The Background Screening Credentialing Council

The Background Screening Credentialing Council volunteer members drafted the following response to a question about information security in Clause 4.5 of the BSAAP Standard, version 2.0, effective April 6, 2018. This letter is an informal discussion of the noted issue and does not constitute a legal opinion of the BSCC.

TITLE: Clause 4.5 – Information Security

Issue (revised slightly): We have a client that recently went through an audit. The auditor has told our client they need to call out '[insert platform provider]' as a secure integration obligation within contracts, ultimately forcing them to recertify all contracts and to some degree forcing new contracts or amendments should they ever move from [software platform] to another software.

This is the first time in all the times I've gone through audits that a required software call out was a point of nonconformance.

Response: Your answer appears to relate to the confidentiality requirement in Accreditation Standard 2.0, Clause 4.1 (implemented August 6, 2018) and the secure transmission requirement in Accreditation Standard 2.0, Clause 4.5 (implemented August 6, 2018), most specifically the two highlighted sections below, including the highlighted sections describing what Attributes the Auditor should look for during the Onsite Audit of the CRA to determine conformity with these two clauses.

> ***4.1 Public Record Researcher Agreement***
> ***Clause***
> *CRA must have and follow a procedure requiring a signed agreement, which may include amendments and/or addenda, from all non-employee public record researchers. The agreement must clearly define the scope of services to be provided, including jurisdictions covered, search methodology, depth of search, disclosure of findings, methodology and time frame for communication and completion of requests, methodology for confirming identity of subject of record(s), confidentiality requirements, reinvestigation requirements, and other obligations as furnishers of information under the federal FCRA.*
>
> ***Measure & Documentation Typically Subject to the Desk Audit***
> *CRA must provide written policy, procedure, or other written documentation describing how a signed agreement covering scope of services is obtained from and retained for all current public record researchers. CRA must also provide copy of current agreement. (Note: This agreement may also incorporate Certification requirements of Clause 4.3.)*

Potential Verification for On-site Audit

CRA must present written procedure for obtaining signed agreement, copy of agreement, and demonstrate where/how signed agreements are retained. CRA must make available the person responsible for obtaining and retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more public record researchers. If interviewed, CRA workers responsible for working with public record researchers must demonstrate understanding of requirement for signed agreement prior to utilizing services of public record researcher OR technology must prevent utilization of public record researcher by CRA workers until CRA Leader has enabled use. CRA must provide evidence of adherence to procedures.

Attributes of and Suggestions for Onsite Audit
(What auditor should look for in policy, procedure, activity)

The agreement [must] include, but is not limited to: 1) the requirement to conduct all searches in full compliance with applicable law and regulation, 2) jurisdictions covered, 3) search methodology, 4) depth of search, 5) disclosure of findings, 6) methodology and time frame for communication and completion of requests, 7) methodology for confirming identity of subject of record(s), 8) confidentiality requirements, 9) reinvestigation requirements, 10) other obligations as a furnisher of information under the federal FCRA, and 11) the requirement for public record researcher to obtain a similar agreement from subcontractors, if subcontractors are used. In particular, the agreement must emphasize confidentiality requirements including: 1) the legal requirement to treat all consumer information as confidential, 2) secure data transmission, and 3) secure and timely disposal of confidential information. (Note: This agreement may incorporate the Certification requirement of Clause 4.3) Auditor will seek evidence of adherence to policies and procedures.

4.5 Information Security
Clause

CRA must have and follow a procedure providing a secure means by which public record researchers will receive orders and return search results.

…

Attributes of and Suggestions for Onsite Audit
(What auditor should look for in policy, procedure, activity).

Security procedures, which must be agreed to in writing by researcher, for transmission of personally identifiable information to/from public record researchers must include, but are not limited to use of an electronic system designed for secure transmission of information between CRA and researcher; or if other transmission methods are used, security procedures must include, but are not limited to: 1) all transmissions must be directed to a named party, 2) all transmissions must be clearly marked as "CONFIDENTIAL" and include a request to notify sender if received by someone other than named party, 3) if faxed, a cover page must always be used and must not contain any personally identifiable

information, 4) if faxed, CRA must have verified receiving fax is in a non-public location, 5) if transmitted using CRA network, such network must be secured using a minimum of 128 SSL, 6) if transmitted via Internet, data must be encrypted or protected in a comparable manner. Auditor will seek evidence of adherence to policies and procedures.

While Accreditation Standard 2.0 does not specifically require the CRA name their third-party platform provider in their agreements with their public record researcher, it does require the agreements to contain provisions which specifically establish satisfaction of the confidentiality and data security requirements. We appreciate that the Auditor is challenged to establish conformity with these two provisions in a situation where the CRA is not the ONLY entity that is responsible for ensuring the Agreement specifies and emphasizes "confidentiality of all consumer information", "secure data transmission", and "secure and timely disposal of confidential information," as well as establishing conformity by the CRA with the requirement of "securing using a minimum of 128 SSL" or "encrypted or protected in a comparable manner".

Having said that, we believe that a CRA can establish conformity in different ways. Two possible methods of establishing conformity are outlined below:

1. The CRA's contract with the third-party platform provider should address topics like who is responsible for confidentiality of all private identifying information, masking, secure data transmission, data security standards, disposal of records, etc. In addition to the CRA-Platform contract, the CRA has a contract with a public record provider in which CRA describes the manner in which the CRA and the provider will transmit data between one another (via a secure third party platform specified by the CRA and subject to change from time to time) and requires with specificity that those transmissions will satisfy the terms of the CRA's Agreement with their platform provider.
2. Same as (1) above only CRA chooses to specify the name of the third party platform provider and specify and refer to that platform provider's obligations to deliver a means of confidential and secure transmission as well as to hold the public record researcher to the same standard.

In the case of example (1) above, the CRA would not need to specify the name of the third party platform provider. In the case of example (2), the CRA could choose to specify the name of the third party platform provider.

Please note, if your public record research agreements make no reference to these security and confidentiality requirements and the manner in which every party fulfills the obligations, then the Auditor would not be able to establish conformity. Opportunity for improvement could also be noted if a broad reference is made without specifying the obligations of each party to the arrangement.

Accordingly, naming the actual third party platform provider in those Agreements is a reasonable attribute to look for in satisfaction of this requirement. However, this statement alone would not suffice without additional specifications contained in the Agreement describing what the CRA is doing (via that third party platform provider) to satisfy these confidentiality and data security transmission requirements. Furthermore specifying the name of the platform provider is not necessarily required in order to satisfy these provisions.

The Accreditation Standard 2.0 does not require the software provider be named in the contract between the CRA and the public record researcher.

We believe we have responded fully to your inquiry. Please let us know if you have any further questions.

November 2018