**A Comprehensive List of Standards for Credential Evaluators**

**Submitted for review for the GDN Symposioum on Credential Evaluation Professional Issues**

**Written by: Rebecca Chamula**

**Senior Credentialling Officer**

**Canadian Alliance of Physiotherapy Regulators**

**March 31, 2017**

**ACKNOWLEDGEMENTS**

I would like to express my gratitude to my colleauges for their support and collaboration: Shereen Mir-Jabbar, Lindsay Weidelich, Jennifer Lippa and Hervé Jodouin. Your time and efforts are greatly appreciated. I am also indebted to Beka Tavartkiladze for his valuable insight and expertise.

**INTRODUCTION**

The Groningen Declaration seeks to address the needs of the ever growing globally mobile workforce and international student population through the development of a Digital Student Data Ecosystem. This ecosystem, which is comprised of digital student data depositories, would improve upon the pace, ease, and accuracy of transmitting student data. The Groningen Declaration Network has identified its main goal as the development of “best practices and globally-accepted standards for secure, citizen-centered consultation and portability of digital student data” (Groningen Declaration Network [GDN], 2015, p. 1). The following standards are recommended for implementation as international standards for the use and acceptance of digital student records. Specifically, these standards are meant to address the needs of credential evaluators in assessing internationally obtained academic credentials, while balancing the Declaration’s overriding principles of respecting autonomy and diversity of systems and modes of delivery (Groningen Declaration, 2012). They strive to allow for flexibility in the way institutions send digital student data, while ensuring that the student’s record contains all of the data needed by credential evaluators for the purpose of assessing an academic credential. While it is understood that the implementation of these standards will vary owing to different contexts and institutions, these standards should be considered by all organizations who create, store, and transfer electronic student data for the purpose of credential evaluation.

**STANDARDS**

***Security* – The student data record must be delivered to credential evaluators through a digitally secure technology which allows a credential evaluator to determine, with certainty, that the data has been securely transferred to the receiver’s database, free from alteration or modification.**

As a core value of the Groningen Declaration, it comes naturally that security should be one of the primary standards that must be met for credential evaluators (GDN, 2015, pg. 1). Ensuring that digital student data is securely transferred would be one, if not the first, point of evaluation in any assessment. While there are many reasons from the student’s perspective to have security standards in place, there are also reasons from an evaluator’s perspective. An evaluator needs to know that the student data has been guarded against alteration or modification (GDN, 2015, pg. 3). For the proposed Digital Student Data Ecosystem to work, credential evaluators need to be able to trust the original data source. It is also an essential part of the assessment process that evaluators be able to determine that the student’s record was securely transferred to them in accordance with existing standards and policies for the specific country, level and type of education. By receiving documentation in a secure manner, the relationship between the credential evaluators and the senders of the original data, will also be strengthened as they will become trusted points of contact if further clarification or information is required.

***Verification* – The credential evaluator must be able to authenticate the digital student record and the data contained therein with the issuing institution.**

In conjunction with security, authentication of the academic credential is vital. The credential evaluator must be able to verify that the digital student record they are assessing is legitimate. Modern technology has increased the ability for a common user to manipulate or fabricate data. According to the Higher Education Degree Datacheck (2016), “there is reported to be a growing number of instances of misrepresentation and forgery in the presentation of academic credentials” (p. 2). It is imperative that a verification process exist to protect the integrity of the credential evaluation process by reducing the risk of fraud, while also reducing barriers to student mobility for legitimate students. To ensure protection against fraudulent documents, credential evaluators must be able to verify with the issuing authority that the credential and related student data that they have received is authentic and accurate. It is recommended that signatories to the Declaration implement a verification process for credential evaluators that is delivered in a timely manner, is easily accessible, and is straightforward to interpret and use for all digital student records. The method of verification employed by institutions will vary dependent upon the resources available to those institutions.

***Data Quality* – Institutions housing and transferring digital student data must have a policy for quality assurance to ensure that student data is accurate, complete and up-to-date.**

It is essential that issuing institutions put into practice a system of ensuring that data transferred electronically to a recipient institution meets this standard. They must be able to identify inconsistencies and errors in their records. In addition, similar to diploma supplements, electronic student data records should “be free from any value judgements, equivalence statements or suggestions about recognition” (European Comission, 2007). When these systems are in place, the credential evaluator will be able to determine with confidence that the student data they are receiving is from a trustworthy and reliable source and that the data is free from error, contains sufficient information, and is up-to-date.

***Informed Consent* – The digital student record must include sufficient information for a credential evaluator to confirm that the student provided informed consent regarding the release of their data to a third party evaluator.**

Another core value of the Groningen Declaration, privacy, includes the principle of informed consent (GDN, 2015, p. 2). A student’s informed consent must be obtained before a credential evaluator can assess their information. The purpose of obtaining student consent is to ensure that the individual who requested the data to be reviewed for assessment has provided proper authorization for the evaluator to assess their credentials and release the results (GDN, 2015, p. 1). As Herman de Leeuw (2013) highlights, in his article for Transcending the Maze, “citizens should be at the helm of their data; only they may authorize third-party access to their data” (p. 17). Institutions that are required to release data to a third party will need to have privacy regulations in place that meet national privacy regulations. The Declaration’s Statement of Ethical Principles previously commits signatories to keeping the collection, use, transfer, disclosure and storage of student data in compliance with privacy and data protection laws and regulations. This standard strives to strengthen this existing commitment by identifying the need of informed consent from an evaluator’s perspective.

***Purpose Specification* – The digital student record must include information that allows the evaluator reading the credential to understand why the student is submitting their academic records to them for assessment.**

For credential evaluators to assess an academic credential, in many cases, it is necessary to know the context in which they are reading the credential. Evaluators need to know if a credential is being assessed for immigration, continued education, or employment purposes. For example, the academic data required and the outcome of a credential assessment may vary widely for an individual applying to transfer into a new program at a foreign institution versus an individual applying to work in a regulated profession. As identified in the Declaration’s Statement of Ethical Principles, “personal student data should be relevant to the purposes for which they are to be used” (p. 2). The Statement of Ethical Principles sets out more detailed guidelines for the purpose of transferring student data, further supporting the need for standards that acknowledge the importance of identifying a purpose of exchange of an individual’s academic records.

***Adequate Information* – The digital student record must contain sufficient academic and demographic information in order for a credential evaluator to complete an assessment for equivalency, recognition and placement.**

Without sufficient information, a credential evaluator may not be able to accurately complete a fair assessment of the academic credential they have received. The digital student record must include enough information with regards to academic work for an assessor to be able to complete an evaluation and make a recommendation of equivalency, recognition and placement (when applicable) for the receiving institution. Erroneous or omitted information can impact the results of an assessment. For example, if grading schemes are not included with a transcript of grades, grade conversions may be inaccurate or may not be able to be completed. Therefore, as a minimum requirement, it would be advisable that information for understanding the record itself be included with the student data. In other cases, contingent upon the required service and the purpose of the assessment, additional information such as details about the course exemptions or transfer credits would also be necessary. Basic identifying information is essential as well. According to AACRAO’s committee on the Standardization of Postsecondary Education Electronic Data Exchange (SPEEDE), “a complete College Transcript should include sufficient information about the student so the recipient of the transcript can, with a high degree of certainty, insure that the transcript is matched with the correct student in the receiver’s data base.” (AACRAO SPEEDE Committee, 2007, p. 1). This standard would be applicable to all digital student records and ensure that an accurate and thorough assessment of the student’s credentials can be completed.

***Institution-specific formatted documents*– The issuing institution must produce student credentials and academic records in a consistent manner within their own institution to allow for comparability of credentials from previously assessed students.**

Being able to use previously received and verified documents is a leading tool in assessing foreign credentials. Multiple versions of student credentials can cause difficulties and delays in producing an assessment. Having institutions commit to an institution-specific standardized format will reduce variations in content, which further supports data quality. Institutions committing to standardized formats for their credentials is also valuable in assisting credential evaluators with learning, recognizing and understanding the different formats from various institutions, which will aid in verifying and authenticating the credential. This standard is designed to support the Declaration’s commitment to convergence as opposed to standardization (GDN, 2015, p. 1), which is why it is not recommended to develop one standardized record format for all institutions. In recommending institution-specific standardized formatting, the standard understands and respects an institution’s autonomy over the management of their educational documents and data.

***Original Language Record* - The digital student record must be submitted to the receiving institution in the original language.**

A best practice in evaluating international credentials is to include the original language document in the assessment and to not rely solely on the translation of the information (World Education Services, 2012). Translations can be inaccurate or, in some cases, omit details. In order to best understand and evaluate a credential, an evaluator will use the original language document to verify and authenticate the student’s academic data. In her paper [*The Forensics of Academic Credential Fraud Analysis and Detection*](https://www.nafsa.org/uploadedFiles/NAFSA_Home/Resource_Library_Assets/ACE/forensics_of_academic.pdf?n=6546), Eva-Angela Adán states “never use English translations in lieu of original language documents to evaluate and make admissions determinations. Translations should be used as a ‘road map’ to identify and confirm critical information. Remember, for every translation there is an original” (2002). For a credential evaluator, receiving the student’s digital record in the original language, in addition to any translations, is a necessity to prevent fraud and to complete an accurate and fair credential assessment.

**CONCLUSION**

One of the overriding themes of the Groningen Declaration is to promote convergence over standardization. However, for a Digital Student Data Ecosystem to succeed, institutions will need guiding principles to ensure that the ecosystem meets the requirements of the Declaration’s signatories and stakeholders. Credential evaluators will be a primary user of digital student records. The development of digital student data portability is an opportunity for evaluators to create new tools and improve upon existing credentialling tools to increase the pace and accuracy of their assessments. Having a digitally secure method of transferring student data will also assist evaluators in limiting the use of fraudulent documents. However, such changes in assessment practices can only be properly implemented and successful if there is some measure of guiding principles and standards to ensure that trust remains prevalent between institutions. The standards outlined in this paper address the needs of credential evaluators in completing assessments, while respecting the various contexts and landscapes that are present in a global initiative such as the Groningen Declaration.

**REFERENCES**

AACRAO SPEEDE Committee. (2007). *Recommended Implementation Practices for PESC XML College Transcript.* Retrieved from <http://aacrao.org/about/committees>

Adán, E. (2002). *The Forensics of Academic Credential Fraud Analysis and Detection*. Retrieved from <https://www.nafsa.org/uploadedFiles/NAFSA_Home/Resource_Library_Assets/ACE/forensics_of_academic.pdf?n=6546>

de Leeuw, H. (2013). A maelstrom of abbreviations: On the emerging global digital student data portability landscape. *Transcending the Maze…Moving Forward with Global Credentials*, 1, 15-21.

European Commission, Council of Europe, UNESCO/CEPES. (2007) *Diploma supplement model.* Adopted by the Lisbon Recognition Convention Committee. Retrieved from <http://ec.europa.eu/dgs/education_culture/repository/education/policy/higher-education/doc/ds_en.pdf>

Groningen Declaration Network’s Executive Committee. (2012) Proceedings from Groningen, 16 April 2012: *Groningen Declaration on Digital Student Data Depositories Worldwide*. Groningen, Netherlands.

Groningen Declaration Network’s Executive Committee. (2015). *Statement of Ethical Principles.* Retrieved from <http://www.groningendeclaration.org/statutes-and-more>

Higher Education Degree Datacheck. (2016). *Advice and guidance on degree fraud a toolkit for employers* [Handbook]. Prospects. Retrieved from <http://cdn.prospects.ac.uk/pdf/hedd%20degree%20fraud.pdf>

World Education Services. (2012). *Best Practices: Strategies and Processes to Obtain Authentic International Educational Credentials* [Handbook]. Retrieved from <https://www.wes.org/ca/licensing/bestpacticesstrategiesprocesses.pdf>