POLICY	# Record Retention
POLICY: This policy establishes mandatory guidelines for ProVest to manage, maintain and dispose of data and records in an orderly, reasonable and lawful manner. * "ProVest" includes ProVest LLC, ProVest California LLC, ProVest Services LLC, ProVest Litigation Services LLC, ProVest Holdings LLC.	The following role(s) is/are accountable for the accuracy of the information contained in this document: Policy Owner(s): Risk & Compliance Management** ** *References to Management shall mean person(s) with ultimate responsibility for the applicable Department.*

TABLE of CONTENTS

1. Policy Statement 2
2. Scope 2
3. Policy 2
3.1 Record Definition 2
3.2 Basis for Retention 3
3.3 Storage Locations 3
3.4 Secure Medical Records Storage 3
3.5 Retention of Records 3
3.7 Disposal of Records 5
3.8 Litigation Holds and Retention Notification 6
3.9 Back-up Procedures 6
3.10 Communication 6
4. Record Retention 7
5. Enforcement 7
6. Revisions 7
7. Contacts 7
8. Appendices 7

1. Policy Statement

ProVest is committed to effective records management, including meeting legal requirements for record retention and protection of confidentiality, optimizing the use of space, minimizing the cost of record retention and properly destroying outdated records.

Records should only be retained for their period of immediate use, unless longer retention is specifically authorized or mandated. Official retention periods are as reasonable as possible in order to control ProVest's record inventory. Because records may sometimes relate to threatened or contemplated litigation or government investigations, audits or inquiries, this policy also provides a mechanism for immediately stopping any scheduled discarding of all such records.

2. Scope

This policy applies to all ProVest Team Members, data, and records.

3. Policy

3.1 Record Definition

This policy defines records as all forms of communication, data or information relating to ProVest or its business. Records include both hard copies and anything stored in electronic format. The most typical types of records are:

- Paper documents, files and notes;
- E-mails and instant messages;
- Documents, files, data or other information stored electronically on computers (including the metadata for electronically stored records), hard drives, disks, CDs, DVDs, any other external drives or storage devices, servers, back-up tapes, tablets) or any other similar personal data storage and communication device;
- Microfilm and Microfiche;
- Videotapes, cassette tapes, and all other recorded media;
- Vital records.

3.2 Basis for Retention

Many corporate records do not require long-term retention; they may be vital to current goals and useful for analysis of current operations but are of little or no value to ProVest after a determined period of time. Longer retention periods are based upon legal, audit, or management requirements.

Legal Requirements may include:

- A specific federal or state law requiring ProVest to keep the record;
- A provision of contract establishes a particular retention period;
- Important property rights which ProVest has a legal obligation to protect; or
- ProVest is aware of a specific, impending or threatened claim or legal action.

Audit Requirements may include:

- State and federal tax audits.

Management Requirements may include:

- Proprietary records of technical or economical use to ProVest.

3.3 Storage Locations

In the event any of ProVest's departments house physical documents containing restricted information of any kind, such departments must utilize a secure storage location for their records. Once removed from the active file location, written records must be boxed and stored in a central and secure location at each facility or off-site as approved by the Risk & Compliance Department and/or a member of ProVest's Management Team.

At no time shall ProVest records, files, or duplicate copies that are deemed to be internal, confidential or restricted be stored at home or on a personally-owned computer/device.

3.4 Secure Medical Records Storage

Team Members' personal medical information will be maintained by ProVest's Human Resources Department, and is kept in a secure location.

3.5 Retention of Records

3.5.1 Records Retention Schedule

The retention period for records depends upon the contents of each particular record and there is not a single retention period that is applicable to all records. Some records may be discarded immediately or after a brief period, others must be retained for many years, and still others will warrant permanent retention.

The determination of the appropriate retention period is the result of legal and business requirements pertaining to each record and ProVest's business needs. ProVest's Record

Retention Schedule accompanies this policy and provides a time schedule for the retention and disposition of records of ProVest. If you do not have a copy of the Record Retention Schedule you may find it on the Company's intranet. If you have any questions about the Record Retention Schedule, please contact the Risk & Compliance Department.

3.5.2 General Guidelines for Retention

All records shall be managed and retained in a manner that protects the integrity of the information in compliance with ProVest's ***Document Integrity Policy*** while ensuring appropriate access to same. Records that have reached the end of their retention period shall be deleted or destroyed in compliance with this policy, subject to any Hold Orders (defined below), laws or regulations. Guidelines for the review, retention and discard of records are outlined in the following sections.

3.5.3 Retention of Records, Generally

Each Department shall be responsible for periodically scheduling a records review to determine what of their retained records can be appropriately disposed of in accordance with this policy. The following principles shall be adhered to:

1. Records relating to completed matters, inactive matters, or records that are not used or referenced with sufficient frequency to warrant having them immediately accessible, must be centrally stored or sent off-site. Records that meet these criteria should be sorted into files or boxes according to their record type as set forth in the Record Retention Schedule. When documents are placed in storage or otherwise removed from active use, such files and documents shall be marked with the destruction date (or Indefinite IND. notation) and indexed so as to allow ease of location at the appropriate date of destruction. If files within the same box have different destruction dates, all dates shall be identified on the outside of the box and individual files shall be marked with their respective destruction dates. To the extent possible and practical, all related records with identical retention periods should be stored together.
2. All records that are centrally stored in centralized filing cabinets must be reviewed by the department designee and stored or destroyed in accordance with this policy.
3. Records that have reached the end of their retention period, as set forth in the Record Retention Schedule, must be discarded by shredding all hard copies or, in coordination with ProVest's Information Technology Department, by appropriately deleting all electronically stored records. These actions need n o t occur exactly on the end-date identified in the Record Retention Schedule but may occur as part of the next scheduled records review. Destruction of records requires management approval.
4. When disposing of confidential or restricted information, all such information shall be shredded and deleted from all electronic media, including hard drives or other electronic storage, all in accordance with ProVest's ***Data Destruction and Device Reuse Policy and Procedures***.

5. Unless they are necessary for independent business purposes or client request, no copies or drafts of records should be retained longer than the period established in the Record Retention Schedule for unofficial retention.
6. NO RECORDS MAY BE DISCARDED UNDER THE CIRCUMSTANCES OUTLINED IN THE LITIGATION HOLDS AND RETENTION NOTIFICATION SECTION.

3.5.4 Retention of Electronic Records and Electronic Mail

Electronic records are informational files or data files that are created and stored in digitized form through the use of computers and applications software. In managing electronic records, metadata must be captured along with electronic records to enable them to be understood and to support their management and use. ProVest's Information Technology Department must ensure that metadata is captured and preserved in the same manner and for the same duration as the electronic records themselves. Electronic records, wherever located, shall be reviewed in the same manner as hard copies, as described above. Electronic documents or data that have exceeded their retention period in the Record Retention Schedule must be deleted unless otherwise set forth in this Policy.

The person who transmits an email message is responsible for retention of that message in accordance with the retention guidelines described in this policy. All electronic mail communications and attachments that do not need to be retained pursuant to this policy shall be deleted. Each Team Member is responsible for reviewing their email or other electronic folders to determine if retention is warranted.

3.5.5 Retention of Records Maintained in ProVest Databases

It is ProVest's policy to define its databases as the *Official* Record of the organization. The Retention Period applied for records maintained within ProVest's databases has been established as retain until *Superseded* (SUP) to reflect that only the current version needs to be maintained.

3.7 Disposal of Records

It is imperative that the proper disposal, purging and overall destruction of these records adhere to the Retention Schedule and comply with the guidelines set forth within the ***Data Destruction and Device Re-use Policy*** and that Litigation Hold Orders are complied with. The following guidelines are provided to facilitate compliance with this policy:

- Destruction of records shall take place only in compliance with this standard policy in order to avoid the inference that any document was destroyed in anticipation of any specific problem.
- All disposed materials must be securely destroyed (i.e. shredded, overwritten, etc.) in compliance with the ***Data Destruction and Device Reuse Policy and Procedures***. All

back-up and archive copies of a record must be destroyed when the original is destroyed.

- On an ongoing basis, duplicate and unnecessary materials should be eliminated. Whenever possible, the official record is the one to be retained.
- Departmental records should not be destroyed without clearance from the department or area Vice President or its designee.

3.8 Litigation Holds and Retention Notification

From time-to-time, ProVest may need to ensure that certain records are not destroyed. The Risk & Compliance Department will provide written notice or a Litigation Hold Order to all necessary Team Members when records must be preserved pursuant to this policy.

If you receive such notice or a Litigation Hold Order and believe that fellow Team Members who have not received the notice/Litigation Hold Order may have relevant records, please immediately inform the Risk & Compliance Department. As soon as a Team Member receives such notice or simply becomes aware that records may relate to a threatened, anticipated or actual government inquiry, investigation or matter, or any internal investigation conducted or initiated by ProVest, he or she must not discard, conceal, falsify or alter any such record.

It is important to note that ProVest does not have to be the subject or target of an inquiry or investigation for the foregoing policy to apply. Whenever a notice is given or a Litigation Hold Order is in place, Team Members must immediately stop discarding relevant records and must search all hard copies (i.e. paper) and electronic records in their possession or custody to determine if they have any relevant records that must be preserved. All such relevant records then must be sent or forwarded to a separate, secure, location designated by the Risk & Compliance Department.

The length of time for a records presentation notice or Litigation Hold Order will vary greatly depending upon the particular circumstances. The Risk & Compliance Department will notify Team Members in writing when a Litigation Hold Order or other request to preserve is lifted.

3.9 Back-up Procedures

ProVest's Information Technology Department will establish procedures for the safekeeping and periodic back-up of electronic files. All personnel are required to comply with Information Technology Department procedures and to take reasonable precautions to ensure that vital data is not lost due to equipment failure or natural disaster as defined in any ***Business Continuity Plan*** that may be in place. Data that is stored electronically shall be stored on media that will withstand the retention requirements contained herein.

3.10 Communication

The Risk & Compliance Department will ensure that Team Members are made aware of the current Record Retention Policy and the Record Retention Schedule which is available on ProVest's intranet site.

4. Record Retention

ProVest's Risk & Compliance Department will maintain records and other relevant documentation related to this policy.

5. Enforcement

Failure to comply with this policy may result in the following:

- Personal criminal and/or civil liability
- Corrective action up to and including termination of employment or contract
- Suspension or termination of access
- Any other sanctions deemed necessary
- Any combination of the foregoing

6. Revisions

This policy and its related procedures will be reviewed and revised as needed, and no less than bi-annually by Risk & Compliance Management.

7. Contacts

Please direct any inquiry concerning this policy to Risk & Compliance Management.

8. Appendices

Use this section to include any attachments or supplemental information.

8.1 Appendix A — Record Retention Schedule

ProVest's Record Retention Schedule is available under the Compliance Tab on PV4U