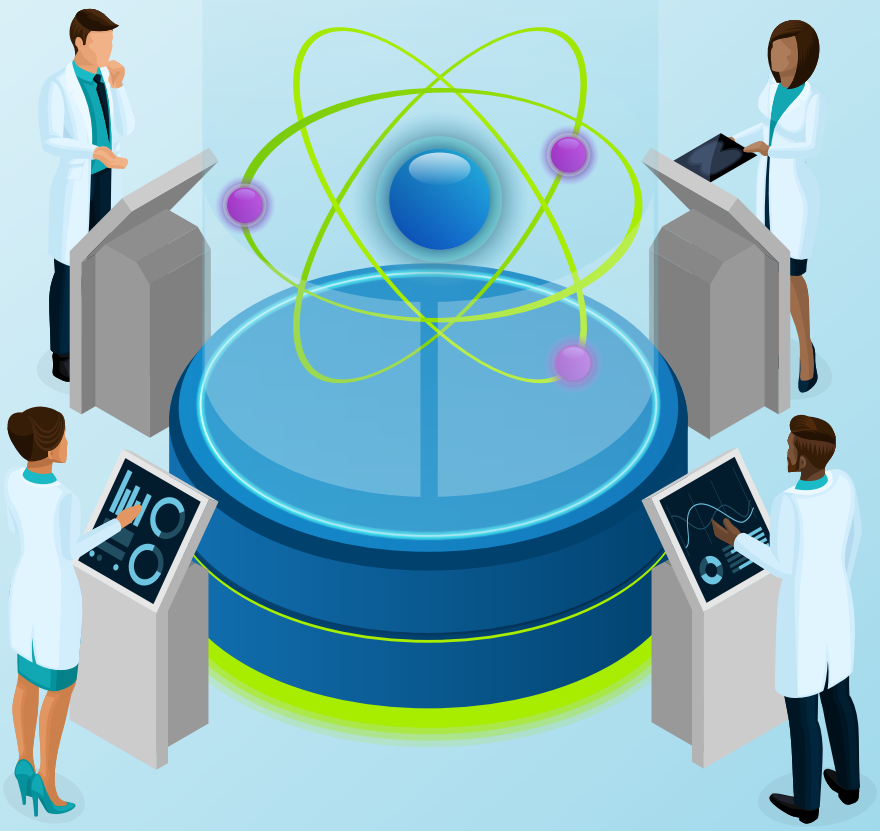
Our **life science policy** in action

In the fast-paced world of life sciences—where biotech startups, medical device innovators, research labs, and global pharma giants often work side by side—collaboration fuels innovation. But with that collaboration comes a growing web of interdependency on suppliers and increased risk. With ideas, data, and materials crossing borders and between companies, exposures can emerge from unexpected places.

Here we'll explore how our package policy comes to life through a variety of claims scenarios, highlighting how our coverage responds when the complex becomes critical.

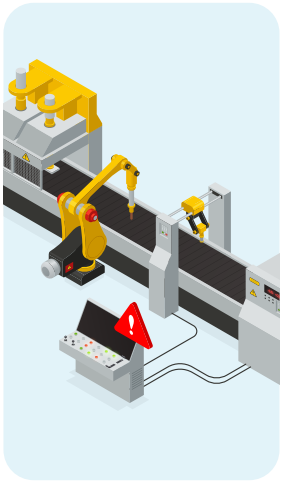


Research and development

Errors and omissions: Bodily injury

A clinical research organization (CRO) was managing a clinical trial on behalf of a pharmaceutical sponsor. Whilst conducting the trial, an employee of the insured responsible for screening the participants failed to identify that a participant had been taking an over-the-counter (OTC) drug that is contraindicated to the investigatory study drug, which led to the participant suffering a serious adverse event.

Our policy specifically provides bodily injury under the Errors and Omissions insuring clause for clinical trial research services performed by the insured.

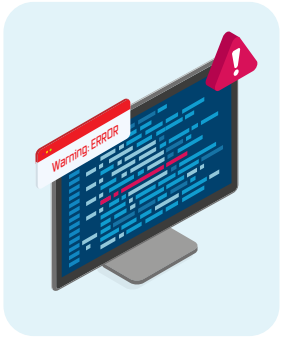


Errors and omissions: Property damage

A contract research service laboratory specializing in high-throughput assay processing has developed a custom in-house automated system to manage overnight assay runs for its pharmaceutical clients. A software scheduling error caused the robotic liquid handling system to dispense an incorrect reagent across an entire batch of client samples overnight.

The assays being run were pre-clinical assays testing the effect of a clients' novel pharmaceutical drugs on tissue samples. The results from these assays would be used for submission to regulatory bodies for approval to conduct clinical trials. The pre-clinical assays would need to be re-run so replacement stock needed to be re-manufactured for the insured to re-run the experiments.

Our policy specifically covers property damage and consequential financial loss under the Errors and Omissions insuring clause.



Errors and omissions: Technology

A specialist life science technology provider developed an AI platform designed to collect, store and analyze clinical trial data for pharmaceutical and biotech clients. Following a routine software update, a coding error caused critical data corruption, resulting in the permanent loss of clinical trial datasets across multiple clients.

As the affected data could not be recovered, the impacted trials had to be repeated in full, leading to substantial delays and significant additional costs for the insured's clients. Our policy can be extended to include technology E&O cover under the Professional Liability insuring clause to cover liability arising out of technology services errors.

Products liability: Bodily injury

A contract manufacturing organization was engaged to produce a novel vaccine for use in a client's clinical trial. During production, a batch of the vaccine became contaminated with foreign microbial material—an issue that was not detected during the quality control phase. The contaminated batch was released and administered to trial participants, several of whom suffered adverse reactions and bodily injury as a result. The incident triggered a full clinical investigation, regulatory scrutiny, and a halt to the trial.

Our policy provides products liability coverage that specifically provides bodily injury arising out of a product manufactured or supplied by the insured.

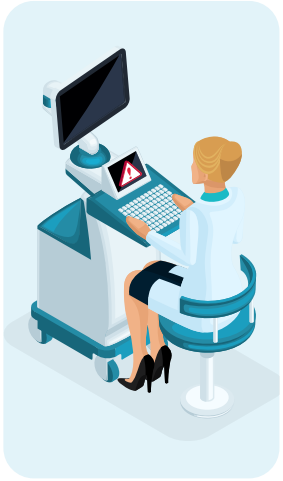
Cyber business interruption: Research and development expenditure

A research and development (R&D) biotech company, in the pre-clinical phase of developing a novel cancer therapeutic, suffered a cyber attack that rendered its computer systems inaccessible. The threat actor infiltrated the company's network, encrypted critical files containing years of pre-clinical toxicology and pharmacovigilance data derived from animal models and ex-vivo tissue samples, and disabled system functionality.

The insured had no offline or offsite backups, rendering the data temporarily inaccessible and halting all R&D activity. At the time of the attack, the company was preparing a regulatory submission to advance to the clinical trial phase, a milestone that would have triggered the release of significant investor funding. The cyber incident not only caused delays but led to unproductive cash burn as fixed operational costs continued during the disruption.

CFC's cyber cover for life science organizations includes affirmative cover for research and development expenditure that is specifically designed to protect the insured's balance sheet of non-revenue generating R&D companies following an interruption to their business.

Commercial products



Technology triggered: Bodily injury

A medtech company sold advanced ultrasound imaging devices to hospitals, designed for use in emergency departments to support rapid cardiac diagnostics. Alongside the tangible devices, proprietary artificial intelligence (AI) powered software was installed onto the hospital network, intended to assist clinicians by highlighting abnormalities during suspected cardiac events.

Following a recent software update, a subtle coding error introduced image distortion that reduced diagnostic clarity. Initially unnoticed, the error impaired the AI's ability to flag critical abnormalities, leading to missed diagnoses. Seven patients were affected—one suffered a mild cardiac arrest, while the others experienced minor but measurable cardiac and pulmonary complications.

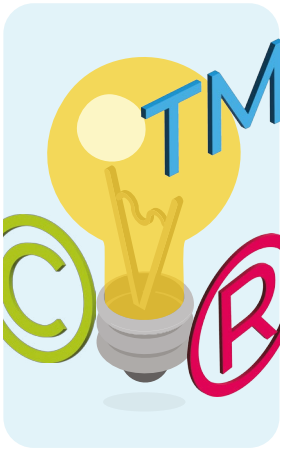
Our policy provides cover for bodily injury arising from technology products errors and omissions.

Products liability: Bodily injury

A medical device company specializing in orthopedic implants manufactured and distributed an anterior cruciate ligament (ACL) reconstruction kit, comprising an anchor screw and rope suture device designed to repair ACL injuries.

The surgical procedure involves drilling into the tibia, securing the anchor screw into the tibia, and feeding the suture through to connect the ligament to the femur. In one reported case, a patient underwent ACL reconstruction using the device, however, due to a design defect, the head of the anchor screw—through which the suture is fed—fractured under stress. This caused the suture to disengage and release, resulting in instability of the knee joint and subsequent tearing of the meniscus.

Our policy provides bodily injury arising out of products manufactured or supplied by the insured.



Errors and omissions: Intellectual property infringement

A specialist R&D service company has created their own proprietary generative AI large language model algorithm, to be used by pre-clinical R&D companies to aid in their research. The model pulls data from scientific publications and databases, allowing R&D customers to ask questions and be offered resources about novel R&D concepts.

Certain R&D authors alleged copyright infringement against the R&D service entity, asserting their AI algorithm was generating responses that were obtained from their research literature without their knowledge and consent.

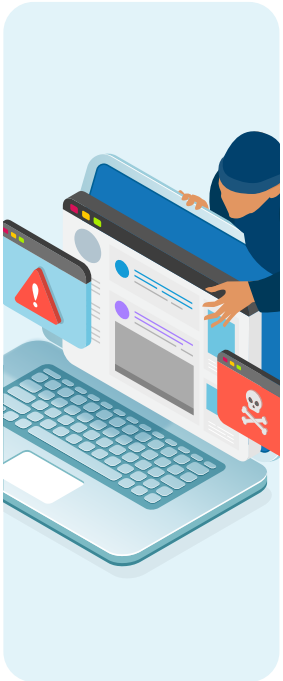
Given the need to access vast amounts of data points to inform generative AI models, the entity had inadvertently not obtained appropriate licenses for the use of all third-party literature used in their algorithm, triggering cover under the Intellectual Property Rights Infringement section of the Errors and Omissions insuring clause.

Product recall

A specialist medical device company manufactures and sells screws, rods, and plates with bone granules from cadavers. The granules provide a bone void filler that remodels to the patient's own bone and fills the bone void to prevent bacteria buildup and infection forming.

The original cadaver bone allograft used as a component in the granules is sourced from a licensed allograft bone biobank. An error in the tissue bank testing procedures failed to pick up the presence of streptococcus spp. This one bone allograft was used to produce a batch of bone granules that was packaged over 100+ products. Unfortunately, the streptococcus spp led to sepsis in one patient who received the bone granules. The official medical device governing body issued a Class II product recall of the medical device companies' bone granule products.

Our policy provides product recall cover that specifically reimburses product recall costs as a direct result of an official regulatory body issuing a Class I or Class II recall.

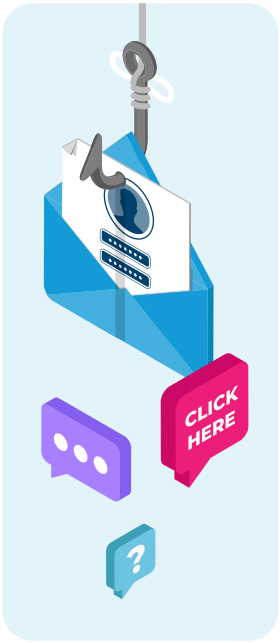


Cyber: Privacy liability, system damage and rectification costs

A clinical research organization (CRO) experienced a sophisticated cyber attack in which a threat actor gained unauthorized access to the insured's computer systems, effectively disabling operations and disrupting the organization's ability to conduct ongoing clinical trials. In addition to the operational impact, prior clinical trial data was lost, and the attackers exfiltrated and published sensitive health information of many of the patients on the dark web.

This data breach triggered investigations by the US Department of Health and Human Services' Office for Civil Rights (HHS-OCR) and several state attorneys general to assess whether the CRO had met its obligations under HIPAA and relevant data protection laws. The insured faced potential regulatory penalties and was required to notify the individuals affected by the data breach, incurring significant costs.

Our cyber cover picks up the incident response costs to remove the threat actor from the CRO's computer systems and the costs associated with notifying affected individuals, as well as any fines or damages stemming from lawsuits or regulatory actions taken against the organization. Our system damage cover also picks up the cost to re-create lost data and reconstitute the CRO's computer systems to the same position they were in prior to the cyber attack.

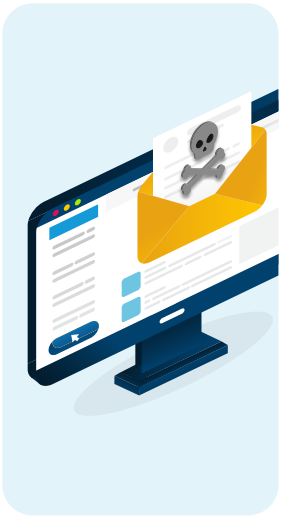


Cyber: Extortion

A specialist spinal surgery company sells and licenses virtual augmented reality software. This software works by reading and analyzing the patients' X-ray & MRI scans. Having read the scans, it enables a 3D visualization of the anatomy while looking and operating directly on the patient. This allows surgeons to visualise the patients' spine as if they have live X-ray vision and accurately navigate instruments and implants during spinal surgery procedures. As a result, the company holds large amounts of sensitive health information.

A threat actor sent phishing emails to the company's HR department, with fake job applications attached. Once opened, the document downloaded malware onto the recipient's computer, allowing the threat actor to gain a foothold into the company's network. From here, the threat actor escalated user privileges and was able to start exfiltrating sensitive health information from the network. Once a significant amount of data had been stolen, the hacker sent the company an ultimatum, threatening to release the data into the public domain unless a ransom was paid. To prevent patient data from being exposed in this way, the company chose to pay the ransom demand.

Our policy provides extortion cover, reimbursing the insured for any ransom payment made in response to a cyber extortion event, including threats to leak confidential information.



Cybercrime

A medical device distributor sells third-party durable medical equipment (DME) to a large number of hospitals and healthcare institutions. The DME is supplied from different suppliers globally. Through the use of a phishing email that tricked the company's finance director into giving up their login credentials, a hacker was able to gain remote access to the director's inbox.

Pretending to be the finance director, the hacker then emailed the accounts department asking them to send $40,000 to a new supplier and attaching a seemingly legitimate invoice. To prevent being caught, the hacker also added that they were on a flight so couldn't communicate by phone. Assuming the request was legitimate, the employee transferred the funds to the fraudster.

Our cybercrime cover provides cover for funds transfer fraud losses, including those caused by social engineering attacks that result in senior executives or employees being tricked into sending money to fraudsters.

Proactive protection

With the threat of cybercrime impacting life science companies more frequently, it's crucial to have the right cover in place.

Every CFC policyholder has access to the CFC Response app, providing vulnerability scanning, threat monitoring and real-time security prevention to help prevent cyber attacks before they happen.

Get in touch at lifescience@cfc.com to find out more.