LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

AI Brings New Insurance Concerns For Healthcare Providers

By **Marialuisa Gallozzi and Megan Mumford Myers** (December 6, 2023, 2:21 PM EST)

As businesses across the U.S. consider new uses for rapidly developing artificial intelligence tools, the medical sector stands out as an early adopter.

Marialuisa Gallozzi

Megan Mumford Myers

According to an American Medical Association survey last year, over half of U.S. physicians either already used AI tools to augment their clinical practice or planned to do so within the next year.

There are more than 150 radiology AI products already on the market for tasks like detecting tuberculosis and cancer at lower radiation and contrast doses than required for review by a human radiologist.

Hospitals like Mass General Brigham use about 50 algorithms for a range of patient care applications, from detecting aneurysms and signs of stroke to tracking changes in biomarkers to predict a heart attack. Commentators have emphasized the immense potential and unique risks of deploying AI technology for patient care.

As hospitals, physician groups, health tech startups and others consider increasingly large investments in medical AI tools, they are confronting a variety of risks of liability to third parties and of loss of, or damage to, their own assets and income.

These users need to understand (1) what those risks are, (2) what steps they are taking or need to take to minimize potential losses and liabilities arising from those risks, and (3) whether they are insuring or self-insuring those risks.

Critical Risks

A few examples of these critical risks are discussed below.

Data Breaches and Exposure to Privacy Liability

AI exacerbates data breach and privacy liability exposure for healthcare providers in three ways: (1) it increases interconnectivity and therefore increases the potential opportunities for attack and resulting corruption or exfiltration of data, (2) it makes data deidentification more difficult to maintain; and (3) it relies on massive datasets for training.

These risks are especially important in the healthcare regulatory context; for example, the Health Insurance Portability and Accountability Act security rule promulgated in 2003 requires sufficient security measures to protect electronic protected health information.

More recently, the Federal Trade Commission's Health Breach Notification Rule requires health apps and connected device companies to notify consumers when their health data is breached. But there is still potential privacy liability exposure even in the absence of a data breach.

For example, a **class action** filed against Medtronic on Aug. 30 alleges breach of privacy and HIPAA violations based on Medtronic's smart device and app for insulin management, InPen, sending data to Google, which in turn allegedly connected that health data to customers' Gmail account information.

Medical Errors

Although AI tools could eliminate human error, they may also replicate human error or introduce new types of errors. Common examples may include malfunctioning surgical robots that injure patients or diagnostic tools that misdiagnose serious diseases, either delaying vital care or requiring unnecessary follow-up care.

But there are countless other risks: For example, the U.S. Food and Drug Administration recalled a prior version of Medtronic's InPen app when a software bug caused the app to fail to refresh, noting that this could lead to hyperglycemia in patients who did not receive dosage alerts from the malfunctioning app.

And, although much of the focus for medical errors has been on risks in using AI tools, it's possible that certain AI tools will become so commonplace that hospitals or physicians could face liability for not using them, if a human error becomes rare due to an AI solution.

For example, it has been suggested that AI models may be better at diagnosing rare diseases than human doctors, whose experience is typically skewed toward relatively common diseases.

Discrimination

Use of AI in medical care may also eliminate human bias in delivering medical care, but runs the risk of replicating statistical disparities instead. For example, studies have shown that AI models may exacerbate racial disparities in pain treatment due to bias in underlying training data, such as recommending fewer surgical treatments and less pain medicine. In the healthcare context, these risks may result in lawsuits under the Affordable Care Act's anti-discrimination provision, Section 1557.

Unsurprisingly, medical providers are concerned about addressing such risks: in the same American Medical Association survey which found that most physicians are using or planning to use AI tools soon, the respondents' number one concern was whether their malpractice insurance coverage would cover these tools.

Despite the rise of AI tools, medical malpractice policies have not yet been revised to address these risks. To the extent AI risk imitates human risk, traditional policies may still respond.

As a practical matter, when new or increased risks emerge, insurers often respond in a few ways — they can exclude them altogether, they can provide a sliver of coverage under a sublimit of a larger policy and they can also write new policies.

As discussed below, we expect all these things to happen in the coming years. An example of this response to risk was when insurers attempted to excise what they called silent cyber coverage from commercial property policies by adding electronic data exclusions or lower cyber sublimits and also offering separate cyber policies for a separate premium.

Cyber Policies, and Tech Errors and Omissions Policies

Cyber policies may be a logical fit for many AI-related losses. For example, many cyber policies now cover both a policyholder's own costs to respond to a data breach and costs to defend third-party claims based on the breach. However, cyber policy terms vary significantly, particularly in terms of whether they provide business interruption coverage and, if so, whether business interruption due to a voluntary shutdown is covered.

They also vary in whether they exclude property damage, or carve out cyber-related property such as computer hardware from this exclusion. Cyber policies may also provide ransom coverage for cyber hacks or other costs like payment cost industry fines.

However, insurers may attempt to separate AI risk from cyber risk. For example, some cyber policies are written to provide coverage for damage to data. But an AI loss may result from inaccurate data rather than damaged or destroyed data.

As another example, insurance companies have introduced new exclusions for state-sponsored cyberattacks, cyberwar and cyberterrorism after the pharmaceutical company Merck & Co. Inc. successfully litigated a coverage dispute involving the NotPetya computer virus. Even if a provider is not practicing medicine in a war zone, insurers may be especially likely to argue that hacks of medical facilities are forms of cyberterrorism.

Property Policies

Traditional property policies may also provide coverage for property damage caused by medical AI tools. Damage to surgical robots and advanced imaging machines should be covered in the same way as damage to less advanced equipment. This should be true even if the cause of an accident is AI-related, such as an algorithmic error causing a machine to spin out of control.

Even where there is a clear nexus to physical damage, insurers may argue that losses caused by AI-specific accidents implicate the electronic data exclusions imposed after the silent cyber movement. Policyholders should carefully evaluate any potential gaps between their property coverage and cyber coverage, to the extent the two are provided separately.

Commercial General Liability Policies

Medical technology that utilizes AI may blur the line between commercial general liability coverage and professional liability coverage as physicians utilize AI products in performing their job.

For example, a misdiagnosed patient may file a claim against both the medical provider for medical malpractice and against the AI diagnostic tool developer for product liability.

Causation will be a key issue — was the error the physician's failure to supervise the automated diagnostics system properly or a coding error in the diagnostic product? In some cases, the healthcare facility could be both the provider and the tool developer.

In a similar vein, policyholders should pay careful attention to the definition of "insured" in their policies. Insurance policies typically cover claims against the policyholder and its employees. Because insurers underwrite risk based on the performance history of the organization and its risk management practices, they are likely to argue that traditional policies are not intended for algorithmic liability, but rather, errors by humans.

As such, policyholders should evaluate whether the definition of "insured" covers the organization broadly or only lists specific types of individuals. Commercial general liability policies may also exclude discrimination liability, so policyholders should consider negotiating for this coverage if their use of AI tools may increase such risk.

New Policies

Apart from coverage for AI risks under traditional policies, some insurers have launched AI-specific offerings. Although there is room for disagreement on this point, we note that the underlying premise of these new offerings is that traditional policies do not cover these types of novel risks.

To fill this perceived gap, Munich Re Group has developed first-party "aiSelf" AI insurance for business interruption caused by the need to retool a company's AI model to respond to model drift, which occurs when the composition of input data changes from the training model or the statistical relationship between the input and the target changes over time in unforeseen ways. This product is intended for companies that develop AI solutions for internal use.

For companies offering AI solutions to others, Munich Re also offers insurance to backstop AI tool developers' warranties to reimburse clients for model errors. Armilla Assurance, a new Toronto-based startup, has also begun to offer a product warranty for a similar purpose.

Although medical providers developing AI tools may not offer them to other organizations for profit, they should monitor the types of risks that insurers are separating into new policy forms.

Programwide Considerations

In addition to medical malpractice coverage, healthcare providers should consider how AI risks fit into their overall insurance programs. In the first instance, policyholders are focused on reducing their risk and then on insuring that risk. The policyholder assumes the residual risk.

To evaluate coverage for AI risk, policyholders need to consider the insurance program as a whole. A single loss or claim can trigger multiple lines of insurance and the insured might need to provide notice to multiple insurers, often on a very expedited schedule.

Given the increasing focus on AI risk, policyholders will need to address their AI risks carefully when applying for insurance. Underwriters are beginning to ask about use of AI in insurance applications. Providing complete answers to such questionnaires may be challenging in large systems where knowing which departments are developing AI tools is difficult in the first place.

Providers should conduct a thorough survey of their AI risks and make sure that the application is vetted by those with knowledge of the risks, much like preparing an informed response to a questionnaire for cyber risk insurance.

Although insurers have not begun to draft specific AI exclusions, there are other ways in which insurers could seek to limit coverage for AI losses and liabilities. Insurers might look to existing policy language to support the position that AI losses and liabilities are not included in coverage in the first place or are ousted from coverage by existing exclusions.

Insurers might also limit their financial exposure by imposing sublimits for AI risk or by restricting the choice of or rates for breach response vendors. It is often possible to add a provider's preferred vendors to the list of approved vendors, particularly for regulatory expertise that is needed for proper notification to regulators and affected third parties and response timing.

As medical providers and insurance companies grapple with AI risk in real time, it is critical for policyholders to assess and anticipate their risks, and ensure that their risk management programs adequately respond to these risks.

Marialuisa Gallozzi is a partner and Megan Mumford Myers is an associate at Covington & Burling LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.