Government Records Office,
Archives of Manitoba

Electronic Recordkeeping

FAQs

The following are some of the questions we are asked on a regular basis about electronic records management. We will add to this compilation as questions arise. These are general answers - please contact us (GRO@gov.mb.ca) for assistance with your specific questions and issues.

Updated June 2018

- **Is email a government record and what do we do with it? What about text messages?** Updated
- **How long should email be kept? Is there a retention policy for email?**
- **In electronic systems, what is a record anyway?**
- **If we scan our records can we destroy the original paper records?** Updated
- **Can we go fully electronic?**
- **Why doesn't government have a policy on electronic records retention and disposal?** New
- **You say that our systems don't have recordkeeping capability but what does this mean?**
- **We have electronic documents/files, but do not have paper copies. Can we just copy to CD/DVDs or to an external drive and keep them in the office or transfer them like we would paper records to get them off our shared drives?**
- **What would authorized destruction of electronic records look like in an automated environment?**
- **In our current environment, how would we destroy electronic records in a way that is clearly authorized and documented?**

Is email a government record and what do we do with it? What about text messages? Updated

Yes, messages sent or received by government employees, which relate to government business, are government records and must be managed accordingly. Like other records, they must be captured in an organized recordkeeping system so that they are linked to related records, available to the program area as long as needed, and retained and disposed of according to the provisions of a records schedule. Sometimes the methods we use to communicate are not the best methods to capture records as evidence of our activities or actions. See our Text & Instant Messages guidance for more information.

How long should email be kept? Is there a retention policy for email?

Retention rules are not applied to records based on their format (email, electronic files, paper, video, photographs). Instead, they are applied to groups (*series*) of records supporting particular functions or activities. **It is what they are about – not what form they are in.**

The records schedules developed by and for each business area are the plans (sometimes referred to as policies) for how long records need to be kept. They reflect functional groups of records and the retention periods that are needed to meet operational, legal and fiscal requirements. Records series often contain a mix of document formats. Refer to the appropriate records schedule for approved retention periods.

In electronic systems, what is a record anyway?

This question sometimes stems from the idea that only certain types of documents are records, or that it's only a record if it needs to be kept for a certain length of time, or that it isn't a record because it is electronic. "Records management is just about paper right?" In fact, if you are doing government work the simple answer is:

> It is all a record, and it must be managed as a government record whether it is needed for a very short time (such as a draft that has no value once it is replaced by a new version) or for many years.

Record (as defined in *The Archives and Recordkeeping Act*): "a record of information in any form, including electronic form, but does not include a mechanism or system for generating, sending, receiving, storing or otherwise processing information."

Records provide evidence of, and information about, government's functions and activities. Records are an integral part of government business. They are the product of every process in every government office – from the most routine administrative processes to unique program activities and services that government is responsible for.

Records can be created deliberately by individuals -- e.g. when they receive and file a report or an email message, or when they make notes of a meeting or investigation. Some records are generated by a business process in which the record is part of the transaction – think of the signing of a contract or the offer to purchase property. Or they can be captured automatically by an electronic system (e.g. a business application) that has been designed to do this.

If we scan our records can we destroy the original paper records? Updated

Yes, if the approved records schedule allows for destruction. If the series is unscheduled, the imaged records and the paper records must both be scheduled to provide for their retention and disposal. If you have digitized a series of records that is already under an approved records schedule, the schedule needs to be revised to update the information about your recordkeeping practices and to provide for disposal of the image files. Depending on the nature of the series and the disposal action, some consideration may have to be given to determining the official recordkeeping copy.

For more information on scanning, see our Digitizing Records guidance.

Can we go fully electronic?

Business is increasingly done electronically, but our electronic systems do not provide the ability to manage records reliably. What program areas need to know is that in the current environment there are risks involved in keeping records solely in electronic form.

By keeping records on shared drives instead of in corporate recordkeeping systems, you might not be able to meet the statutory requirements of *The Archives and Recordkeeping Act* or even basic recordkeeping needs of the organization. Specifically **you might not be able to**:

- make and keep full and accurate records of your activities. Most information on shared drives can be easily edited and there are only rudimentary audit trails to indicate who has made modifications. In addition, given the nature of desktop applications, related records about a function or activity are often not grouped together or otherwise linked.
- ensure the safe custody and proper care of the government records you receive and create. While some security measures can be added, most information on shared drives can be easily deleted.
- apply retention periods, disposal actions and other rules for accessing and managing records in a systematic, controlled way. Current desktop systems do not provide this kind of automated capability.
- properly document records management actions. Unlike the records management processes in place for paper records, there is no method to adequately document authorized destruction of records stored on shared drives. This is required in order to prove that the records were due for disposition and were disposed of in an authorized way under the correct authority (records schedule).

Our office has identified recommended standards for electronic recordkeeping systems, and we anticipate that these will be incorporated into government systems in future. One of the many benefits of this will be to *enable* departments to achieve the modern business goal of going “fully electronic.” In the meantime, there are no simple solutions. We hope that departments will identify electronic recordkeeping capability as a need when undertaking business process re-engineering and system development.

Please contact us for assistance with assessing how to manage records and information appropriately.

Why doesn't government have a policy on electronic records retention and disposal? New

The *records schedules* developed by and for each business area in departments and agencies *are* government's policy on retention and disposal. These plans for how long records need to be kept and disposed of are intended to apply to records in all media (i.e. paper and electronic). So, in other words, the policy is there for electronic records retention and disposal (embodied in approved and records schedules); it's the 'how to' that is currently missing on an enterprise-wide basis (i.e. electronic recordkeeping capability built into our government systems).

You say that our systems don't have recordkeeping capability but what does this mean?

Records management capability refers to the capability, or functionality, that is needed in an electronic system to manage records. There are standard specifications that describe the functions that systems must be able to perform in order to capture and manage reliable records. These are based on the principles set out in the ISO Records Management standards (see - Recordkeeping Standards: Fact Sheet). Organizations whose business practices and supporting systems comply with these standards will be able to have confidence in their electronic records and demonstrate the reliability of their recordkeeping systems. They will also have the significant benefits that come from integrating recordkeeping with new business processes, and automating records management processes that were once paper-based.

Records management capability includes the full range of functions needed to capture, retain, use, protect and dispose of records. It also includes the ability to support document management and workflow, access rights management, and protection of personal and sensitive information.

An electronic records management system (ERMS) captures and organizes electronic records into a system that provides the necessary structure, content, and context of records; ensures records are fixed so they cannot be altered; links related records; enables retrieval; retains; controls access; and allows for the disposal of records according to business and records management rules.

The way in which this capability can be implemented can vary widely. With the convergence of related technologies and the fact that recordkeeping is closely allied with business process, ERMS solutions are often integrated with other technologies such as document management, workflow, case management, and web content management, to meet various business needs. Systems with this broad range of capability are sometimes referred to as Enterprise Content Management (ECM) systems. Deployment of ERMS or an ECM can be expected to involve business process transformation and automation. In addition, integration of ERMS with enterprise systems like SAP is a need and may also be required for department line of business applications.

We have electronic documents/files, but do not have paper copies. Can we just copy to CD/DVDs or to an external drive and keep them in the office or transfer them like we would paper records to get them off our shared drives?

Storing records on external drives or on removable storage media is not equivalent to filing or capturing related records together in a paper or electronic recordkeeping system. We do not recommend use of removable storage media such as DVDs or flash drives as a substitute to filing to a recordkeeping system. They are a temporary storage solution. While they can be useful to transport and store information offline, records stored on these media are not protected from degradation or technology obsolescence and cannot be readily accessed for corporate use or records management purposes. When removable storage media *are used* for temporary storage, special care must be given to ensure protection against unauthorized access (breach) or data loss.

What would authorized destruction of electronic records look like in an automated environment?

Currently, our desktop environment (office applications, shared drives, SharePoint, etc.) is not supported by the kind of records management capability that is needed. To dispose of electronic records in a way that meets basic records management standards, we need functionality that can apply scheduled retention periods to groups of electronic records and destroy them (i.e. delete all copies in repositories and back-up systems) in a way that is reliable, systematic, transparent and documented, and that avoids ad-hoc, individual decisions on what to destroy.

This kind of functionality is not just about destruction – it is intended to manage files from the point of creation so that they are well-identified, protected from alteration, accessible as long as needed, and then regularly destroyed so that we don't have unmanaged records accumulating in the first place. We know what the needed practices and supporting technology look like, and we look forward to departments implementing them in future -- hopefully not too far down the road! In the meantime, we are very aware that departments are having to make do with user-driven workarounds that are far from ideal.

In our current environment, how would we destroy electronic records in a way that is clearly authorized and documented?

For your immediate issue, we can suggest an interim solution. It is not ideal and involves some risk, so it is something that needs to be considered and decided upon by your management (given their responsibility for program records).

Interim measures for destruction of electronic files

Records schedules may be used to authorize and carry out disposal of electronic records, provided that:

- The records schedule accurately reflects the current activities, records (including electronic), and retention requirements. Regular review of business records requirements and updating of schedules is recommended.

- The electronic records can be clearly identified with a current records schedule (and series component where applicable) and the correct disposal date can be calculated based on known end dates of the records.
- It is possible to apply the retention and disposal actions to groups (e.g., folders, document libraries) of related records governed by the same schedule. Destruction of individual documents in isolation, or in an ad hoc manner, should be avoided.
- The manager responsible for the business area has authorized this action and has assigned the task to a suitable employee. Other staff may need to assist in identifying records, but responsibility for carrying out and documenting the disposal of records should not be left to individual users/employees.
- The records are not subject to a FIPPA request, litigation hold, audit or investigation.
- The deletion is documented in a way that demonstrates the branch's due diligence and accountability for its actions. Key information to capture includes:
    - basic identification of the records destroyed
    - the applicable records schedule
    - the end date of the records
    - the date the records were due for disposal under the schedule
    - the date destroyed
    - the signature or electronic identifier of the person who completed the deletion.

The following considerations should be taken into account:

- Electronic files may not have been well identified or managed in a central, shared directory, so it may be difficult to identify and isolate records for controlled, scheduled disposal. Managers will need to assess the feasibility, effort required and risk of unauthorized destruction or loss of critical information.
- Deletion of electronic files from shared drives may not result in complete destruction of the records. Managers should be aware that copies may continue to reside on system back-ups and in other repositories.
- Records management processes should conform to best practices and accepted standards, so interim measures like this one, which do not conform, should be undertaken as an exceptional measure, and only where the risks are low and alternatives are not available. This is most likely to be the case for records that are routine in nature (low value / low risk), have short retention periods, and are not required for high risk functions or services.

Government Records Office, Archives of Manitoba
T: 204-945-3971 |E: GRO@gov.mb.ca
Visit our web site to learn more about Government Recordkeeping