



Why CMS Backups Don't Satisfy Open Records & FOIA Requirements

Recordkeeping Guidelines for Government Websites

CONTENTS

4

Government Website Open Records Requirements

1. Definition of a Record
2. Website Records
3. Digital Recordkeeping Guidance

6

Why CMS Backups Don't Meet Open Records Requirements

6

CMS Backups vs. Compliant Archiving

8

The Problems with Using CMS Backups for Open Records

1. Lack of Full-text Search
2. Absence of Digital Signatures
3. Lack of Accessibility
4. No Live Replay
5. Lack of Metadata
6. Non-Compliant Storage Solutions
7. Unable to Fulfill Open Records Requests

10

The Solution: FedRAMP® Authorized Website Archiving with Pagefreezer

“The Government cannot be open and accountable if it does not preserve — and cannot find — its records.”

—David S. Ferriero, Archivist of the United States

As more communication moves online, government agencies of all sizes are relying on websites to inform and engage the public. From policy updates and emergency notices, to meeting announcements, public statements, and service changes, important information from public sector organizations is often published online first.

Hopefully it comes as no surprise that all of your government agency’s website content is considered public record, and thereby subject to the [Freedom of Information Act \(FOIA\)](#) or [State Open Records laws](#).

In this guide, we’ll cover:

- What are the open records requirements for websites?
- What is the difference between CMS backups and archives?
- Why aren’t CMS backups enough when it comes to open records requirements?
- How implementing proper website archiving will save time, money, and help you build trust with the public.

Government Website Open Records Requirements

Navigating the landscape of FOIA and open records laws in the U.S. can be complex, especially when it comes to digital records.

Federal Agencies	State & Local Government Agencies
Must comply with: • Freedom of Information Act (FOIA) • Federal Records Act • Guidance from NARA, which explicitly includes electronic records	Must comply with: • State-level Open Records Laws • Public disclosure requirements for electronic records • Retention schedules that often span several years

These requirements apply to websites, social media, and other digital communications as well. While requirements vary by jurisdiction, the expectation is consistent: digital content must be preserved in a complete, authentic, and retrievable form.

Regardless of whether you’re working at the federal government level under FOIA or at a small local government under state mandated open records laws, here’s what you need to know:

1. Definition of a Record

In nearly all cases, anything produced, kept, held, filed, transmitted, or reproduced with or for a government organization, regardless of physical form, could be considered a record. The content, nature, and purpose of a document, not its physical form, impact its classification as a record.

2. Website Records

Websites are usually considered records. As such, a website's design elements and user interactions are considered part of that record as well. Most states don't give website-specific guidance in their recordkeeping requirements, with exceptions like [Massachusetts](#).

3. Digital Recordkeeping Guidance

Accessibility and organization are a major concern in most recordkeeping guidance, second only to the emphasis on the security and authenticity of records.

For example, [California](#) has put forth guidance on making sure records are captured and stored on “trusted systems.” [Florida](#) insists that electronic recordkeeping systems include, at a minimum, backup and recovery procedures, automated methods for integrity checking and digital signatures. [Illinois](#) mandates the capture of “metadata” and [New York](#) requires records be organized, secure, and accessible.

The key recordkeeping requirements for government agency websites are:

- Collect both webpages and metadata
- Retain websites in their original file format (HTML or [WARC](#), not screenshots or PDFs)
- Retain website records for 7 years

Why CMS Backups Don't Meet Open Records Requirements

Most agencies are using a [content management system](#) (CMS) like Wordpress, Hubspot, [AEM](#), or Drupal to manage their website content.

Though many of these systems do have 'backups' to ensure crucial data is not lost, [CMS are not designed for compliant archiving or recordkeeping](#). Unfortunately, backups or versions from CMS do not meet open records requirements and cannot help you fulfill open records requests.

CMS Backups vs. Compliant Archiving

Archives and backups might be used interchangeably in conversation, but they are not the same.

Website backups essentially copy and save data for the purpose of restoring it, if ever lost. What a backup might include depends on the CMS you're using, but generally, they do not exist to serve as long-term storage of data. You may be able to recall a former saved version of your website or a webpage if you are diligent about keeping and managing different versions, but that takes a lot of manual work. Backups are also not admissible as records or evidence in court, because they don't capture timestamps or metadata.

CMS backups are not designed with compliance or accessibility in mind.

An archive is a collection of historical data stored for long periods of time, often for compliance and legal reasons. When data is archived, content is stored with metadata and other authenticating details. Archives are inactive and historical. Archiving holds on to the record without it preventing new, updated information from being presented.

The main difference between backups and archives is that a backup takes periodic snapshots of data to help you recover records that get lost. Most backups are saved for a few days or weeks until they make way for new backup data to overwrite it. This works well in the short-term in the case of an emergency recovery of data. An archive, on the other hand, is a record. It is a verifiable, authenticated account of your website at a particular point in time.

Archiving vs. CMS Backups for Websites

	Archive	CMS Backups
Full-text Search	✓	✗
Digital Signatures	✓	✗
Accessible	✓	✗
Live-Like Replay	✓	✗
Metadata	✓	✗
Long-term Retention	✓	✗
Allows Legal Holds	✓	✗
Tamper-Proof	✓	✗
Compliant Data Storage	✓	✗
Compliant Export	✓	✗
Best for	Compliance, Open Records	Emergency data recovery

The Problems with Using CMS Backups for Open Records

1. Lack of Full-text Search

One of the main advantages of a proper website archive is the ability to perform a full-text search across all archived pages. This functionality is critical for finding specific content quickly, especially in legal or compliance situations. CMS backups, however, do not offer this feature, making it difficult to locate specific information within the backup.

2. Absence of Digital Signatures

Website archiving solutions often include digital signatures that authenticate the archived content, ensuring its integrity and proving that it hasn't been altered. In contrast, CMS backups do not provide this level of verification, which means anyone can export a file and manipulate it, making it an unreliable, possibly fraudulent record.

3. Lack of Accessibility

Accessing data from a CMS backup often requires technical expertise and assistance from the IT department, which can delay access and make it impractical for everyday use. Website archiving tools, on the other hand, can provide easy-to-use interfaces and advanced search capabilities, allowing non-technical teams like legal or marketing to retrieve archived content independently and quickly.

4. No Live Replay

A significant benefit of a proper website archive is the ability to replay the site exactly as it appeared at a certain time, including interactive elements and multimedia. CMS backups typically don't offer this feature. Instead, they only store the raw data, leaving users with a static and incomplete version of the site that doesn't fully replicate the original experience.

5. Lack of Metadata

CMS backups often do not store the necessary metadata—such as timestamps, version history, or authorship—needed for open records. Metadata is critical when proving when changes were made or who was responsible for a particular update, and its absence can create significant gaps in the archived data.

6. Non-Compliant Storage Solutions

CMS backups are stored in ways that don't meet open records compliance standards. A website archiving solution, however, ensures that archived data is stored securely, with the necessary features like encryption, tamper-proof storage, and full audit trails to meet industry regulations.

7. Unable to Fulfill Open Records Requests

Without proper website archiving, you'll be left struggling to fulfill requests and unable to adequately verify the historical authenticity of your records. Backups can't be exported into a format that is universally accessible nor can they be properly authenticated, which can leave your agency at risk of not being able to fulfill a basic FOIA request.

The Solution: FedRAMP® Authorized Website Archiving with Pagefreezer

“Switching to Pagefreezer has saved us 800-900 hours per year. That’s a dramatic impact. We’ve also seen a 30% reduction in open records requests with the public portal.”

– Kelley Smith, Information Technology Specialist (INET), US Federal Government Agency

Pagefreezer’s [FedRAMP® authorization](#) means our web archiving solution meets the US government’s strictest standards for cloud security and continuous monitoring.

We’ve worked with hundreds of government agencies to build a solution that effectively archives and preserves your website to comply with state and federal open records laws—so records are accurate, secure, and ready when they’re needed.

With Pagefreezer, government agencies can:

- Automatically archive websites and social media in native, tamper-proof format
- Capture edits, deletions, metadata, timestamps, and digital signatures
- Ensure compliance with open records and FOIA requirements
- Reduce staff time spent responding to public records requests
- Provide self-service public access through a customizable records portal

Pagefreezer is trusted by government agencies of all sizes, including major federal, state, and local organizations, to support transparency and long-term records integrity.

Still relying on CMS backups for Open Records?

Let us show you how we are helping hundreds of government agencies simplify open records compliance, build trust, and get peace of mind.

Email:

sales@pagefreezer.com

Phone:

+1.888.916.3999 (North America)

+44 (0)20 3314 7921 (U.K.)

+31 (0)76-5324275 (Europe)

pagefreezer.com