Digital Health Law Update—An Overview of Notable Happenings Affecting Digital Health, Mobile Health, and Telemedicine
Vol. II | Issue 2 | April 2016 JONES DAY

Industry Insights

FAQ: Purchasing a Cyber Liability Insurance Policy

by Richard D. Milone and Richard DeNatale

There is a saying making its way through the insurance marketplace that there are two types of companies—those that already have purchased a cyber liability policy, and those that will soon wish they had.

This is probably more true with respect to companies in the world of digital health than in practically any other industry. The potential costs associated with a data security breach are well known, and they have potential to spiral out of control. These costs include liability for actual damages caused to customers and other parties; forensic and investigative expenses; notification costs; credit monitoring and similar preventative costs provided to potentially affected parties; fines and penalties assessed by state and federal enforcement authorities; and fees for lawyers and for technical, public relations, and other professionals—the list of potential costs flowing from a breach event continues almost without end.

In addition to these direct financial costs, health care companies that fall victim to a breach may suffer harm to their reputation and goodwill. These risks are enhanced in the digital health field because not only are companies entrusted with customers' credit cards, Social Security numbers, and other information exposing individuals to identity theft and similar financial crimes, but also customers' most private and sensitive health-related information is

CONTACTS

Alexis S. Gilroy
Washington

Soleil E. Teubner
San Francisco

Cristiana Spontoni
Brussels

Kevin D. Lyles
Columbus

Stephen E. Gillette
Silicon Valley

Maureen Bennett
Boston / San Francisco

Todd P. Kelly
Dallas

Jessica Jardine Wilkes, Laura E. Koman, Whitney A. Ehlin, and Olaf Hohlefelder assisted in the preparation of this Digital Health Law Update.

Detailed Contact Information

UPCOMING EVENTS

April 6, June 7, and September 13, 2016: Jones Day is part of the program planning committee and encourages you to attend the Illinois Telehealth Law Forum, a three-part series examining the telehealth landscape in Illinois and the broader Midwest. Meetings will be held simultaneously in Chicago, Carbondale, Naperville, and Springfield on all dates. Click on these links for more information about the Forum and overarching Illinois Telehealth Initiative. Registration for the April 6 meeting

put at risk as well.

In light of the high costs associated with a data breach and the practical inevitability that most companies will be victimized by cyber criminals at some point, an increasing number of companies are purchasing cyber liability policies. These policies—which vary widely in terms of what exactly they cover—bill themselves as protection against both first-party costs (i.e., costs of investigating and fixing the problem, and lost revenue), and third-party costs (i.e., liability to customers and other third parties, and to government entities).

Currently, approximately one-third of U.S. companies have purchased cyber policies, and the number is increasing at a steady pace. There are approximately a dozen major property and casualty insurers in the United States and London markets competing for market share, and therefore pricing is reasonable and conditions are generally favorable for policyholders in the marketplace. Those conditions are likely to change as more companies purchase policies, and as insurers begin booking large claim payments. Therefore, now is a good time for those companies that have not yet purchased cyber policies to consider doing so.
Read More below

Federal Features

OCR Launches Phase 2 HIPAA Audits
On March 21, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced that Phase 2 of the HIPAA Audit Program is underway.

Phase 2, which comes four years after the 2012 pilot testing audit program, will consist of three stages of audits: first, desk audits of covered entities; second, desk audits of business associates; and third, onsite audits to examine a broader scope of requirements. The Audit Program is intended to review both covered entities and their business associates for compliance with the Privacy, Security, and Breach Notification Rules. The audit reports will be used to develop new guidance, technical assistance, and policies to strengthen adherence to HIPAA. The first two stages of audits are expected to be complete by the end of 2016.

MedPAC Meeting
On March 3, the Medicare Payment Advisory Commission ("MedPAC") held a meeting regarding telehealth and Medicare as part of its public meeting to discuss Medicare issues and policy questions and to develop and approve reports and recommendations to Congress. The discussion focused on whether telemedicine can deliver expanded health care access at reduced costs and why more physicians are not using the technology. Some have concerns that the ease of access provided by telemedicine is leading to unnecessary consults, but a 2014 survey cited by MedPAC members suggests otherwise. The members explained that telemedicine will reduce overall expenses by cutting back on emergency room visits, hospitalizations, and imaging costs, particularly as digital health is better utilized to target specific populations.

closes at 11:00 a.m. Central Time on April 5.

May 14–17, 2016: John Kirsner, Mark Paulson, Doug Pearson, and Alexis Gilroy will be speaking at the 2016 American Telemedicine Association Annual Meeting & Trade Show in Minneapolis.

June 21–22, 2016: Alexis Gilroy will be presenting at the second Telemedicine & Telehealth Service Provider Showcase in Phoenix, Arizona. More information about the event can be found here.

DIGITAL HEALTH LAW UPDATE ARCHIVES

Digital Health Law Update Vol. II Issue 1

Digital Health Law Update Vol. I Issue 5

Digital Health Law Update Vol. I Issue 4

Digital Health Law Update Vol. I Issue 3

Digital Health Law Update Vol. I Issue 2

Digital Health Law Update Vol. I Issue 1

RELATED PRACTICE

Digital Health & HIT

RELATED PUBLICATION

Global Privacy & Cybersecurity Update

Confronting Information Blocking and Civil Penalties for Data Breaches
At the end of February, HHS Secretary Sylvia Burwell announced a collaborative effort to promote access to and safety of patient data. The arrangement included some of the biggest hospitals and firms that use digital health records. Participants agreed to stop the practice of "information blocking," which occurs when entities knowingly interfere with the exchange of electronic health data. Almost 75 percent of physicians and almost all hospitals use electronic health records, so many hope this agreement will bridge gaps between existing technical interfaces and encourage secure, efficient electronic health data-sharing and promote interoperability, improved patient care, and cost savings.

Additionally, a March 22 hearing on health information technology before the House Oversight and Government Reform Subcommittee on Information Technology dealt with information blocking and other issues facing health data flow. The heads of the Office of the National Coordinator for Health Information Technology ("ONC") and the Federal Trade Commission's ("FTC") Bureau of Consumer Protection were among the witnesses appearing before the subcommittee discussing outdated privacy laws, conflicting rules, and the lack of usability across systems, particularly with respect to medical apps and wearable devices. Both the ONC and FTC expressed an interest in harmonizing state privacy laws and preventing information blocking.

The FTC agency official also suggested that the agency should have authority to issue civil penalties for all data security and breach notice violations; currently, the FTC may seek such penalties only for violations involving children's online information or credit report information.

OCR Creates Health App Use Scenarios
In February, OCR posted guidance regarding HIPAA applicability to mobile health apps. OCR published the "Health App Use Scenarios & HIPAA" guidance to reduce uncertainty related to health app innovation. The guidance includes six scenarios to help developers determine when they qualify as a "business associate," a person or entity who creates, receives, maintains, or transmits protected health information on behalf of a covered entity. While such inquiries are fact- and circumstance-specific, developers are generally not business associates when a customer must download the app and manually input or upload protected health information. Such arrangements require no relationship between the app developer and a covered entity except for an interoperability arrangement. Importantly, an app developer who is not a business associate may still be subject to regulatory authority under the FTC Breach Notification Rule or under state laws.

CONNECT for Health Act: New Telehealth Bill in Congress
On February 2, a bipartisan group of senators introduced the CONNECT for Health Act to expand the scope of Medicare reimbursements for telehealth and remote patient monitoring services. An identical bill was introduced in the House. The bill has already been endorsed by numerous organizations, including AARP, the American Medical Association, the American Psychological Association, and the American Telemedicine Association. Its sponsors cite a study claiming that waiving existing statutory limitations on Medicare payments for telehealth and remote monitoring services would save the federal government $1.8 billion over 10 years. The bill would permit substitution of telehealth for in-person services in multiple circumstances, such as for treating patients with chronic health conditions and meeting visit requirements for dialysis patients. The bill would also allow Medicare Advantage plans to use telehealth to provide basic benefits under Medicare Part C.

State Summaries

States Continue to Adopt the Interstate Medical Licensure Compact
In December 2015, Wisconsin became the 12th state to enact the Interstate Medical Licensure Compact, an initiative that streamlines certain administrative requirements of

licensure for physicians practicing medicine across state lines. So far in the 2016 legislative session, Alaska, Arizona, Colorado, Kansas, New Hampshire, and Washington have introduced legislation to adopt the Compact. This brings the total number of states with pending Compact legislation to 26. Follow the status of these bills and learn more about the Compact.

Alaska Bill Would Allow Out-of-State Telemedicine Consults
S.B. 74, unanimously passed by the Alaska Senate on March 11, would enable out-of-state telemedicine providers licensed in Alaska to treat Alaska residents without first establishing an in-person relationship, subject to practice standards the legislation directs the Alaska State Medical Board to establish consistent with national norms. The bill, currently being considered by the Alaska House, would amend the existing law, which requires that telemedicine providers who do not have an established relationship with a patient be located in Alaska during the telemedicine consult or work with a patient facilitator as part of the encounter. The bill is also at odds with the Alaska State Medical Board's current Telemedicine Guidelines, which permit telemedicine consults between an out-of-state physician and a person in Alaska only if there is an established physician–patient relationship based on an in-person physical exam.

D.C. Department of Health Proposes New Telemedicine Rules
On February 26, the D.C. Department of Health issued a proposed rule on telemedicine, the first official rules to be published by the Agency and the only guidance issued since its 2014 Telemedicine Policy. The proposed rule defines "telemedicine" as the practice of medicine "through the use of health information and technology communications, subject to existing standards of care and conduct," and provides that in general, telemedicine does not include audio-only, email, instant messaging, or facsimile communications. Among other things, the proposed rule would (i) require that telemedicine providers be licensed to practice medicine in D.C. and, for services rendered outside of D.C., comply with any other licensure requirements of the jurisdictions where the provider and patient are physically located; (ii) require that a physician perform a patient evaluation to establish diagnoses and identify underlying conditions before treatment or prescribing medication; and (iii) require that a physician use real-time auditory or real-time visual and auditory communications for the telemedicine encounter if the physician–patient relationship does not include a prior in-person interaction.

Florida Board of Medicine to Allow Controlled Substance Prescribing via Telemedicine
Effective March 7, the Florida Board of Medicine modified its final rule on telemedicine standards, allowing controlled substances to be prescribed via telemedicine for the treatment of psychiatric disorders. The previous version of the rule prohibited the prescribing of controlled substances via telemedicine, except in the case of patients hospitalized in a Florida licensed health care facility.

Indiana Adopts New Telemedicine Policy
The Indiana legislature adopted a new telemedicine policy (House Act No. 1263), signed into law by the governor on March 21 and effective July 1. The statute allows a variety of providers, including licensed physicians, physician assistants, advanced practice nurses, and optometrists, to provide health care services to patients located in Indiana via telemedicine, defined to include secure videoconferencing, interactive audio-using store-and-forward technology, and remote patient monitoring technology. The statute requires that physicians and other providers utilizing telemedicine establish a proper physician–patient relationship through an appropriate examination. Importantly, this examination does not require an in-person visit but must involve appropriate disclosures, informed consent, an adequate medical history, and the creation of a medical record and "telemedicine visit summary," among other things. The statute also permits remote prescribing of certain drugs and devices without a prior in-person examination but specifically excludes the prescribing of controlled substances, abortion-inducing drugs, and ophthalmic devices (glasses and contact lenses). Further, the statue calls out that telemedicine does not include, among other things, an audio-only communication,

electronic mail, instant messaging, a telephone consultation, or an internet consultation. Under the law, out-of-state telemedicine providers must file a certification with the appropriate Indiana licensing agency, expressly agreeing to be subject to Indiana law and jurisdiction in connection with any claim asserted against the provider arising from the provision of health care services in Indiana.

The statute appears to conflict with current regulations of the Medical Licensing Board, which the Board has previously interpreted to require an in-person "physical evaluation" to establish a provider–patient relationship.

Louisiana and Missouri Consider Telemedicine Bills
During the 2016 legislative session to date, legislatures in Louisiana and Missouri considered bills to amend telemedicine policies. Louisiana H.B. 570, introduced on March 3, would remove the current requirement that a physician providing services via telemedicine maintain an office or an arrangement with a physician who maintains an office within the state. Further, the proposed legislation deletes the requirement that communications via telemedicine be both video and audio, leaving a choice between video or audio transmission. Missouri H.B. 1923, introduced on January 6, would establish a new telemedicine policy dictated by the standard of care applicable to in-person services. Although the law would require a telemedicine provider to establish a proper physician–patient relationship before rendering telemedicine services, under the law, such relationship can be established through the use of telemedicine.

West Virginia Adopts Telemedicine Legislation
West Virginia legislature adopted H.B. 4463 on March 11, and it was approved by the governor on March 24. Effective June 9, the legislation clarifies current telemedicine policy in the state and explicitly provides that a physician–patient relationship may be established through a telemedicine encounter incorporating either (i) interactive audio-using store-and-forward technology, (ii) real-time videoconferencing or similar secure video services, or (iii) for the practice of pathology and radiology, store-and-forward telemedicine alone.

Reimbursement Review

Several State Legislatures Consider Telehealth Parity Laws
Several state legislatures are considering bills regarding reimbursement for telemedicine services. Rhode Island and New Jersey are both considering legislation to adopt mandated telehealth parity legislation for the first time. Rhode Island S.B. 2577 would require health insurers to provide coverage for the cost of health care services provided through telemedicine, and New Jersey S.B. 1954 would require the same for telemedicine services delivered to covered persons in a health care facility. Several other state legislatures are considering bills to expand current telehealth parity laws. Hawaii S.B. 2395 would remove language requiring a health care provider to be physically present with the patient at the originating site during a telehealth encounter to ensure reimbursement, and it would require all insurers to provide current and prospective insureds with written disclosure of coverages and benefits associated with telehealth services. Arizona S.B. 1363, introduced on January 28, would remove the "rural region" limitation in the telehealth parity law. Washington S.B. 6519 would add the patient's "home" to the list of approved originating sites.

Proposals for Telehealth Payment in Florida Lay Initial Groundwork for Reimbursement
On March 11, the Florida legislature passed HB 7087 requiring the Agency for Health Care Administration, the Department of Health, and the Office of Insurance Regulation to collect information related to telehealth reimbursement. Although the law does not mandate commercial insurance coverage for telemedicine services, the law creates the "Telehealth Advisory Council" within the state Agency for Health Care Administration to review the current insurance landscape and make a formal report to the governor and

legislature, setting the stage for a more permanent telehealth reimbursement policy.

A proposed rule by the Agency for Health Care Administration would provide for Medicaid reimbursement for telemedicine services rendered using interactive audio and video equipment permitting two-way, real-time, interactive communication between a recipient and a practitioner. The rule specifies that Medicaid will not reimburse for telephone, email, or facsimile communications; chart reviews; or the equipment required to provide the telemedicine services. The rule was published in the Florida Administrative Register on March 15.

Global Happenings

EU and U.S. Release Terms of Privacy Shield
The European Commission and U.S. Department of Commerce recently released the full text of the EU–U.S. Privacy Framework, which replaces the recently invalidated Safe Harbor program for transatlantic data transfers. More details can be found on the Jones Day Cybersecurity publications website.

Germany Passes eHealth Act
In December 2015, Germany passed the Act on Safe Digital Communication and Applications in the Healthcare Sector (the "Act"). Among other things, the Act provides a roadmap for the implementation of a digital infrastructure and expanded applications of the so-called "*Gesundheitskarte*." The *Gesundheitskarte* is a chip card issued to each insured person in Germany that carries the individual's health data so that doctors and other authorized persons can access the data in connection with the treatment of the individual. The Act provides for a number of new applications of the card such as emergency data availability, medication plans, an electronic patient file, and an interface for private service providers.

Jones Day Digital Health Law Contacts

Alexis S. Gilroy
Washington
+1.202.879.5552
agilroy@jonesday.com

Soleil E. Teubner
San Francisco
+1.415.875.5709
steubner@jonesday.com

Cristiana Spontoni
Brussels
+32.2.645.14.48
cspontoni@jonesday.com

Kevin D. Lyles
Columbus
+1.614.281.3821
kdlyles@jonesday.com

Stephen E. Gillette
Silicon Valley
+1.650.739.3997
segillette@jonesday.com

Maureen Bennett
Boston / San Francisco
+1.617.449.6884 / +1.415.875.5772
mbennett@jonesday.com

Todd P. Kelly
Dallas
+1.214.969.5122
tkelly@jonesday.com

Digital Health Law Update—An Overview of Notable Happenings Affecting Digital Health, Mobile Health, and Telemedicine
Vol. II | Issue 2 | April 2016 JONES DAY

Industry Insights

FAQ: Purchasing a Cyber Liability Insurance Policy
by Richard D. Milone and Richard DeNatale

There is a saying making its way through the insurance marketplace that there are two types of companies—those that already have purchased a cyber liability policy, and those that will soon wish they had.

This is probably more true with respect to companies in the world of digital health than in practically any other industry. The potential costs associated with a data security breach are well known, and they have potential to spiral out of control. These costs include liability for actual damages caused to customers and other parties; forensic and investigative expenses; notification costs; credit monitoring and similar preventative costs provided to potentially affected parties; fines and penalties assessed by state and federal enforcement authorities; and fees for lawyers and for technical, public relations, and other professionals—the list of potential costs flowing from a breach event continues almost without end.

In addition to these direct financial costs, health care companies that fall victim to a breach may suffer harm to their reputation and goodwill. These risks are enhanced in the digital health field because not only are companies entrusted with customers' credit cards, Social Security numbers, and other information exposing individuals to identity theft and similar financial crimes, but also customers' most private and sensitive health-related information is put at risk as well.

In light of the high costs associated with a data breach and the practical inevitability that most companies will be victimized by cyber criminals at some point, an increasing number of companies are purchasing cyber liability policies. These policies—which vary widely in terms of what exactly they cover—bill themselves as protection against both first-party costs (i.e., costs of investigating and fixing the problem, and lost revenue), and third-party costs (i.e., liability to customers and other third parties, and to government entities).

Currently, approximately one-third of U.S. companies have purchased cyber policies, and the number is increasing at a steady pace. There are approximately a dozen major property and casualty insurers in the United States and London markets competing for market share, and therefore pricing is reasonable and conditions are generally favorable for policyholders in the marketplace. Those conditions are likely to change as more

companies purchase policies, and as insurers begin booking large claim payments. Therefore, now is a good time for those companies that have not yet purchased cyber policies to consider doing so.

There are two structures emerging for companies looking to purchase cyber policies. Small to mid-sized companies will typically be offered stand-alone policies with limits anywhere from $1 million to $20 million, and they are likely to find relatively customer-friendly underwriting on the part of insurers who are anxious to compete for their business. Larger companies, on the other hand, will likely need to craft layered programs resembling their directors and officers ("D&O") and general liability towers (i.e., several excess policies stacked above a primary policy), providing upwards of $100 million in limits.

The current trend is for underwriters to delve deeply into a company's security measures and cyber preparedness as part of the application process. Obviously, companies should present themselves in the best light that they can in connection with this process, and indeed it may be worthwhile to update security policies and implement appropriate procedures in conjunction with the application process. Companies that present more favorable risk profiles can often obtain better terms and pricing on cyber policies.

When preparing applications, companies should bear in mind that the application is not a privileged document and may be discoverable in a lawsuit or investigation following a breach, and therefore it should be prepared with that possibility in mind. It is critical, however, to make absolutely sure that all statements on the application are truthful and complete. Insurers might not investigate the information particularly closely during the sales process, but after a claim is made, they frequently take a much closer look and may seek to rescind the policy if they believe that an argument can be made that there was fraud or misleading conduct in the application process. The risk for policyholders is heightened by new terms that are starting to appear in some cyber policies requiring companies to warrant their security protocols or excluding coverage when companies depart from those protocols.

As a case in point, a coverage dispute involving a health care company was briefly in the public eye during 2015, and it illustrates two arguments that potentially can be asserted by insurers to deny coverage. Cottage Health Systems paid $4.1 million to settle a class action lawsuit alleging that patients' medical records were compromised as a result of a data breach. Its insurer, Continental Casualty Company, initially funded the settlement but then filed a declaratory judgment action against Cottage Health, seeking a ruling that the matter was not covered and seeking return of the settlement funds. *Columbia Casualty Company vs. Cottage Health System*, USDC Case No. 2:15-cv-03432 (C.D. Cal.) (filed May 7, 2015).

Columbia Casualty argued that Cottage Health failed to comply with Minimum Required Practices as required by the insurance policy, because it stored patients' medical records on an unsecure server, without encryption or other security measures. In addition, Columbia Casualty asserted that Cottage Health answered questions inaccurately on the insurance application concerning the measures it had taken to protect its patients' data.

Shortly after the suit was filed, Cottage Health moved to dismiss the case in favor of arbitration on the grounds that Columbia Casualty had filed the suit in violation of a mandatory arbitration provision, and shortly afterward, the suit was referred to arbitration. The dispute will therefore be decided in a confidential proceeding but offers a brief glimpse into the coverage issues that may be asserted under cyber policies.

When purchasing a cyber policy, the analysis needs to go beyond the basic economic terms such as price, retention (i.e., deductible), and limits of coverage, and must focus on the wording of the contract itself. Companies should ask their broker to obtain quotes from multiple companies and should carefully compare the terms of the policies to determine exactly what they are purchasing. Unfortunately, this task is made more

difficult by the current state of the cyber insurance market. Cyber policies are extremely complex; standard forms have not yet emerged, and the forms currently on the market vary widely in terms of scope of coverage. It may be prudent, therefore, to seek help from insurance coverage attorneys with experience pursuing cyber claims to help identify problematic features of the policy and to recommend improvements to the wording. Due to most insurers' willingness to negotiate and manuscript changes to their forms, a few hours of review and negotiation can make a world of difference in the value of the policy obtained.

Cyber policies frequently contain alternative dispute resolution clauses requiring coverage disputes to be submitted to binding, confidential arbitration, rather than litigation in federal or state courts. A byproduct of confidential arbitration is a lack of published court decisions interpreting cyber insurance policies. This makes it all the more important to consult with coverage counsel experienced in cyber and data breach claims, who can explain how insurers interpret cyber policies, what arguments they are likely to make, and which provisions matter most in the event of a breach.

Once a policy has been purchased, if a claim arises, it is important to give prompt notice, and to comply with other requirements in the policy. Seeking prompt approval of attorneys and other vendors is helpful to making sure that their fees will be reimbursed, and compliance with consent and cooperation provisions in the policies increase the likelihood of favorable claims treatment.

Before long, cyber policies will be as standard for businesses as general liability or D&O insurance. In the meantime, any company handling large quantities of confidential health data and other sensitive personal information would be well served to be ahead of the curve and have this important protection in place.

Return to Homepage.