ARIAS•U.S. Practical Guide for Information Security in Arbitration

DRAFT

Introduction

This Practical Guide, and the accompanying checklist, is provided by ARIAS•U.S. to help participants in insurance and reinsurance arbitrations address issues of data privacy and cybersecurity. Most companies and law firms have IT and privacy professionals to help them maintain the security of confidential information. This Practical Guide is drafted primarily to provide guidance to arbitrators and to outline how companies and law firms can help arbitrators comply with the responsibility to secure and protect confidential information. Arbitrations often involve the exchange of regulated forms of information, such as "personally identifiable information" and "protected health information," or other information that is sensitive from a business operations standpoint. Moreover, as stated in the ARIAS•U.S. Practical Guide to Reinsurance Arbitration Procedure, most parties to arbitration prefer that the proceedings remain confidential. Indeed, it is generally agreed throughout the industry that reinsurance arbitrations are and should be confidential in most circumstances, even absent the parties' complete agreement. Accordingly, the ARIAS•U.S. standard confidentiality form broadly classifies *all* information exchanged in an arbitration as confidential "Arbitration Information."

Personally Identifiable Information ("PII") – Under United States law, in general, personally identifiable information is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. This information is regulated currently by the data breach notification statutes of 47 states, plus Puerto Rico, and by a host of industry specific regulations and guidance documents.

Protected (or Personal) Health Information ("PHI") – The HIPAA Privacy Rule protects all "individually identifiable health information" that is, with some exceptions, (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Individually identifiable health information is information, including demographic data, that relates to (a) the individual's past, present or future physical or mental health or condition, (b) the provision of health care to the individual, or (c) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

Arbitration Information ("AI") – Generally defined as all briefs, depositions and hearing transcripts generated in the course of an arbitration, including documents created for the arbitration or produced in the arbitration proceedings by opposing parties or third-parties, final award and any interim decisions, correspondence, oral discussions and information exchanged in connection with a confidential arbitration proceeding.

The handling of sensitive business and personally identifiable information requires care, thoughtful processes, and deliberate action. Companies, counsel, and arbitrators are encouraged to consider and discuss these issues early and throughout the arbitration process. Even though all information exchanged in the typical reinsurance arbitration is usually considered to be confidential, not all information is equally sensitive and therefore, different procedures can and should be implemented for specific circumstances. Therefore, keeping in mind the proviso that arbitrations involving PII or PHI may require additional precautions beyond those listed below, it is a sound practice for all participants to consider applying, at a minimum, the practices described below to *all* information relating to confidential arbitrations.

****

Table of Contents

I. Organizational Meeting

At the organizational meeting, the parties and panel should discuss:

- Whether the parties are likely to exchange PII, PHI or other types of regulated or sensitive information.
- If the parties anticipate that these types of information or documents will be exchanged, they should ask whether that exchange is truly required and necessary. If there is no reason why this information must be exchanged, consider steps to avoid the exchange. For example, ask whether a column of a spreadsheet may easily be removed or documents be redacted.

The parties and panel should also discuss:

- Whether the parties are likely to file/submit to the panel, PII, PHI or other types of regulated or sensitive information.
- If the parties anticipate that they will file/submit this information, ask whether the filing/submission is truly required and necessary. If there is no reason to file/submit PII or PHI, consider steps to avoid the filing/submission of this information.

Document the treatment of Confidential Information. The parties and panel should address the requirements of exchanging and submitting AI, PII and PHI. For example, they may consider incorporating these issues within the Confidentiality Agreement signed as part of the arbitration, the Scheduling Order, in arbitrator engagement letters, and/or in arbitrator hold harmless agreements, *e.g.* the company will hold the arbitrators harmless for claims associated with the disclosure of Confidential Information provided they follow certain practices, such as those outlined in this Practical Guide.

Discuss mode of transmission. If Confidential Information is to be exchanged and submitted to the Panel, the parties should agree on a transmission mode for Confidential Information. See the discussion below for transmission options.

Exchange passwords in person. At the organizational meeting, the parties should consider exchanging passwords in person for encrypted files – the password should never travel with the encrypted files.

Cross-border transmission. Sending PII or PHI across national borders can trigger special obligations. If the cross-border transfer of PII or PHI is necessary, the parties should speak with each company's privacy officer and the parties should discuss with the arbitrators any special processes that will be required by any of the applicable jurisdictions.

II. Confidential Information at Rest

The goal is to ensure that all Confidential Information "at rest" is kept secure. "At rest" means information maintained in some form of persistent storage, for example hard copy paper, laptop computer disc, or a portable electronic storage device.

In general, there are two ways that Confidential Information can be stored "at rest": electronically and in hard copies (generally, paper). Care should be taken to ensure that both are secure.

A. Hard Copy Confidential Information

The guidance provided below for storing hard copy confidential information can be neatly summarized as putting into place, and maintaining, a "clean desk" policy for your workspace. Indeed, many companies have a "Clean Desk Rule" for their employees.

1. Equipment Necessary

To implement this policy, arbitrators need a few items of basic equipment that most likely already possess. Every arbitrator working on a matter involving Confidential Information should have a drawer, desk, or safe that locks. Arbitrators should also have an office shredder.

2. Practical Guidance

Once you have the basic equipment, follow the following policies:

- If possible, use a single dedicated space for your workspace when you have to access or review Confidential Information, such as an office. Where practicable, restrict access to that workstation, and secure your workstation when you leave to prevent unauthorized access.
- Follow a "Clean Desk" rule – remove Confidential Information from the top of your desk and lock it in a drawer when the desk is unoccupied and at the end of your work day.
- Close and lock file cabinets containing Confidential Information when not in use or when not attended.
- Do not leave the keys used for access to Confidential Information at an unattended desk.
- Immediately remove from the printer or fax machine documents containing Confidential Information.
- Erase whiteboards containing Confidential Information.
- Treat mass storage devices such as CD-ROMS, DVDs, or USB drives (sometimes called "flash drives" or "thumb drives") as sensitive and secure them in a locked drawer.

B. Electronic Confidential Information

Managing electronic Confidential Information is slightly more challenging than securing hard copy documents, but nevertheless can be done with some basic principles.

1. Equipment Necessary

You should absolutely invest in a computer (laptop or desktop) with **full disk encryption** or software for full disk encryption. Full disk encryption is described more fully below with example products that can be used.

Use and update regularly **anti-virus software**. Most anti-virus software or third-party providers include an option that prompts you to install updates. Take advantage of these options.

We recommend that you invest in a surge protector or battery power backup for your computer, as well as a cable lock or locking desk drawer for laptop storage.

2. Practical Guidance

- Use a dedicated computer for your arbitration work. Do not allow friends or family to use that dedicated computer.
- Any computer that contains Confidential Information should employ "whole disk encryption," and the whole disk encryption should be deployed.
    - Encryption is a process by which data is transformed into a format that renders it unreadable without access to the encryption key and knowledge of the process used.
    - Whole disk encryption comes standard with many newer Apple computers ("FileVault") and PCs using Windows 10. It is also available using certain commercially available software, including McAfee Complete Data Protection, Symantec Endpoint Encryption, Sophos Safeguard, Microsoft BitLocker, Dell Data Protection/Encryption, Apple FileVault 2, and Trend Micro Endpoint Encryption.
- Use commercially available, standard, supported anti-virus software. Download and run the current version; download and install anti-virus software updates as they become available.
- **Important:** We cannot overemphasize the importance of a strong password. Your passwords should meet or exceed the attached "Password Guidelines." *See below*.
- Enable a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password should comply with the Password Policy.
- Never leave passwords on post-it notes attached on or under a computer, nor should they be written down in an accessible location.
- Logoff of your computer when you are not using it.
- Turn off your computer when you are done working or at the end of the day.
- Exit running applications and close open documents when your work is complete.
- Ensure that your workstation computer is protected with a surge protector (not just a power strip) or a UPS (battery backup).
- Recommended: Secure laptops using a cable lock or lock the laptop in a drawer or cabinet.

- We do not recommend using portable electronic storage devices such as thumb drives, CD-ROMs, or DVDs, to store Confidential Information. However, if you do use these devices to store electronic devices, the Confidential Information must be encrypted.
    - There is commercially available encryption software that permits encryption of portable electronic storage devices, including McAfee Complete Data Protection, Symantec Endpoint Encryption, Sophos Safeguard, Microsoft BitLocker, Dell Data Protection/Encryption, Apple FileVault 2, and Trend Micro Endpoint Encryption.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding.
- Regularly empty your Trash folder.
- Never download files from unknown or suspicious sources.
- WiFi Routers - All home or business wireless infrastructure devices should adhere to the following standards:
    - Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS – this information should be printed on the box or in the instructions that come with the device.
    - When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point – many devices have a randomly generated password already configured for that router.
    - Disable broadcast of SSID.
    - Once operational, consider changing the default SSID name.
    - Regularly change the device password – quarterly or twice yearly.
- Smartphones: If you send or receive Confidential Information using a smartphone, you should have the smartphone password protected and have it set up so that the screen locks if not used within a relatively short time period (i.e., one minute).
- Avoid using public WiFi when possible. If necessary, however, the use of public WiFi connections is acceptable if you are otherwise following the practical guidance outlined above.
- Do not access Confidential Information using a public computer.
- If you are printing documents containing Confidential Information in a public or office environment, do not leave confidential documents at the printer. Also note that many printers have secure printing options that allow you to send your confidential print jobs and hold them in the print queue until the user comes to the printer.

The law, regulations, guidance documents, and technology changes. Particularly if your arbitration will involve the submission of PHI, a full discussion of the most up-to-date requirements under HIPAA (or its state-based equivalents) should take place with the parties so that you understand any additional practices that must be followed.

III. Confidential Information in Motion

Confidential Information "in motion" includes data being transmitting over public, untrusted networks such as the internet or data being transmitted within private, trusted networks, and includes hard copy information or electronically stored information (often referred to as ESI) being physically transported by mail or other delivery service.

A. Electronic Transmission of Confidential Information

The following provides guidance for handling Confidential Information "in motion."

1. Equipment Needed

Use a secure email service provider. Gmail, Hotmail and other commonly used "free" email services tell you in their terms of service that they are essentially reading your emails. Some examples of secure email services are Proton Mail, Tutanota, and Lavaboom, all of which have free versions that are secure.

If you are using an email service provider that is not fully encrypted, such as those described above, use one of the commercially available services that allow for the secure transmission of attachments (*e.g.*, HighTail, Citrix Sharefile).

2. Practical Guidance

- Consider using an encrypted email service.
    - You can invest in a commercial email account. There are numerous high-security options available for a small fee. For example, instead of a Gmail account, you can use Google Apps for Work.
    - You may also use a free service, including the following high-security options - Proton Mail, Tutanota, and Lavaboom.

      Important: For many email products, you don't just get encryption "out of the box"; you have to take steps to enable the encryption, but the commercially available services have "Help Desks" that can help you make sure your email is encrypted.

        - **Note:** We recognize that many arbitrators currently use free email services like Gmail, Yahoo, and Hotmail. Many of these services now advertise that emails are encrypted; however, there have been reports of breaches in these services. Moreover, these services' Terms of Service all warn that the companies may scan the content of your emails. We do not, therefore, recommend those services as a first-line choice for confidential arbitrations. If you must use one of these services, all Arbitration Information should be attached to emails using password-encrypted attachments. Documents that are compressed using "Winzip" can be password encrypted. Moreover, most versions of Microsoft Excel, Microsoft Word, and Adobe Acrobat permit password encryption of individual files.

- Consider enabling "two-step authentication," also called "two-step verification" or "cell-phone confirmation," to secure your email account. The secure email services above provide for this. Two-step authentication uses a password for your account and some other method of confirming your identity. For example, you can set up a trusted mobile device on which you will receive a verification code. With two-step authentication, someone can try to gain access to your email with your password, but cannot do so unless they also have your cellphone. *This does not require the user to input two passwords every time you log onto your email. It requires the password and the authentication code when you log into your email from a new computer. Once you log in from that computer, the authentication code is not required for subsequent log-ins from that computer.*
- Set up a dedicated email account for your work as an arbitrator and, to the extent possible, use that account only for business.
- Whenever possible, no Confidential Information should be contained within the body of the email, but within a secure, encrypted attachment.
- Create a strong password using the "Password Guidelines."
- Highly sensitive information should be transferred or access given by a secure method. For example, a File Transfer Protocol (FTP) transfer can be used to downloaded information directly to your encrypted computer. Most law firms will have dedicated FTP transfer capabilities and counsel can assist with how to upload and download documents. In the alternative to transferring information, firms and companies can set up virtual data room a/k/a "Deal Rooms" where information can be securely accessed by only those given access. The "Deal Room" can be set up such that information cannot be copied, downloaded or otherwise removed from the deal room, making the issue of deleting files inapplicable.

B. Physical Transport of Confidential Information

You may have to travel or physically transport Confidential Information. When that is the case, follow these tips.

1. Equipment Necessary

- If you use your laptop on planes or in public places, invest in a physical laptop privacy screen, which are very inexpensive. These screens keep people from seeing your screen unless they are directly facing it.
- For your mobile device or your laptop that contains Confidential Information, you might consider a laptop security product that allows you to remotely locate/disable/wipe clean a laptop that has been lost or stolen. For these to work, the device needs to be connected to the internet, so it is important that the computer or mobile device have full disk encryption as described above. Also, these features or products must be configured before the device is lost/stolen, so plan ahead. Apple has the "Find My" services available for its devices. Android has a built in Device Manager feature that you can enable. For laptops, there are many third-party apps and pieces of software that you can use for remote tracking and wiping of the computer.

2. Practical Guidance

- Avoid traveling with Confidential Information.
- Avoid traveling with portable electronic storage devices (e.g., thumb drives). They are small and can easily be lost or misplaced. If you travel with one of these devices, encrypt it. And, you must not keep the encryption key with the device. A better option is to transfer the data to a secure computer (i.e., encrypted) and return or destroy the device.
- Avoid sending PII or PHI via hard copy if possible. Insist that counsel redact unnecessary PII or PHI that will be transmitted in hard copy.
- Avoid using your laptop to work on Confidential Information in public spaces – but if you do, consider investing in a laptop privacy screen.
- Do not check bags with Confidential Information and do not check your laptop.

IV. Disposal of Confidential Information

The lifecycle of Confidential Information ends with disposal. When disposing of Confidential Information, follow these practices:

A. Hardcopy Confidential Information

1. Equipment Necessary

- Shredder (cross-cut or diamond, preferable)

2. Practical Guidance

- Review any confidentiality agreement or other agreements that discuss obligations for disposal of Confidential Information and follow them.
- Shred Confidential Information or send back to the party that filed it.

B. Electronic Confidential Information

Simply deleting a file on your laptop generally removes only the reference to the file, not the file itself. Special steps need to be taken to securely delete electronic files. Keep in mind that, even if you do not save Confidential Information on your computer, care should still be taken. For example, if you open a file sent to you, but do not save a copy of that document on your computer, your computer may very well store a version of that document as a temporary or other file.

Information on external hardware (a disk or drive) can be destroyed by destroying the hardware itself, i.e. the hammer or shredding method. The following deals primarily with disposing of files stored on your computer.

1. Equipment Necessary

- Computer with secure file deletion capabilities
  - Recommendation: Update your computer software and operating system regularly. Use software that employs the most up to date standards. Currently, appropriate software will disclose that it is compliant with the U.S. Department of Defense 5220.22-M standard (3 pass or 7 pass) or Guttman method (overwriting 35 times).

2. Practical Guidance

- Windows
  - Download and use a file deletion program. For example, you may consider:
    - Fileshredder: www.fileshredder.org
    - Eraser: www.eraser.heidi.ie
    - Secure Eraser: www.secure-eraser.com

- Entire hard drive deletion. Use only if wiping an entire hard drive. ***Be very careful with this program***, as it could wipe the wrong drive if you are not careful.
    - Darik's Boot and Nuke: www.dban.org

- Apple
    - Single file deletion: Drag item into Trash, then choose Finder > Secure Empty Trash (OS X Yosemite and prior).
    - For operating systems OS 10.11 or later, you can download the product Permanent Eraser.
    - To erase the entire hard drive, you can use the Disk Utility, secure erase option.
    - Apple SSD drives: Enable whole drive encryption (FileVault 2)

- Portable Electronic Devices
    - Secure deletion using a minimum of 3 pass deletion
    - Destruction: Some shredders permit destruction of CD-ROMs and thumb drives. Physical destruction works nicely for thumb drives.

V. Incident Response – "*Break the Glass*"

- Things happen.
- You are obligated to report potential compromises of confidential information because, among other reasons, the companies and law firms should be able to assist you in determining the extent of any issue and help mitigate the issues. In addition, companies and firms may have reporting requirements when they or one of their vendors has a potential incident.
- There are various scenarios that can trigger your reporting requirement to the parties, including times when you are not even certain that Confidential Information has been compromised. Some of these scenarios are obvious, for example, you leave a pile of paper in your hotel room after checkout or on the seat of a taxi. Or, you receive a "ransomware" note from a bad actor who has locked down all of your data.
- Examples of potential incidents that should be reported are: a package of papers arrives to you and had been opened already or a thumb drive (even encrypted) was in your suitcase that the airline lost.
- When something happens:
    - Stop. If you are dealing with a potential breach by a third-party, do not proceed on your own.
    - Report to everyone – parties and firms.
    - Today, not tomorrow.

Strong Password Tips

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

Avoid writing down passwords. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

- (NOTE: Do not use either of these examples as passwords!)
- Considering using a passphrase. A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

Change your password periodically. Changing passwords on a quarterly or bi-annual basis is ideal.

Practical Guide for Information Security in Arbitration

Checklist

This checklist is intended to be used with the Practical Guide and is not a substitute for the full document.

I. Organizational Meeting

Discuss whether the parties are likely to exchange PII or PHI and whether they must.

Discuss whether the parties will be submitting/filing PII or PHI to the Panel. If not required, try to avoid submission.

Address the requirements of exchanging and submitting Confidential Information through the Confidentiality Agreement, Scheduling Order, arbitrator engagement letters and/or in arbitrator hold harmless agreements.

Agree on a transmission mode and consider exchanging passwords for encrypted files.

II. Storage at Rest

Clean Desk rule for paper documents.

Use password protected computer with encryption.

Keep anti-virus software up-to-date.

Never download files or click on links from unknown or suspicious sources.

Password protect your smart phone and use the timed screen lock feature.

Avoid using public WiFi when possible.

III. Storage in Motion

Use an encrypted email service dedicated for your work activity or take other precautions described in the Practical Guide.

Transfer Confidential Information via an encrypted attachment, not in the body of the email.

Create a strong password.

Highly sensitive information should be transferred or access given by a secure method, e.g. FTP or a Deal Room.

IV. Disposal

Shred paper documents to return them to the party that filed them.

Use the most up to date deletion standards for electronic files.

Use entire hard drive deletion if you want to wipe everything on your computer.

For Portable Electronic Devices (CDs or thumb drives), delete using a minimum of 3 pass deletion or physically destroy.

V. Incident Response – "*Break the Glass*"

Stop.

Report to everyone – parties and firms.

Today, not tomorrow.