CERTIFICATION & CREDENTIALING 411

A TRENDS 2019 special focus sponsored by GKG Law

EXAM SECURITY

BY RICHARD BAR, ESQ

Perhaps no challenge facing Credentialing Boards is as important as protecting their credentialing exams. The most valuable assets of a Credentialing Board are the credentials it confers on those who have earned the right to use them. Credentialing Boards, rightly so, go to great lengths to register, protect and enforce their credentials' intellectual property rights.

Many credentialing boards require credentialing applicants pass an exam in order to be eligible for a credential. If an exam is flawed or compromised, the credential itself will be devalued. The protection of the confidentiality and veracity of the credentialing exam is essential to protect the Credentialing Board's most valuable assets. The equation is simple: flawed or compromised exams devalue the credential which devalues the Credentialing Board, perhaps even making it near obsolete. Moreover, each time an exam is compromised, the Credentialing Board may have to spend hundreds of thousands of dollars to generate a new secure and valid exam.

What can you do? First, your organization should have strict policies and procedures regarding the security of the exam. The exam and credential applications should clearly set forth the rules for exam taking and the penalties for breaching the confidential nature of the exam, including damages and permanent revocation of all credentials. All of the applications should be signed by the applicant. Second, if the exam is being held in a testing center, then the organization should clearly define and understand the security protocols provided by the exam testing company and at the testing center, including the roles of proctors. The contracts between the Credentialing Board, the exam testing company and the testing center should clearly set forth the rights and obligations of all parties, as well as properly placing liability risk for a breach of exam security. Third, the Credentialing Board should have adequate insurance to protect against a security breach of the exam so that, if the content of the exam becomes public and/or invalidates the exam, the organization is protected and will have insurance proceeds to help offset the extraordinary costs of creating a new exam.

While it may be impossible to prevent all security and confidentiality breaches of the exam and exam taking process, there are certain basic steps each Credentialing Board can take to mitigate these risks so that the Credentialing Board can continue to best protect these vital assets and deliver credentials that have value to credential holders and have meaning to consumers.

"COMMON SENSE" ETHICS AND DISCIPLINARY REVIEW PROCESS

BY KATHARINE MEYER, ESQ

As a certification body, your organization is responsible for reviewing alleged violations of its Code of Conduct/Code of Ethics/Standards of Practice (the "Code"). In order to review these cases, your organization likely has: (i) a Professional Disciplinary Committee ("PDC") that consists of qualified experts in your industry; and (ii) clear disciplinary review policies and procedures that are fair and provide sufficient due process to certificants.

However, even with clear procedures and committee members who understand the ethical responsibilities of your profession, your PDC may be making decisions that could be successfully challenged. Set forth below are several "common sense" recommendations to your PDC in making legally defensible decisions:

1. **Frequent Training**. While PDC members may be experts in your industry or profession, that does not mean they fully understand legal concepts such as due process, conflicts of interest or confidentiality. We recommend that PDC members have ongoing training to ensure they understand their legal responsibilities and the PDC review process. Training should include a sample case review, an in-depth review of PDC procedures and a discussion of the legal issues involved with the disciplinary process. Training also gives you the opportunity to remind PDC members of their confidentiality and conflicts of interest obligations.

2. **Provide the Same Information to all Certificants**. Occasionally, we see organizations that draft substantially different decision letters to sanctioned certificants. Some of these letters have detailed descriptions of the reasoning behind the PDC's decision, while others may have no explanation at all. This may occur because the PDC does not know how much information should be provided. There may be an assumption that certain violations are self-explanatory. This may result in one certificant receiving an explanation of a decision, while another does not. This may mean that one certificant is being afforded more due process than another certificant. If sufficient reasoning behind the PDC's decision is not provided, it can become very difficult for that certificant to determine if the PDC conducted a fair and comprehensive review. Additionally, a certificant cannot effectively appeal a decision when he does not understand the basis for the decision.

While each decision letter should address the specific facts of each case, we recommend that all decision letters also include a short summary of the review process, a list of the Code sections the certificant violated, and a clear explanation of how the certificant violated each section of the Code. This will help ensure that all certificants are treated equally and fairly, while, at the same time, reduce time and risk to your organization in the event the decision is challenged.

3. **Speak with One Voice**. Ideally, there should only be one individual who is responsible for communicating with certificants and complainants. This person should be properly trained and have a clear understanding of what can and cannot be stated to parties involved in the complaint.

   For the sake of consistency, we recommend that the contact person be a qualified staff member instead of a committee member. Among other things, having a staff contact person ensures that the organization is aware of ongoing complaints and committee decisions. It also ensures the contact person will not be constantly changing because of committee term limits. This staff person can also be responsible for drafting letters from the committee, keeping proper records of every case and ensuring that the PDC adheres to any timelines set forth in its procedures.

   The PDC contact person should keep records of the conversations she has with certificants and complainants. She should note the date and time of the conversation and draft a brief summary of what was discussed. Occasionally a person will make a claim that the PDC contact person was unresponsive or made certain representations. It is easier to defend against these claims when there is a written record of what was discussed.

4. **Follow Past Precedent**. Make sure your committee is making consistent, defensible decisions. The PDC needs to have a rational explanation for discrepancies in its decisions between similar cases. One of the best ways to ensure the PDC is making consistent decisions is to keep a database of past decisions. When the PDC is deciding a case, it should look at its prior decisions to determine past precedent. It can then review the facts of each case and decide whether past precedent should be followed, or whether there are circumstances that make the current case different from prior from PDC decisions.

5. **Assume Correspondence Will Become Public Information**. Finally, always assume that any correspondence from the organization will be posted on social media. Even though your PDC may take all necessary steps to ensure the confidentiality of the complaint, there is always a chance a party to the complaint will post correspondence on social media. Therefore, make sure that all correspondence: (i) is clear and well-written; (ii) does not make any statements that could be considered defamatory or discriminatory; and (iii) shows that the PDC conducted a thorough and thoughtful review of the complaint.

These common-sense recommendations can help your PDC make informed, fair and consistent decisions and make it less likely that a person will dispute a PDC decision. Ultimately, always remember you can ask for help. Many times, a short conversation with legal counsel can help resolve issues before they spin out of control.

CRIMINAL BACKGROUND CHECKS FOR CERTIFYING BODIES SUBJECT TO THE GDPR

BY OLIVER KRISCHIK, ESQ

Since the European Union's ("EU's") General Data Protection Regulation ("GDPR") came into effect on May 25, 2018, organizations across the world have worked to evaluate the applicability of the GDPR to their data processing activities and, where appropriate, become compliant with the GDPR's new standards for personal data privacy and processing. The scope of the GDPR extends beyond the borders of the EU and applies to many organizations in the U.S. and elsewhere that process the personal data of individuals located in the EU.

In addition to the GDPR's general standards for processing personal data, however, the GDPR sets forth heightened restrictions on processing of certain categories of sensitive data. One of these sensitive categories of data is personal data about criminal offenses and convictions ("Criminal Records Data"). This presents an issue to certifying bodies in the U.S. subject to the GDPR that perform background checks on certification applicants.

Specifically, the GDPR states that *"[p]rocessing of personal data relating to criminal convictions and offences . . . shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects."* Article 10, GDPR.

This requirement has not changed from the EU's previous data privacy rules under Article 8(5) of *Directive 95/46/EC of the European Parliament*

and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. What has changed is the scope of the underlying regulation. Unlike Directive 95/46/EC, the GDPR applies to many non-EU companies who offer services and products to individuals in the EU. Accordingly, there should be very little change in how organizations located in the EU process this type of data, which is already regulated by Member State laws.

In those circumstances where the GDPR applies to a U.S. certifying body or the personal data it processes, any processing of Criminal Records Data must be under the control of a government authority or expressly authorized by EU or EU Member State laws. The requirement of government control or express legislative authorization exists even where the data subject has provided explicit consent to process his or her Criminal Records Data. To complicate matters, EU Member State laws on processing Criminal Records Data often differ from country to country. This means that certifying bodies outside the EU who are subject to the GDPR's expansive scope would need to engage in a multi-jurisdictional analysis of the applicable rules for processing Criminal Records Data. As EU Member States have been updating their respective national data privacy regulations to incorporate the new GDPR framework, this also means that affected certifying bodies would need to monitor the implementation of new data privacy legislation.

Depending on the relevant national laws involved, it may be that the GDPR outright prohibits affected U.S. certifying bodies from processing Criminal Records Data for individuals in certain EU Member States. Moreover, the applicable rules or restrictions would attach to the individual or certifying body – not to the source of the data. Put differently, where a certifying body would be prohibited from collecting French Criminal Records Data on an individual in France, that certifying body would likely also be prohibited from collecting US criminal records on that person. This is because both sets of Criminal Records Data would be considered personal data about that individual in France.

Please note that the GDPR does not prohibit solely U.S.-based certifying bodies (i.e., organizations with no EU establishments) from processing Criminal Records Data on persons located outside the EU. Accordingly, for most U.S. certifying bodies, these new rules would only apply in situations where an individual located in the EU is applying for a certification that requires a criminal background check. Violations of the GDPR can carry serious penalties, including fines of up to €20,000,000 or 4% of annual global revenue, whichever is greater. See Article 83, GDPR. Having said that, the GDPR's expansive jurisdiction over U.S. organizations is controversial and has yet to be tested. To date, most major data privacy cases have proceeded against U.S. organizations that have offices, subsidiaries, or affiliates located in the EU. For these reasons, it is still too early to tell whether the EU or its Member States will be successful in enforcing administrative fines against organizations located solely in the U.S.

GET MORE 411

1. Circular 64 - Copyright Registration of Secure Tests: www.copyright.gov/circs/circ64.pdf
2. The Secure Test Declaration Form: www.copyright.gov/forms/securetest-declaration.pdf
3. The Secure Test Questionnaire: www.copyright.gov/forms/securetest-questionnaire.pdf
4. Visit www.gkglaw.com to read detailed articles about: certification programs and antitrust laws, protecting your organization's intellectual property, tax issues related to tax exempt organizations, and other articles relevant to certification organizations