Information Security in Arbitrations

Three experienced arbitrators discuss how the arbitration community should assess and adopt best practices and strategies for identifying and protecting private information.

By John D. Cole, David A. Thirkill and Daniel E. Schmidt, IV
Moderated by Robert N. Hermes and reported by Douglas Winter

Bob Hermes recently sat down with three experienced arbitrators—Dan Schmidt, David Thirkill and John Cole—to hear their experiences in this area, how their awareness of these issues has been heightened, and how they themselves have adopted practices for protecting confidential information.

MR. HERMES: We have all seen news reports about the problems associated with the disclosure of personal information as a result of cyber security breaches at companies and government offices. Insurers have reported that 101.4 million people were affected by data breaches in 2015.

It's interesting to note that it wasn't that many years ago that most of us in the arbitration community had never heard of personal identifying information (PII) or personal health information (PHI). Now we are more attentive to things like encrypted computers and password-protected computers.

However, as discussed at the Fall ARIAS conference, the arbitration community has come to recognize that in the course of an arbitration, panel members may be provided with personal information and medical information of individuals involved in underlying claims. This is especially true for proceedings involving financial insurance products like annuities, credit indemnity, mortgage insurance and managed care disputes. Arbitrators, like the companies and their counsel, must be mindful of best practices and strategies for identifying and protecting private information.

These practices in many ways are steps we all should consider incorporating into the way we protect our own personal information, as well as the confidential information we are entrusted with, as attorneys and arbitrators who assist companies in resolving their insurance and reinsurance disputes.

The first question I have for the group is: Have you been involved in arbitrations in which it was necessary for the panel to receive personally identifiable

information? That is, information that can be used to identify, contact or locate a person?

MR. SCHMIDT: Well, I started in this business of actually serving on arbitration panels in 1987. We received that information in the form of underwriting files and claim files and what have you, without much comment and without much concern. As a panel, we did not really need the personal information, it was just provided to us.

I do not even recall that the issue of confidentiality, in the late '80s and even into the early '90s, was much of a consideration, let alone some of the other issues we'll be discussing about protecting this material.

Over time, particularly after ARIAS U.S. became involved in helping us better organize arbitrations and when the confidentiality agreement came out and was used widely, people were aware that they had to keep this information confidential.

MR. HERMES: David, what about you? Have you had arbitrations where it was necessary for the panel to receive personally identifiable information?

MR. THIRKILL: I have not. And perhaps that goes to Dan's point, about the necessity for such information.

As a panel, we are most often focused on the contract between the insurance company and the reinsurance company. But, we often get information regarding the underlying claims. For example, asbestos claims, we may learn the identification of individuals who suffer from some of the more horrendous parts of asbestos injuries, mesothelioma, and so on. I'm sure all three of us have done clergy abuse and similar claims where we received information about individuals who were molested.

So we get the information. Whether it's actually necessary or not is something else altogether. It's necessary in the sense of its cumulative effect. But the individual information is not necessary and could perhaps be eliminated. But then of course, that leads into, particularly in an electronic sense, how and where and who gets to pay for it.

MR. HERMES: John, what about you?

MR. COLE: Just to add one thing to what Dan and David mentioned. I'm asked, from time to time, to do premium audit disputes based upon issues with respect to loss-sensitive, large account programs. And at times in those cases—not always, but at times—the handling of individual underlying claim files becomes an issue.

A policyholder, for example, will challenge the propriety or professionalism of the claim handling. And in those cases, PII and PHI both may be contained within those individual claim files. So that is an area that is somewhat of an exception. It's a relatively small percentage of what I do and I suspect what most of us do. But that certainly is one example where the spectre or the potentiality of the need for confidential information may be present.

MR. SCHMIDT: I would add one more thing. And I'm sure that John and David have gone through this as well.

Often, one or the other party or counsel would redact information that would identify who the claimants are. That's particularly true where hard copy files or copies of hard copy files were presented to the panel.

We also had heightened confidentiality agreements where a limited number of copies would be made and people would receive copies on a need-to-know basis. Those are some other protections that we used.

MR. HERMES: Let's focus now on what's even more sensitive than personally identifiable information, that is, information that can be used to identify, contact or locate a person, and instead focus on the so-called PHI, personal health information, which is information relating to an individual's health that identifies the individual or can be used to identify the individual.

Have you had occasion to have PHI find its way to you in the course of resolving an arbitration?

MR. THIRKILL: Yes. But until recently, I don't think the parties, counsel or panel focused on the information per se, because the PHI was interesting but unnecessary in its complexity and detail and could well have been redacted.

Given the statutory protection of PHI under HIPAA, etc., parties and counsel really need to assess the need for providing such information to the panel.

MR. HERMES: John, what's your experience been with PHI?

MR. COLE: Well, first, I think an over-arching point that I think we all are in complete agreement on is that the sensitivity regarding this information, as Dan and David have alluded to, is simply much higher than it was a decade ago.

The second observation that I would make is that arbitrators don't introduce evidence or provide evidence within the arbitration hearing. It comes from the parties and it comes more directly to us, of course, from counsel. And I suspect that this requires and will increasingly require an emphasis on counsel understanding the record and

being able to determine the extent to which, if at all, the PII or PHI may be contained in any documents that they wish to present to us.

MR. HERMES: Dan, anything you would like to add?

MR. SCHIMIDT: I would just add that, in my pretty recent experience, some cases have not handled PHI with any greater care beyond the typical confidentiality agreement and destroy at the end. They were life settlement cases so the panel received detailed medical and personal information regarding underlying insureds. Yet we employed only the standard confidentiality provisions. So, the heightened concern for PHI is quite new in my experience.

MR. COLE: Bob, if I could add real quickly. I was in an organizational meeting recently in New York in a case that, by at least its character, you would have believed that there may have been the potentiality of protected information to come out.

And when asked by the panel, the parties, represented by two very, very sophisticated law firms, did not anticipate there would be any need to protect that information in any kind of particularly careful or comprehensive way.

And again, counsel certainly had a better understanding of the potential document production, but the degree of awareness and sensitivity may not be uniform across the board, as we all increasingly have to grapple with this.

MR. HERMES: Dan, let me shift to you for a minute. What's been your experience with actually engaging in a discussion with the parties, panel members and counsel on the topic of PII or of PHI and what steps need to be taken to keep that information secure and confidential? Have you had discussions like that?

MR. SCHMIDT: Yes. Over the years, the topic typically came up in a discussion of the confidentiality agreement and an effort to ensure agreement as to what it meant and what it applied to.

We did not use the acronym PII or PHI. We talked in terms of enhancing the confidentiality agreement.

I have also spent a lot of time talking at organizational meetings about redaction. Again, it may or may not have fit the definition of PII or PHI, but there was a lot of sensitive information in there, so the parties wanted to ensure that details that might reveal a person's identity would be redacted before disclosure to the panel or third parties.

MR. HERMES: David, what about you?

MR. THIRKILL: I think the one thing perhaps that we should recognize is while PII and PHI information areas are particularly sensitive, in effect, anything that's subject to a confidentiality agreement and could be confidential is possible to be hacked and could possibly be used. We don't know where. So the issue of what do we do is perhaps a little wider.

Thanks to a ruling last year, that while idiosyncratic and certainly unique, nonetheless, opens a possibility for error, panels now routinely add an item to the agenda in relation to when do ex parte communications reopen. And so that normally goes on an agenda now. I suspect that the same thing will happen with respect to protecting PII and PHI.

I also think that it is something that ARIAS could look to make sure that it's on the agenda. It can be raised. And each time that happens, people's awareness becomes heightened and it becomes much more easy to deal with.

MR. HERMES: John and Dan, would you care to comment on David's suggestion that perhaps it ought to become a standard agenda item for discussion at all organizational meetings?

MR. SCHMIDT: I'm happy to comment on that. I completely agree with David on that. And I believe that ARIAS could help a great deal by putting it in their standard agenda.

I would also suggest ARIAS advise arbitrators that newly-formed panels should include it in their organizational letter that attaches the agenda. Umpire questionnaires should also seek confirmation of password protected encrypted computers and any other special confidentiality protections the parties feel are necessary.

MR. COLE: Let me both agree and add that I think over time, uniformity will become even more important.

In the organizational meeting that I made reference to, it was actually very positive that counsel brought up the issue, kind of sua sponte, it was not—as David alluded to—a specific item on the agenda for the meeting. I have not seen that yet. The more uniformity that we wrap around this subject in terms of covering any and all requirements necessary for the proceedings, the better.

MR. HERMES: Now I'd like to put you guys on the spot a little bit more and get a little more personal in my questioning.

And, Dan, let's start with you. Would you mind sharing with us what steps do you personally employ as a matter of routine to keep information that you are provided in the course of an arbi-

tration confidential, especially with respect to your computer practice?

MR. SCHMIDT: Well, looking first at the computer practices, only late last year were all my devices encrypted. I have always had pretty strong passwords.

I confess to not having changed them very frequently over time. But that's something that I'm definitely going to change.

With respect to the screens themselves, they are password-protected and they go off pretty quickly. As a matter of course, they always have. And with respect to hard copy documents, I have offices in New Jersey and Arizona that I use for work. If I'm not there, they are locked.

I also have a safe in Arizona, a fairly large safe that anything that's particularly sensitive can go in there. I have not had any such material. But I could use that if needed.

MR. HERMES: David, what about you?

MR. THIRKILL: Well, I'm slightly more of a dinosaur than Dan in that regard. I do have my computer, my laptop and my cell phone encrypted as best I can.

I remember seeing an ad relatively recently, sometime in the middle of last year, which really spurred me on, which had an "encrypt now or you will regret it later" type heading.

I mean, for example, iPads and iPhones can have fingerprint technology to get in now. You can encrypt your computer quite easily through various, you know, Geek Squads. One day I actually went to the Apple store and went through a short course with them at the "idiot bar" or whatever they call it. So I do my best.

I don't have locked facilities for sensitive information. But, I do live in the woods in New Hampshire, so there's not too many people that break in around there.

I do have a suggestion though. Some while ago, I'm not sure which ARIAS meeting it was at. But I think it was in New York. They had a photographer there. And if you turned up, you could go have your photograph taken. And, I think the arbitrator community would welcome and participate in a similar process at a conference where they could be taught by IT professionals how to protect their computer.

MR. HERMES: John, anything you would like to add? Will you share your security practices?

MR. COLE: First of all, I have the advantage of being a partner in a large law firm. So as a matter of course, everything that I do through our system is encrypted. And I assure you they spend thousands of hours on our IT support team. And often we have to change passwords and take other steps in order to make sure those safeguards are in place.

At home, I do have a locked office and my cell phone is encrypted.

MR. HERMES: Turning to the issue of what needs to be done when an arbitration concludes, I have two questions for the group. First of all, what's been your experience with respect to having a discussion, either at the outset or at the termination of the proceeding, as to what should be done with the confidential information and materials that parties and counsel have provided to you. And absent any discussion on that, what's your practice?

MR. SCHMIDT: I would say that in the vast majority of my cases, there's been no specific discussion concerning that.

At the other end of the spectrum, in the rare instances where the material was focused on because it was so sensitive, we had very specific and explicit discussions with respect to either returning the documents or the destruction of the documents. And that includes electronic information.

My default practice has been to destroy all documents by employing shredding companies.

I have always watched such destruction and received a certificate of some sort verifying what was destroyed.

MR. HERMES: Has anybody ever asked you to return material?

MR. SCHMIDT: Yes. Because it was very sensitive information. And my vague recollection is it had more to do with proprietary information than some insured's or third party's name and identification number related to their business. The parties required us not to make any copies beyond those that we had received and they wanted them returned when we were done.

MR. HERMES: John, what's been your experience with destroying or returning information at the conclusion of a proceeding in which you have been a panel member?

MR. COLE: I have only had one case where it was required. It was particularly sensitive information regarding minors. And I will just leave it at that. So, as a general rule, it's quite an exception.

I return everything in hard copy to my firm that has a very rigorous policy with respect to hard copy documenta-

tion and storage.

So again, I have, I suspect, I'm at somewhat of an advantage, from having the luxury of that kind of support.

MR. SCHMIDT: If I could just jump in. I think you have to retain documents at least three to six months because of the time within which a challenge to an award can be raised.

I retain files that I think might be subject to a challenge or have been challenged. And I keep them until the ultimate resolution of the case. And that can be years, sadly. And then I deal with it after that.

MR. HERMES: Let's shift to a different topic.

My and my law firm's awareness and sensitivity to protecting confidential information really became heightened and our focus sharpened when we began to receive requests from our insurance company clients that we certify to them that we practice certain security measures at the firm with respect to how we protect information on our computers and how we protect hard copy information, especially hard copy information that contains PHI.

As a practical matter, if you were involved in a proceeding where the parties involved wanted some type of written certification of practices or procedures that the panel members would follow in the course of an arbitration proceeding, do you have any views as to how that could best be documented or where that should be memorialized?

MR. THIRKILL: The typical arbitration clause is narrow with respect to arbitrator qualifications other than the usual either active or retired director or officer of an insurance company or reinsurance company or underwriter at Lloyd's.

There's nothing in it that says, for example, needs to have an encrypted computer. And I guess we're straying into an area of — it's one thing talking about responsibility, but we're straying into an area that talks about panel selection.

Now, I have never seen perhaps an item on the questionnaire form that, if it was there and it said, relative to umpires, do you have an encrypted computer? Does that mean that if that individual does not, he or she will not be a candidate? Well, very possibly so. Should that be extended on to arbitrators? Well, very possibly so.

But it is an issue that has to be addressed first. Because you can't afterwards, once the panel is formed, then say oh, well, we can't give you information because you are not encrypted. In other words, we have to deal with the issue at a macro level before we can deal with it at a micro level.

MR. COLE: I think human nature tells us that we tend to react as either groups or individuals at either extreme of the spectrum. We either do too little or don't do enough. And probably it's not controversial that that's the stage that we would find most of us in terms of our awareness of these issues. But at times, and then in reacting to them, we do too much or more than is realistically appropriate or proportionate to the problem.

That's why I really tend to favor having ARIAS take a look at this issue, and a broad look at this issue to encompass parties, counsel, as well as arbitrators in terms of what standards might be applicable. I think that generally gives you the best informed view, if you will, from a lot of different constituencies and allows you to make good judgments in making progress and addressing it.

As respects the issue as to at what point this will become something that becomes part of what arbitrators have to consider in terms of being able to certify or make clear, I think that's a completely fair subject for that kind of broad ARIAS discussion.

MR. SCHMIDT: This topic should be front-ended as much as possible—particularly if counsel and parties believe that this can be an issue—to make sure that the selection of their arbitrator and the people who are nominated as umpire are qualified or willing at least to do what's necessary to protect information in a way that the parties and counsel feel that they are legally required to ensure protection.

So that starts, as we talked about earlier, right at the initial discussion with the arbitrators, the candidates and in the questionnaire for the umpire candidate.

With respect to the next steps, how do you certify this or document arbitrators' recognition, I personally do not want to see this added to a hold harmless indemnification agreement.

The hold harmless was intended to place the arbitrator, as the arbitrator should be, in kind of a semi-judicial protective environment that judges receive. And to start adding more and more requirements and conditions and all the rest of it to a hold harmless indemnification is not the way I would want to see it go.

I have no problem with additional and more specific information being put into the Confidentiality Agreement. Personally, my experience has been, just like Bob mentioned. They are sep-

arate undertakings. The counsel have asked the panel members to confirm what they did and when they did it. I think that's sufficient, quite frankly.

MR. THIRKILL: I agree with what Dan and John said, particularly Dan's last point there. Because the whole issue comes down to whose responsibility is it?

I think there's a level of reasonable due care that panel members should take and certainly would take. They wouldn't be selected if they did not. But the onus on protecting the information shouldn't be on the judge of that information. It should be on the parties and/or counsel. And I think there are certain things that could be done quite swiftly.

For example, if there was a particularly sensitive area, one of the things that you might be able to do—it sounds expensive, but it really isn't, in the overall scheme of things, it's de minimis as a whole—is send a small computer to each panel member, which was totally set up to receive and deal with encrypted information, irrespective of what I and Dan or John or anybody else might have on their own systems that could be exclusive to that particular arbitration, and could be returned at a particular point in time.

In other words, it should be the users and providers of the information, as far as I'm concerned, not the panel members who take responsibility for the protection of the information. Although I do recognize and absolutely agree that we, as arbitrators, should exercise a reasonable duty of care.

MR. COLE: Bob, if I could just jump on David's point there and very much agree with it.

I know that there's some cynicism at times among the arbitrator community that ARIAS' solution to any problem is, at times at least, to add a further requirement to the arbitrators and rarely, if ever, to counsel or to the parties.

There's no question that the arbitrators have a big role and a big responsibility in this equation, lest that be misunderstood. But I was reviewing in advance of this call and your asking us to become involved in this, the very good materials that were provided at the ARIAS fall conference. And you don't get more than two pages in there before there is a list of requirements on the arbitrators that is proposed.

Arbitrators should have an office shredder; arbitrators should have a dedicated computer that is used only for arbitrator work; arbitrators should do this and do that. And certainly, again that's not inappropriate.

But I'm also interested, and I think a holistic response to this issue requires that there be standards considered by those that provide information.

MR. HERMES: Let's stay with this idea for a minute. As someone whose practice has been in the reinsurance arbitration arena for 35 years, I always view myself, as one of the other roles I play, as well as being an advocate for my clients, as trying to make sure that the arbitration proceeding itself runs as efficiently and fairly and smoothly as possible.

So with that in mind, David, let me go ahead and I will start with you on this one. What would you like to see counsel do to help further the protection of confidential and proprietary information that we have been talking about?

MR. THIRKILL: I think at the organizational meeting or prior to it, counsel should explain to the panel whether or not there is going to be information that will come in that falls under the headings that need to be protected.

If there is, be prepared to explain to the panel what the information is and what the parties want to have done to protect the information. And that duty, like the reverse duty in an arbitrator's ongoing disclosure, should also be an ongoing duty. Because often at the beginning, it may not be apparent that there will be such information. But as it comes down the line, and that if and when occurs, counsel should explain to the panel exactly what they are going to do to protect it.

MR. SCHMIDT: I think the most important thing that counsel can do is discuss a plan among themselves and determine if the panel actually has to receive hard or electronic documents that has PII or PHI information on them.

You know, as a matter of course, we'll get exhibits, documents that have tremendous amounts of information. And there might have been a single sentence in 10,000 words of information that was important.

Do we really need to get that information? If so, I think very serious efforts should be made to redact sufficient amounts of information so it falls out of the PII, PHI category.

If they can't do that, then I think there's going to have to be discussion with the panel as to how to treat that information. It may be that it shouldn't go electronically. That it may go in some other way that it can be received and returned with proper certification or received and destroyed with proper certification.

Again, we're talking about, I think, a very limited number of cases where a

reinsurance arbitration panel must receive PII and PHI information. Counsel and the parties could help quite a bit by limiting unneeded information from being sent to panels.

MR. COLE: It's really important that there be sensitivity at the only location that can identify this initially, and that is with the parties and counsel. At times we get much more information than we might legitimately need to decide particularized issues as a panel.

So a two-stage approach may be, as I think Dan was suggesting, first of all, can you identify a priori whether there is any PII, PHI or other legally protected information that you intend to provide to the panel at any stage of the proceeding? Hopefully, you can know that early.

And secondly, what is the character of that information? Certainly not what the details are, but what kind of confidential information as a general rule do you have in mind.

And then a third stage, of course, is if you can identify that for us, can you please explain why you think that it's essential to the resolution of one or more issues in the arbitration.

I think if counsel and the parties can get out ahead of it in that fashion, it provides the best opportunity, if you will, for all of us to consider whether that information exists. And then to take appropriate precautions as arbitrators with respect to that information so long as it is in fact necessary to the resolution of an issue.

MR. THIRKILL: May I jump in and give a very simple example?

We often get in large cases reams of proofs of losses, which come in as fact to show that a reinsurer was billed. We need to know the reinsurer was billed, but we don't need to see every single item that goes into the proof of loss. Much of which, some of those cases that we have identified earlier on, will get down to granular details, such as the individual, where they live and so on and so forth.

It's interesting, but it has absolutely no particular relevance. And so if counsel would get together beforehand and say well, we stipulate to this, that and the other. And here's a list – here's one billing with some items redacted just all the rest are identical and the total of them is X. That's all we really need to know.

MR. HERMES: We have primarily focused on PII and PHI, since it's the protection of that particular information that has moved this topic to the forefront.

But when you step back for a minute and you take into account the fact that the current form confidentiality agreement that is standard procedure at arbitrations currently provides, and let me read it for the record:

All briefs, depositions and hearing transcripts generated in the course of this arbitration, documents created for the arbitration or produced in the proceedings by opposing party or third parties, final award and any interim decisions, correspondence, oral discussions and information exchanged in connection with the proceedings (hereinafter collectively referred to as "Arbitration Information") will be kept confidential.

Is there any reason why arbitration information, as defined in the typical confidentiality agreement should be treated any differently than PHI and PII?

MR. SCHMIDT: I don't think there is. But it's only recently that we're being told that we should be encrypting our computer information. And I think that's the new requirement that companies and counsel are looking for arbitrators to sign on to.

MR. THIRKILL: I agree with that wholeheartedly. I don't think there's any reason why we should have different levels of security. We should take steps to make sure that all information we receive remains confidential.

But how we deal with it is the issue. Increasingly with some particular parties, there seems to be the movement to do away with confidentiality altogether. I often face at organizational meetings one party saying it's not in the contract. There's no reason to have confidentiality. Parties go to court all the time to vacate or confirm.

So, if the confidentiality of the proceedings is being challenged, PII and PHI must be addressed separately to ensure the required legal protections are in place.

MR. COLE: I agree all information should be kept confidential, but if PHI and PII must be disclosed, I think that should be separately noted to the Panel.

Opinions and views expressed by these participants are solely their own and are not attributable to their respective employers, clients, or associated companies.