



MUTUAL INSURANCE COMPANY
OF ARIZONA

CYBER LIABILITY

Reporting a Claim

Cyber Liability Coverage provides limits of \$100,000 per claim and \$100,000 aggregate.

Aggregate limits for an entity will increase based on the number of MICA insured physicians.

If you are a victim of a cybersecurity attack or data breach, time is of the essence. Potential cyber-related claims should be reported as soon as possible.

- Call MICA at **800-352-0402**
Monday – Friday | 8:00 a.m. to 5:00 p.m.
- For urgent matters that occur outside of regular business hours, contact Tokio Marine HCC's breach support team by calling **888-627-8995**.

Please be prepared to identify yourself as a MICA policyholder and provide a policy number, if available, when you contact Tokio Marine HCC. The next business day, Tokio Marine HCC will contact MICA for additional policy information and verify coverage. Expenses incurred are subject to coverage verification.

This literature is a summary description of coverage, and is not intended to be a full statement of the terms, conditions and other limitations of the coverage. For complete details about MICA's Cyber Liability coverage, please refer to Cyber Liability form number MPL-0161 and MPL-0162, or contact MICA or your MICA broker.

Note: MICA does not provide Cyber Liability coverage in Nevada.



CALL MICA

Third Party Insuring Agreements

Security & Privacy Liability –

Coverage for legal expenses and loss resulting from claims alleging liability arising out of a security breach or privacy breach, including allegations of failure to timely disclose a breach and violations of privacy regulations with respect to personally identifiable information.

Multimedia Liability – Coverage for legal expenses and loss resulting from claims alleging copyright or trademark infringement, libel or slander, or plagiarism arising out of dissemination of your media material. Covers both electronic and non-electronic media material.

TCPA Defense – Coverage for legal expenses resulting from claims alleging violation of the Telephone Consumer

Protection Act or similar laws regulating the use of telephonic or electronic communications for solicitation purposes (\$10,000 Sublimit).


Privacy Regulatory Defense & Penalties – Where permitted, coverage for legal expenses, regulatory fines and penalties and/or regulatory compensatory awards resulting from privacy regulatory proceedings brought by federal or state governmental entities due to a privacy breach or security breach.


PCI DSS Assessment – Coverage for legal expenses and assessments (fines or penalties) imposed against you by banks or credit card companies alleging non-compliance with the Payment Card Industry Data Security Standard (PCI DSS).

First Party Insuring Agreements

Breach Event Costs –

 **Privacy Breach Response Costs** – Coverage for reasonable and necessary mitigation costs and expenses incurred by you prior to or following the publication of an adverse media report, including legal expenses, public relations expenses, and IT forensic expenses.

 **Breach Support and Credit Monitoring Expenses** – Coverage for reasonable and necessary expenses incurred by you to provide support activity to parties affected by a privacy breach, including the costs to set up a call center and to provide up to 24 months of credit monitoring services, identity theft assistance services, and credit and identity repair and restoration services.

 **Notification Expenses** – Coverage for reasonable and necessary expenses incurred by you in notifying parties affected by a security breach or a privacy breach, whether such notice is made voluntarily or to comply with privacy regulations, including printing costs, mailing and postage expenses, and the costs to engage a third party to mail notification letters and to prepare substitute or website notices.



Post Breach Remediation – Coverage for post-breach remediation costs incurred by you to mitigate the potential of a future security breach or privacy breach (\$10,000 Sublimit).

System Failure – Coverage for reasonable and necessary amounts incurred by you to recover and/or replace data that is compromised, damaged, lost, erased or corrupted due to an unplanned outage, interruption, failure, suspension, or degradation of service to an insured computer system. Coverage also extends to business income loss and interruption expenses incurred by you because of any of the above events.

Cyber Extortion – Coverage for reasonable and necessary extortion expenses incurred by you and extortion monies paid by you, as a direct result of a credible cyber extortion threat made against you.

BrandGuard® – Coverage for loss of revenue incurred by you as a direct result of an adverse media report or notification to parties affected by a security breach or privacy breach.

Cyber Crime – Coverage for losses incurred by you due to (1) wire transfer fraud, (2) fraudulent use of an insured telephone system, and (3) phishing schemes that impersonate your brand, products or services, including the costs of reimbursing your patients or clients for direct financial losses they sustain as a result of such phishing schemes (\$10,000 Sublimit).

Reward Expenses – Coverage for amounts paid by you to an informant for information leading to the arrest and conviction of persons responsible for a security breach, privacy breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud, or phishing attack (\$10,000 Sublimit).

Court Attendance Costs – Coverage for actual loss of earnings and reasonable costs incurred by you to attend mediation sessions, arbitration proceedings, hearings, depositions, and trials relating to the defense of a claim covered under the cyber liability policy (\$10,000 Sublimit).

