MEDICAL MALPRACTICE JOINT UNDERWRITING ASSOCIATION OF RHODE ISLAND

MANDATORY MFA IMPLEMENTATION
EFFECTIVE OCTOBER 27, 2025

October 13, 2025

Dear Agents and Policyholders,

Effective October 27, 2025, all online users will be required to log in using Multi-Factor Authentication (MFA) when accessing the MMJUA portal.

Please review the instructions below carefully. If you encounter any issues or have questions, email a summary to MMJUAofRI@BBrown.com.

Login Instructions for MMJUA Portal
🔗 https://rimmjua.beechercarlson.com

Step 1: Enter your email address and click "Send Verification Code." The system will email you an MFA code.

Step 2: Log in using your Username, Password, and MFA Code, or select "Recover Password" if needed.

Step 3: If recovering your password, you'll receive a new password via email. Return to the login screen and use the new password along with the MFA code from Step 1. The code is valid for 30 minutes.

How MFA Works

MFA adds a critical layer of protection to your account by requiring a second form of verification. Instead of relying on a single password, MFA requires credentials from at least two of the following independent categories:

- Something you know: This is a password, PIN, or the answer to a security question. These are considered the most vulnerable factors, as they can be stolen through phishing scams or brute-force attacks.
- Something you have: This includes physical or digital items that only you possess, such as a mobile phone, a software-based authentication app, or a physical security key.
- Something you are: This refers to biometrics—unique personal characteristics such as a fingerprint, facial scan, or voice pattern.

How MFA makes you safer

MFA significantly increases security by creating a powerful barrier against common cyber threats, even if one of your credentials is stolen.

- Thwarts password theft: If a hacker manages to steal your password, they are stopped in their tracks because they don't have the second authentication factor, such as your phone or fingerprint.

- Defends against phishing: Phishing scams trick users into revealing their login information. MFA prevents these attacks from succeeding because a stolen password alone is not enough to access the account.

- Reduces risk from common vulnerabilities: Many people use weak or reused passwords across multiple accounts, which increases their risk if one password is breached. MFA makes stolen credentials useless for gaining access, limiting the damage of a single compromise.

- Provides an alert system: If you receive an MFA notification for a login you didn't initiate, it serves as an early warning that someone may have your password. This allows you to immediately change your password and secure your account.

- Protects sensitive data: Industries like finance and healthcare, which handle highly sensitive data, use MFA to protect against fraud, theft, and data breaches. For businesses, MFA compliance can also help avoid legal and financial penalties.

- Secures mobile and remote access: With more employees working remotely, MFA ensures that users securely access company resources from different devices and locations. Adaptive MFA can even increase security requirements for riskier login scenarios, like accessing an account from a public Wi-Fi network.

By implementing MFA, you create a robust, multi-layered defense that dramatically reduces the risk of unauthorized access to your accounts. According to Microsoft, using MFA can prevent over 99.9% of account compromise attacks.

Thank you for your attention and cooperation.

Susan Hughes Mertes
Executive Director
MMJUA of Rhode Island