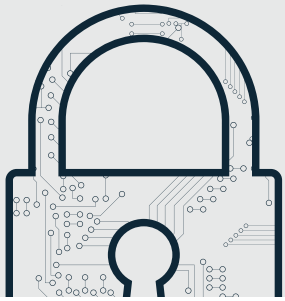
American Arbitration Association® | International Centre for Dispute Resolution®

AAA-ICDR® Best Practices Guide

for Maintaining Cybersecurity and Privacy

Minnesota No-Fault



The AAA-ICDR is committed to the security and privacy of customer and case information. To effectuate that goal AAA-ICDR has implemented best practice policies, procedures and technologies internally to help protect its data and information systems. The protections that have been implemented apply to all case data and equipment stored and managed on the AAA-ICDR technology infrastructure. AAA® employees routinely participate in online training programs designed to heighten their knowledge of security policies and procedures. The AAA has also prepared an *AAA-ICDR Cybersecurity Checklist* which parties and/or their representative as well as arbitrators may use as a resource.

Recognizing that cybersecurity is a shared responsibility, AAA-ICDR is offering to all Minnesota No-Fault arbitrators training courses on Cybersecurity. These programs are designed to educate the arbitrators as to the cybersecurity basics so they can preserve and protect the integrity and legitimacy of the arbitral process in cases in which they are serving.

The level of cybersecurity that should be implemented during arbitration ultimately rests with the parties and the legal advisors. The American Bar Association has issued two opinions regarding a lawyer's obligations either after an electronic data breach or cyberattack (Formal Opinion 483) or when securing email communication of protected client information (Formal Opinion 477).

In accordance with the ABA guidance, legal counsel in consultation with their clients should assess the nature of the information to be shared during arbitration and the impact of a cybersecurity breach on their client's business. A risk assessment should be undertaken in which counsel and the client identify whether highly sensitive data, such as personal, classified, financial, commercial or confidential information, is pertinent to the dispute and whether a particular approach must be taken during the collection, storage and transmission of such data to opposing counsel, arbitral institutions and arbitrators.

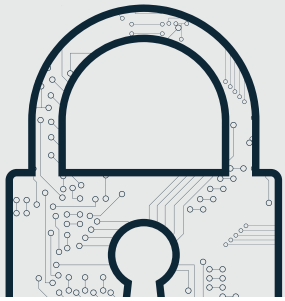
The following best practices are designed to provide guidance to parties, their representatives, and arbitrators regarding cybersecurity measures they should consider adopting. It does not impose hard or fast rules, but rather encourages an in depth discussion of the potential risks and reasonable and proportionate protective measures that might be taken to better secure sensitive information. These best practices are not intended to ensure compliance with any applicable laws, regulations, professional or ethical obligations.

1. Representatives should evaluate whether they plan to exchange information that presents a heightened need for cybersecurity, such as confidential information or personal data. If so, how will this information be transferred?
2. If there is a necessity to exchange such information, parties' representatives should engage in discussions early in the process to determine how each will exchange such information.

AAA-ICDR® Best Practices Guide

for Maintaining Cybersecurity and Privacy

Minnesota No-Fault



3. In connection with the above, parties' representative should discuss the following:
    a. Does this case require an enhanced level of cybersecurity, privacy or data protection? If yes, why?
    b. Is there confidential information that will require specific security practices and measures? If yes, how should these specific practices and measures be incorporated in this proceeding?
    c. How do participants plan to ensure that all case related email communications are secure? Should document transmission take place by email or some other more secure method?
    d. How do participants plan to ensure secure exchange and storage of electronic versions of case related documents and files?
        i. Are the participants willing to use AAA WebFile® and Panelist eCenter® in lieu of email?
4. Once the hearing has been scheduled, representatives should review the Notice of Hearing to identify the arbitrator's preferred method of delivery for hearing materials. If the information to be transferred requires a higher level of security, the representative should notify the case administrator.
5. Arbitrators should carefully consider any requests for heightened security of the delivery of hearing materials when a representative provides notification that the materials will include confidential or sensitive personal identifiers, including national identification numbers, dates of birth, medical health information, privileged information, credit card or financial account numbers, or other personal information.
6. When and how should case related documents be destroyed by the participants?
7. The parties' agreement on the cybersecurity measures to be employed should be adopted by the arbitrator unless the arbitrator determine that applicable law requires additional security measures.

120 Broadway, 21st Floor
New York, NY 10271
Telephone: +1 800.778.7879
information@adr.org