Published on *The National Law Review* https://natlawreview.com

Digital Health Checkup (Bonus): Product Liability and Insurance Coverage

Article By:

John G. Buchanan III

Marialuisa S. Gallozzi

Elizabeth H. Canter

Jeffrey A. Kiburtz

Scott J. Levitt

René L. Siemens

In this bonus edition of our checkup series, Covington's global cross-practice Digital Health team considers some additional key questions about product liability and insurance coverage that companies across the life sciences and technology sectors should be asking as they seek to fit together the regulatory and commercial pieces of the complex digital health puzzle.

1. What are the key questions when crafting warnings and disclosures?

If your product is regulated, your warnings and disclosures will need to comply with any relevant regulations. In the case of a product not regulated by the FDA or equivalent regulatory body, first consider how your warnings and disclosures will be incorporated into the use of the product.

Some disclosures, like an explanation of the data source used by software, may fit best in terms and conditions that a user sees before using the product. Key warnings, however, may be more appropriately placed as part of the user experience.

Example: A warning that patients should consult their doctors if necessary may need to be placed in proximity to specific medical content.

> **Best Practice:** Consider your intended audience: are you writing warnings for doctors, patients, or institutions? The appropriate types of disclosures will vary across populations. Patient-directed warnings may also need to be written in simplified language.

Best Practice: Consider whether it is appropriate for your product to have users to accept or otherwise be required to agree to the warnings and disclosures.

2. How should you craft contracts with vendors or service providers to control your risks?

When drafting or reviewing a proposed indemnification clause, consider whether the proposed language:

- will benefit or bind the intended parties, including successors-in-interest;
- encompasses the intended subsets of costs or expenses from which indemnification will be provided, including attorneys' fees, internal forensic and other response costs, government investigation costs, and settlements with third parties;
- the circumstances in which the indemnification obligation will arise, such as upon a suspected network security event or only upon a third-party asserting a claim;
- the nexus required between the indemnity-triggering event and the indemnity obligation, with common nexus phrases being "directly caused by" and "arising out of" or "in connection with;" and
- the point when the indemnification will be owed for an indemnity-triggering event such as a network security breach: for example, when a reasonable suspicion of the event arises, or only after proof that the event did in fact take place.

Best Practice: In addition to the indemnification clause, you should consider whether the contract counter-party has sufficient financial resources to fulfill its indemnity obligations. An insurance procurement clause, specifying the types and amounts of insurance coverage the counter-party must carry, is often the best way to back up your indemnification protection. An insurance clause requires careful attention, however, with an eye to the principal risks involved in the particular contract.

It is not enough merely to specify **"cyber insurance"** in an insurance procurement clause: cyber policies vary as to the categories of risks they cover, and their non-standardized wordings vary in scope and clarity of coverage for those risks. The contract's insurance procurement clause should specify which cyber-related risks must be insured, and with what minimum limits; and it should permit you to review the actual policies procured, to confirm their suitability.

The contract should also address whether the **counter-party** is required to make you an additional insured under its policies. Again, a right to review the actual policies—not merely certificates of insurance—is important to ensure that the policies properly implement the additional-insured requirement.

3. What traps should you look for in your own insurance policies?

Digital health solutions can give rise to a broad range of risks, including alleged data breaches, privacy violations, faulty technology, theft, bodily injury, property damage, business interruption or extra expense, government demands, and shareholder suits. These risks could involve an equally broad range of insurance policies, including cyber, technology errors and omissions, professional liability, commercial crime, media liability, commercial general liability, products liability, property, and directors and officers liability.

> **Best Practice:** In assessing whether and how your insurance coverage aligns with the risks that your particular digital health solution presents, pay close attention to potential gaps between the various insurance policies that are intended to cover those risks, including policies under which your company qualifies as an "additional insured."

Professional services are often excluded from general and products liability policies on the theory that the policyholder can purchase separate professional liability insurance to cover that risk. But if the definition of "professional services" used in the exclusion to your general or products liability policy is broader than the definition of "professional services" used in the insuring agreement for your professional liability policy, a protection gap may arise between two policies that were meant to provide seamless coverage. Particularly if your company provides post-sale support for a digital health solution, you should carefully review the "professional services" language in all potentially applicable policies to be sure that they are consistent.

Many **cyber policies** exclude bodily injury, while cyber-related exclusions have recently appeared on many commercial general liability policies, which have traditionally covered bodily injury arising from products. If, for example, a cyber hacker could injure a patient by remotely manipulating the digital settings on your medical device, you should be alert both for injury-related exclusions in your cyber policies and for cyber-related exclusions in your general liability or professional liability policies. If you find an insurance gap, you may need to explore specialty insurance products designed for so-called "cyber-physical" risks.

Best Practice: Make sure you have insurance policy limits that are large enough to match your likely liabilities and that your excess policies are as broad as your primary policy.

Marty Myers, Emily Ullman and David Goodwin, attorneys from the Covington Digital Health Team, also contributed to this post.

National Law Review, Volume VII, Number 349