National Student Clearinghouse: Data Sharing Agreement

Presenter: Robert Leonard, CAPM

BCSP | Board of Certified® Safety Professionals

Why we proceeded with a data sharing agreement with NSC

- Where are our blind spots?
  - Didn't have full picture of our certificants

- What can the National Student Clearinghouse provide us?
  - Aggregate data of key knowledge points that we are lacking

Molding to fit the needs of a certification body

- The original agreement didn't fit the needs of a certification body
  - Data privacy and security followed FERPA rules
    - Certification bodies do not operate under FERPA
    - Needed similar protections for certificant PII under relevant rules and standards such as
      - GDPR
      - California data protection laws
      - Accreditation standards

Molding to fit the needs of a certification body

- Worked with NSC to fit to credentialing body needs
  - Strengthened language that protects PII disclosure
    - Defined “Credential Recipients” and what data is provided to NSC
    - Clarified what data will be provided to & shared by NSC
    - Created rules that stated what data other organizations will see that was provided by BCSP.
    - Strengthened breach protocols
      - Instituted a 30-day limit for reporting a breach on both sides.
    - Conducted IT security audit on NSC premises Addressed enforcement of security of PII data
      - Clarified language regarding use of PII data
      - Transparency regarding data destruction between both parties
    - Gave certificants the option to opt-out
      - Have certificant PII not be sent to NSC
      - Remove certificant PII from the NSC database

Molding to fit the needs of a certification body

- Additional measures taken:
  - Included reciprocal rules in the agreement
    - We will receive aggregate information based on information we submit
    - For information we don't submit, we will not receive aggregate information in return
    - Reciprocity extends to other third-party institutions (i.e., we can submit data we don't want other third parties to view, and vice versa)
  - NSC developed tools to prevent junk data due to certification status changes

Other work to align with the Data Sharing Pilot

- Updated the BCSP Privacy Policy for disclosure of PII to third parties **for research purposes**
- Updated internal mechanisms for opt-out.
  - Policies and procedures
  - Certification management systems and communications
    - Certificants are automatically opted in; they must voluntarily opt-out.
    - Communicated privacy policy changes and opt-out choice to new and current certification holders

Other work to align with the Data Sharing Pilot

- Mapped BCSP's certificant data to NSC's database
  - Clarified data definitions between BCSP and NSC
    - Certification statuses (active, expired, revoked, retired, etc.)
    - Renewal vs annual fees
    - Exam score vs PASS/FAIL
  - Mapped and then coded racial/ethnicity/gender data to NSC's parameters.
  - Decided how changes in certification status will be reported to NSC.
    - Created a tiered list of what data is required and what is optional if we have the data to provide.

Contact for questions

I'm more than happy to troubleshoot, give insight, or forward specific/technical questions to relevant parties if I can't help out.

- Robert Leonard, CAPM – Robert.leonard@bcsp.org