

14 *Id.*

15 *Id.* at 53191.

16 45 C.F.R. § 160.520.

Business Law and Governance Practice Group Leadership

Jay A. Martus, Chair
Advantia Health
Washington, DC
(954) 881-9623
jay.martus@advantiahealth.com

Jeffrey L. Kapp, Vice Chair – Research and Website
Jones Day
Cleveland, OH
(216) 586-7230
jlkapp@jonesday.com

Carolyn V. Metnick, Vice Chair – Educational Programs
Akerman LLP
Chicago, IL
(312) 634-5719
carolyn.metnick@akerman.com

Glenn P. Prives, Vice Chair – Membership
McElroy Deutsch Mulvaney & Carpenter LLP
Morristown, NJ
(973) 425-4179
gprives@mdmc-law.com

Lisa D. Taylor, Vice Chair – Strategic Planning and Special Projects
Inglesino Webster Wyciskala & Taylor LLC
Parsippany, NJ
(973) 947-7135
ltaylor@iwt-law.com

Susan F. Zinder, Vice Chair – Publications
The Law Office of Susan F. Zinder PLLC
New York, NY
(646) 380-6715
szinder@zinderlaw.com

Reema Sultan, Social Media Coordinator
Rivkin Radler LLP
Uniondale, NY
(516) 357-3295
reema.sultan@rivkin.com

Judy W. Mayer, Co-Chair– Transactions Affinity Group
Inspira Health Network
Woodbury, NJ
(856) 853-2115
mayerj@ihn.org

Joel C. Rush, Co-Chair– Transactions Affinity Group
McDermott Will & Emery LLP
Washington, DC
(202) 756-8659
jrush@mwe.com