InterPARES Project

International Research on Permanent Authentic Records in Electronic Systems

Due Diligence & Professionals

Keeping Records in a World Gone Digital

Due Care and Due Diligence

- Professionals have a duty of care towards their records, ethically and legally, because they are accountable for their actions to their profession (ethically), to their organization (administratively and legally), to society (legally and morally) and to the next generation (historically and morally)
- To fulfill due care, they need to exercise due diligence, that is, they need to comply with existing legal requirements, standards, best practices, and leading research recommendations. In order comply, they need to be informed.
- To inform you today I will use three primary sources: the findings of the InterPARES research project, the Canadian standard for records as documentary evidence, ISO standards, and Canadian and US case law

The Digital Records Challenge

- Digital Records Issues:
  - accessibility, readability, intelligibility, compatibility of formats and software versions, interoperability of applications
  - no originals, proliferation of copies (but redundancy is good), uncertainty about the final or official version
  - risks for intellectual property rights, accuracy and authenticity
  - vulnerability to viruses and technology failure
  - technological obsolescence
  - inconsistency of hybrid record systems
- Definitions are important:
  - **record**, publication, document, information, data
  - reliability, accuracy, **authenticity**, authentication

Records &Trustworthiness

- Data: the smallest meaningful piece of information
- Information: a set of data meant for communication
- Document: recorded information
- Record: document made or received and set aside in the course of business and kept for action or reference

You are accountable through your **records**, not data

- Reliability: trustworthiness of content (competence of author + control on records creation)
- Accuracy: precision, correctness of data (as above + control on transmission)
- Authenticity: trustworthiness of the records as a record (identity + integrity—control on maintenance and preservation
- Authentication: declaration of authenticity at a given moment in time

You should be able to ensure reliability, accuracy and authenticity without need for authentication

InterPARES Principles

- Technology cannot determine the solution to the reliable and accurate creation of digital records or to their authentic preservation over the long term: **the professional's needs** define the problem and **archival principles** must establish the correctness and adequacy of each technical solution
- Solutions to the digital records challenges are inherently **dynamic** and **specific** to the cultural, disciplinary, administrative and legal situations
- Preservation is a **continuous process that begins with records creation**
- We must be able to **presume records trustworthiness (reliability, accuracy and authenticity)**, till proof to the contrary is established
- We must be able **to retrieve the records that we are required to present for e-discovery and only those records**
- We must remember the four key phrases of the rules of admissibility for electronic records: **system integrity**, **record integrity**, **usual and ordinary course of business**, **circumstances of the making of the records**

1. Selecting Software & Hardware

- Choose software that presents your old materials as they originally appeared (**compatibility**) and allow you to share materials easily (**interoperability**)
- Use software that adheres to **standards** (*de jure* or *de facto*): the Daubert test requires theoretical or empirical testing, peer review, known error rate, general acceptance within the scientific community to meet the standard of evidential reliability of software
- Maintain the **specifications** of software (owner's manual)
- **Document changes** when software is customized (include comments in the software code)
- **Document** the **construction** of your system
- Choose **non-proprietary**, platform independent, **uncompressed** formats with freely available specifications (open format) and software whose code is made freely available and can be modified (**open source**)
- Judicial scrutiny of scientific or technical evidence is rooted in proving that results produced are **repeatable**, **objective**, and **verifiable**, whereas industry measures the reliability of software in terms of **reliability**, **authenticity** and **availability**: open source satisfies both

2. Ensuring Stability of Digital Materials

- **Stability** is the essential characteristic of every record and means:
  - **fixed content** (content cannot be overwritten, altered, deleted or expanded—if it can, make sure you have a log of changes and an audit trail and you consider your system the record rather than its content) and
  - **fixed documentary form** (the rules governing the presentation on the screen are unchangeable)
  - manifested and stored records must be clearly **linked** (the number of variations are limited)
- The **documentary form** of each record associated with each activity should be defined at the outset
- **Do not compress** your digital material
- Documents made in anticipation of litigation are inadmissible under the business records exception, so you cannot stabilize data or information when you get in trouble. Printing to paper? **Best evidence rule** (native form requirement + hypermedia and attachments issues). So, let's stay with digital records.

3. Identifying Digital Materials

- Record essential information about the record so that it may be uniquely identified (**identity metadata**=properties), retrieved, and contextualised:
  - names of **author**, writer, originator, addressee
  - name of **action**, matter, subject, or simply the title
  - **dates** of compilation, transmission, receipt, filing
  - documentary **form**
  - digital **presentation** (format, wrapper, encoding, etc)
  - **attachments**, if applicable
  - intellectual **rights**, if applicable
  - presence or removal of digital signature, or other form of **authentication**
  - name of **person responsible** for the record, if applicable
  - name of or code for the file or **group** of records in which the record belongs
- Distinguish different **versions** of the record and identify the official version among its identity metadata
- This is also important to meet the **business records exception** to hearsay

4. Supporting the Presumption of Integrity

Record information that helps to infer that the record is the same as when created (**integrity metadata** or properties):

- name(s) of **handling persons** over time
- name of person primarily **responsible for keeping** the record
- indication of additions (**annotations**) made to the record
- indication of **technical changes** (e.g. format, encoding, upgrading, changes to digital components, migration)
- indication of presence or removal of **digital signature**
- **planned removal from the system**, transfer to a custodian, deletion—business records exception to hearsay applies here
- existence and location of **duplicates** outside the system

The latter two bullets establish a proper **chain of custody** (more on security later)

5. Organizing Materials into Logical Groupings

- Separate **records** from other types of materials, the **business records** from the personal ones, ephemeral from **official** (not on the basis of form: an e-mail may be considered a contract)
- Create a classification scheme or **filing plan** or a structured directory to provide a logical place for each record
- Ensure that such scheme, plan or directory **corresponds to the way your non-digital records are organized**
- Provide each new digital record with an **identifier** showing its proper place in the scheme (e.g. a code or the name of the file and of the higher groups in which the file belongs) and include this among the record's identity metadata
- Identify **how long records need to be kept**—big buckets theory...not a good idea
- Make **decisions at the group or file level**, not the individual record (maintaining consistency between the records on different media belonging to the same file or group)

6. Authentication

Technology dependent authentication

- Nature of authentication techniques
  - digital signature
- Obsolescence and authentication
  - preservation issues
- Managing documents with digital signatures
  - integrity metadata

Technology independent authentication

7. Protecting Your Materials from Unauthorized Action

- You must be able to demonstrate that it is **impossible to tamper** with your materials without being identified
- **Do not download your records to computers that are not under your direct control** (privacy issues compound problems of trustworthiness)
- **Restrict physical access** to your computer(s)
- **Create access permissions** for all legitimate users of your system
- **Maintain an audit trail of access** to your system and the materials in it
- If you cannot prove the **authenticity** of your material, it is irrelevant that it is authentic
- Authenticity of a record can be challenged by **challenging the identity of its author**
- Evidence that **your record system is trustworthy** lays the foundation for the authenticity of your records
- If you are an organization or community of practice, have a **procedure manual**

Records Procedures Manual

In the event of legal proceedings (or a request by a taxing or other government authority), the procedures manual can be the most important support to satisfy the legal requirements (admissibility and weight) for electronic records in the evidence acts. The procedures manual can be used by a witness as evidence to prove that

- an authorized Records Management System (RMS) program is followed;
- the RMS program provides proof of the system's integrity, i.e., the system reliably records, stores and processes electronic records; and, therefore,
- the electronic records are authentic (have identity and integrity), so trustworthy and reliable documentary evidence can be produced from them at any time and for any purpose.

If you create a manual you should also include in it the activities related to what is detailed in items 1-10 of this presentation

8. Protect Records from Accidental Loss & Corruption

Ensure that **your system is backed up** at least once a day; use the best backup technique for your situation; ensure your backup system include an audit trail

The **purpose of your backup is to recover the system in case of failure**, not to keep records. Destroy your backups on a regular basis (e.g., every third day)

Duplicates of your material should be kept on additional hard drives. If they are on tapes or discs, remember to refresh and upgrade them periodically

The **integrity of the electronic record system** guarantees the trustworthiness of the record (CGSB)

The **business records exception to the hearsay rule does not apply to computer generated records** (as opposed to computer stored records and ESI—Electronically Stored Information) **that are not subject to human interference**: their trustworthiness is assessed on the reliability of the program

The reliability of a computer program can be established by showing that **users of the program actually do rely on it** on a regular basis, such as in the ordinary course of business

9. Protecting Materials Against Hardware & Software Obsolescence

- **Eliminate dependence** on specific hardware by transferring its functionalities to the software (ask IT to help you)
- **Plan for regular technology upgrades** (keeping in mind the need for backward compatibility)
- **Consider external storage** for infrequently used records (including computer output microfilm for textual records that do not require random search)
- If you remove materials from your live system, associate with it the **system documentation and all the necessary information about the material** to be able to maintain accessibility and to understand the material itself

10. Planning for Long-Term Preservation

- Identify the materials that need **to be preserved for the long term**—"total archiving" is a bad idea
- Identify a **trusted custodian for the records** (in-house or external)
- Establish a preservation strategy early and in consultation with the designated trusted custodian
- Follow this set of recommendations

Conclusion

Although you might not be affected by pieces of legislation like the Sarbanes-Oxley Act, which provides for criminal penalties of up to 20 years in prison and/or fines for intentionally altering, destroying, or concealing records or documents in order to impede, obstruct or influence an investigation or official proceeding, or SEC rule 17a (7 years retention), **you should be aware of the risks of neglecting to manage your digital records properly**, and:

- Adopt measures that **work best in your situation**
- **Consult** with professional archivists
- Review other **InterPARES documents**, such as the Framework for Policies and the Preserver Guidelines
- Review the **Canadian Standard "Electronic Records as Documentary Evidence"** (CAN/CGSB-72.34-2005) *(Canadian General Standards Board)*
- For complex recordkeeping systems, review the **DoD 5015.2** (2007) standard and the **MoReq2** standard (2008)

Findings and Products

All findings and products are available on the InterPARES Web site:

www.interpares.org

at

www.interpares.org/ip2/ip2_products.cfm