Understanding bodily injury in eHealth

Technology is fundamentally changing the way healthcare is delivered, monitored and addressed. And **telemedicine** - or the remote delivery of healthcare services - is one of the fastest growing, and most obvious examples of this shift. While the use of technology can deliver great benefit to patients, it also creates new exposures for both traditional and digital healthcare organizations. And questions around medical responsibility in the event of bodily injury or harm to a patient are still being debated.

What is clear is that traditional bodily injury coverage triggers have become outdated and are no longer sufficient due to the global rise of technology within healthcare.

Here is how our policy addresses each of these unique exposures:

Healthcare services

Failure to adequately assess a patient and their symptoms via **telemedicine** could lead to incorrect diagnosis and delayed treatments. Similarly, if a patient is sending a picture of a physical issue such as a rash, a distorted image could lead to an incorrect diagnosis.

If a patient suffers misdiagnosis, delayed or incorrect treatment as a result of healthcare services provided through remote means, the policy will trigger.

Technology activities

Artificial intelligence is now being used to more effectively triage patient conditions, most commonly diagnosing basic illnesses via a **chatbot** function, however, the way in which a patient describes their symptoms can leave them confused or undiagnosed.

If a patient suffers misdiagnosis, or goes undiagnosed via a chatbot, the policy will trigger.

System outage

A failed update or computer system outage could affect **remote patient monitoring** functions, this could pose a risk to patient's safety in the event of a medical emergency.

If a system failure leaves you unable to diagnose or treat a patient, the policy will trigger.

Cyber-attack

A targeted ransomware attack could deny access to systems and patient data, where patients' vitals are being monitored and medications prescribed via **telemedicine**.

If a cyber-attack cripples the telemedicine system or electronic medical records database, meaning patients could be unable to receive repeat prescriptions leading to injury or even death, the policy will trigger.

CFC's eHealth insurance policy addresses this challenge by providing multiple bodily injury triggers. These include four main areas in which exposures can arise: healthcare services, technology activities, cyber events or system outages. To find out more about how CFC's eHealth policy works get in touch with tboyce@cfcunderwriting.com