Large Tech Companies Contract to Access Patient Data:

Critical Issues and Potential Coverage

Management Liability

Healthcare

Gallagher

Insurance | Risk Management | Consulting

Healthcare experts have noted the recent trend of large tech companies contracting for broad access to patient records. Tech companies consider such transactions the future, while healthcare companies weigh whether to engage in such arrangements. This paper explores the critical questions accompanying the rise of tech company partnerships with healthcare record holders, and explores potential insurance coverage for claims that could arise.

Recent Transactions for Access to Healthcare Records

In recent years, large tech companies such as Google have launched initiatives to create a search box-style engine that would enable individual patients or their doctors to access all records in one place. Tech companies have also contracted for access to large volumes of patient data in order to explore more efficient modes of treatment—using analytics to provide everything from comparable case studies to quicker and more accurate diagnoses, to finding opportunities for additional revenue from patients. The counter parties to these agreements (hospitals and other healthcare record holders) cited the potential for streamlining consumer engagement and improving care (See Figure 1).

Figure 1

Transactions: Healthcare Record Holders and Tech Companies

Healthcare Entity/Record Holder	Tech Partner	Record Count	Objective
Duke Univ. School of Medicine and Stanford Medical School (NC and CA)	Google	10,000	Tracked over 4-year period to understand how disease factors affect health "baseline"[1]
Providence Hospital System (WA)	Microsoft	20 million	Cancer-detecting algorithm[2]
Brigham and Women's Hospital (MA)	IBM	1.76 million per year	To build IBM's A.I. capabilities[2]
Mayo Clinic (AZ, FL, MN)	Google	1.33 million per year	Search box, diagnosis and patient compliance algorithms[2]
InterMountain (UT)	Google	1 million per year	Search box, diagnosis and patient compliance algorithms[4]
Stanford University Center for Biomedical Informatics Research (CA)	Google	200 million	Built predictive algorithm identifying, for example, risk for acute kidney disease, risk of death within 3 to 12 months[3]
Ascension (20 states plus DC)	Google	50 million	Search box, diagnosis and patient compliance algorithms[4]
Cerner* (30 countries)	Google	250 million	Search box, diagnosis and patient compliance algorithms[4]
Epic* (at least 9 countries)	Google	190 million	Search box, diagnosis and patient compliance algorithms[4]

* Proposed Cerner and Epic transactions with Google did not move forward.

[1] https://healthcareweekly.com/how-the-big-4-tech-companies-are-leading-healthcare-innovation/
[2] https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200
[3] https://www.wsj.com/articles/your-health-data-isnt-as-safe-as-you-think-11574418606
[4] https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200; https://www.epic.com/contact; Knutson, Ryan and Linebaugh, Kate. (1/10/20). The Journal - Why Google is Pushing Into Health Data [Podcast]. Retrieved from Apple Podcast app.

The Rationale for Tech Incursion Into Healthcare

These transactions are part of a larger trend of tech companies trying to penetrate the healthcare space (see Figure 2). The tech companies aspire to bring a big data solution to the inefficiencies of healthcare in three key areas.

1. **Health record storage and access:** The healthcare industry produces up to one-third of all data on the planet, yet no tech provider has generated a comprehensive search box-style access point for patients or physicians.

2. **Diagnosis and treatment:** Tech companies are exploring the actual provision of healthcare, such as IBM's DeepMind, used to detect kidney problems and prevent blindness with diabetes, or Google's algorithms used to diagnose diabetic retinopathy.

3. **Maximizing patient compliance:** The industry has focused on noncompliant patients regarding medication and testing. Introducing a technology solution to patient follow-up will also provide opportunities for increased revenue per patient and increased efficiencies across all modes of patient treatment.

Tech companies are exploring the actual provision of healthcare, such as IBM's DeepMind, used to detect kidney problems and prevent blindness with diabetes, or Google's algorithms used to diagnose diabetic retinopathy.

Figure 2

Healthcare and Tech: By the Numbers

- $4.7 billion: Amount the top 10 U.S. tech companies spent on 25 healthcare acquisitions in past 8 years[5]
- Healthcare data
  - » Comprises up to one-third of all data generated[6]
  - » Doubles every 73 days[5]
  - » For each individual, will total the equivalent of 300 million printed books over his or her lifetime[5]
- Entire healthcare market in the U.S. ($3.6 trillion) is comparable to total market capitalization of Amazon, Apple and Google parent Alphabet ($3.4 trillion)[7]

Threshold Issues for Participating Entities

There are a number of threshold issues for participants in such arrangements.

Inclusion of personally identifiable data

Finding correlations in data would typically require the largest data sets possible, including personally identifiable information. Patient ages, geographical locations and ethnicities may play critical roles in creating certain algorithms addressing diagnosis or patient compliance.

Potential benefit to patients, physicians and other stakeholders

The transactions as a whole exhibit the potential to transform the tech company, the healthcare company and the field of healthcare overall. The primary gain for patients is more efficient treatment resulting from the transformation of the healthcare field in the years to come.

[5] https://leoinnovationlab.com/2019/03/07/tech-giants-all-have-their-eyes-on-healthcare-how-does-it-affect-you/
[6] https://healthcareweekly.com/how-the-big-4-tech-companies-are-leading-healthcare-innovation/
[7] https://www.forbes.com/sites/robertpearl/2019/12/16/big-tech/#68f916f36d28; https://revcycleintelligence.com/ news/national-healthcare-spending-increased-to-3.6t-in-2018; https://ycharts.com/companies/GOOG/market_cap; https://ycharts.com/companies/AAPL/market_cap; https://ycharts.com/companies/AMZN/market_cap (ycharts sites accessed on February 22, 2020)

Proactively informing patients or physicians of the information-sharing arrangement

Given this potentially transformative effect on healthcare, record holders may consider proactively informing patients, despite not being required to do so in most jurisdictions. HIPAA does not require proactive notice (or any notice) to patients or physicians where a properly contracted business associate accesses healthcare records.

CCPA and GDPR generally enact much stricter notification and opt-in and opt-out requirements, along with providing for private rights of action. CCPA applies to California residents, but will impose no data protection measures to tech agreements discussed here, due to its HIPAA exemption.[8] Florida, Illinois, Washington, Virginia and New Hampshire are considering legislation modeled after CCPA, which may similarly exempt HIPAA-compliant agreements. The GDPR only applies to those residing in the Eurozone. Record access agreements therefore affect patients residing anywhere other than Europe.

Healthcare Is at a Crossroads

For some healthcare record holders, the most significant threshold issue is whether to move forward with such transactions at all. If they refuse to grant tech companies mass access to their patient data, they risk falling by the wayside to potentially groundbreaking and transformative solutions. If they engage in a transaction, they find themselves cast in the new role of data broker and gatekeeper to tech companies. This role may expose them to certain liabilities, should claims arise.

Insurance Discussion

Entities involved in these transactions may be called upon to mitigate damages to or indemnify a stakeholder in a transaction. There are two important items to note at the outset, however. First, the potential for coverage will depend upon the language of the complaint and the policy provisions, known as the eight corners rule. Second, this discussion will focus only on the potential coverage while refraining from commentary on the viability of the claims.

Invasion of Privacy

A patient may sue the healthcare or technology company for invasion of privacy by accessing a patient's healthcare information without consent, and in a way that can be traced back to the patient. Accordingly, a defendant entity may find coverage by reporting under Errors & Omissions insurance—whether under a professional liability, technology E&O or miscellaneous E&O policy. The insured may also notice an invasion of privacy claim under its general liability policy.

The insured may attempt to notice a claim under a D&O policy. For example, the complaint may allege that members of the ethics review board breached their fiduciary duty to the organization by being too permissive with sharing patient data. The insured should work with the broker to explore defense of state regulatory actions under the D&O policy. Additionally, a medical malpractice E&O policy may provide a sublimit for regulatory actions.

[8] https://www.carltonfields.com/insights/publications/2019/ccpa-health-care-hipaa-exemption-apps-data

Data Breach, First Party vs. Third Party

The various tech companies, including Google, have pledged not to use patient data for their advertising businesses, but as cited above, breaches may occur (see Figure 3). One such breach could result in the use of patient data for advertising, in which case the patient may sue for damages. Such a lawsuit may trigger liability (third-party coverages) under the cyber liability policy. Additionally, some cyber policies include failure to follow internal information security procedures in their definition of a covered loss.

Figure 3

Recent Tech Company Fines and Penalties

- September 2019: Google paid $170 million for violating children's privacy rights online in September 2019.[9]
- January 2019: Google paid $57 million (€50 million) under GDPR for failing to disclose to its users how data is collected.[10]
- July 2019: Facebook paid $5 billion to the Federal Trade Commission.[11]
- July 2019: Facebook paid $100 million to the Securities and Exchange Commission due to privacy violations.[12]
- January 2020: Facebook paid a $550 million fine to the state of Illinois for its use of biometric data.[13]

Either the tech company or the healthcare company may experience negative press resulting from a data breach. Cyber policies, D&O policies, and GL policies may provide sublimits for public relations firms or other related expenses.

An insured may also find coverage under a tech E&O policy, for breach of the standard of care. Depending upon the definition of breach, first-party coverage may not be available if the data never leaves the Google environment; first-party breach coverage would typically entail access by an entity outside the business associate agreement.

Either the tech company or the healthcare company may experience negative press resulting from a data breach. Cyber policies, D&O policies, and GL policies may provide sublimits for public relations firms or other related expenses. On the other hand, negative press may result from a tech company or healthcare company mischaracterizing a potential deal. In that scenario, we would look to a GL policy to cover advertising injury or personal injury torts such as libel or slander.

As mentioned, a HIPAA violation requires that the records be accessed outside of the business associate agreement relationship. If the healthcare organization causes or allows a breach, the Office of Civil Rights may bring a regulatory action. For the healthcare company, this would trigger not only defense but also HIPAA fines and penalties to the extent available under the cyber policy or the D&O policy.

[9] https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790
[10] https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html
[11] https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions
[12] https://www.sec.gov/news/press-release/2019-140
[13] https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html

For a non-healthcare party to a business associate agreement, the data security standards are in effect due to a contract (the business associate agreement) and not via statute, as HIPAA only applies to healthcare providers. Barring an exception, the contractually assumed liability exclusion would apply.

Unlike HIPAA, CCPA and GDPR provide for private rights of action; however, CCPA will not apply due to the HIPAA exemption. Coverage for private rights of action under GDPR will vary by policy, and may implicate the contractually assumed liability exclusion, the statutory violation exclusion and any applicable exceptions.

Wrongful Business Decision

In a contract between a tech company and a healthcare company, both may be sued by a shareholder (or, in the case of a nonprofit, a stakeholder) for making a decision that adversely affects the entity. For example, a claim may allege that allowing access to the company's patient records diminished the value or the viability of the healthcare company.

Healthcare providers are not the only holders of patient records. Companies providing digital record-keeping services may also contract with large tech companies providing cloud, analytics and search engine capabilities. If the healthcare record holder engages in such an arrangement, a potential claimant may allege the record holder allowed too much access to its patient records or intellectual property, allowing the larger tech company to become a competitor and resulting in loss of value of the company. This scenario may trigger coverage under the entity's D&O coverage.

As an aside, allegations for failure to safeguard intellectual property would likely result in no coverage under a cyber policy. Cyber policies typically do not cover misappropriation of one's own intellectual property, although they will often cover the taking of intellectual property of business partners or clients.

On the tech company side, such a claim could allege the entity paid too much to access the records, resulting in a competitive disadvantage, a depression in stock price or giving up too large a stake in the resulting intellectual property. On the flip side, a claim could allege failure to pursue partnerships aggressively with a holder of patient data, resulting in lost opportunities to grow in the healthcare business. We would seek coverage under the D&O policy, though the claim may be excluded to the extent that damages stem from contractually assumed liability, such as guarantees or warranties.

Adnan Arain
Senior Vice President
Gallagher
312.803.6342
adnan_arain@ajg.com

About the Author

Adnan Arain fills a multifaceted role specializing in D&O, cyber and professional liability lines of coverage. Deploying a skill set developed as a litigator, former head of claims and subject matter expert, Adnan excels at client advocacy and policy analysis. Prior to joining Gallagher, he served as senior broker in the professional liability space at a large national broker, leading underwriting meetings in the U.S., London and Bermuda. He then served as head of claims and subject matter expert, and led the Management Liability team of a smaller brokerage located in Chicago. Prior to joining the insurance brokerage industry, Adnan practiced law in Chicago, defending professionals who were sued for malpractice.

Adnan earned his BA from the University of Chicago and his JD from Northwestern University School of Law. He is a member of the Professional Liability Underwriters Society.

Gallagher's Approach to Risk

CORE360™ is our unique, comprehensive approach to evaluating our client's risk management program that leverages analytical tools and diverse resources for custom, maximum impact on six cost drivers of their total cost of risk. We consult with you to understand all of your actual and potential costs, and the strategic options to reallocate these costs with smart, actionable insights. This includes advocating for the maximum coverage possible given complex and at times unprecedented claims scenarios, as well as providing risk management consulting such as helping to review your vendor's contracts to help mitigate your risk.

Gallagher employs a unified team approach for our healthcare clients, beginning with veteran producers and client executives. Gallagher surrounds subject matter experts to arm producers and client executives with deep industry insights across multiple lines of coverage. Combined with our **CORE**360™ approach, the Gallagher team will not only examine novel and trending developments within healthcare, but you will also be empowered to know, control and minimize your total cost of risk, and improve your profitability.

The Gallagher Way.
Since 1927.

ajg.com