Hennepin County Written Testimony

November 20, 2025

Legislative Commission on Data Practices

Prepared by Kristi Lahti-Johnson
Hennepin County Responsible Authority and Data Practices Compliance Official

Co-Chairs Feist and Scott and members of the Commission,

I am excited that this Commission is looking at possible opportunities for modernization data and records management statutes that better reflect changing technologies and society's increasing reliance on computer-based services.

As I prepared my testimony for today, I have come to better appreciate the interconnectedness between agenda items 2 and 3: looking to best practices around data minimization, retention, and maintenance, as a way to address some of the challenges faced by location governments. In addition to providing testimony on these issues, Hennepin County has identified some possible solutions.

Laws protecting personal contact information are inconsistent

Best Practices: Modern consumer privacy laws and regulations create privacy expectations related to personal contact information.

While consumers often accept all cookies and tacitly give approval to the sale of their data to other companies for promotional purposes, there is an expectation of privacy as it relates to sharing data with anyone who asks for it. For example, if Caribou would receive a request for a list of names and emails for everyone that has provided feedback on the newest Caribou seasonal drink, they would not share that information with the requester. These expectations often carry over to how individuals believe government entities should handle their data. However, unless classified as private, under the Minnesota Government Data Practices Act (MGDPA), personal contact information is public. So, if a resident contacts Hennepin County to share feedback on the building plans for the new Southdale library, the contact information provided by the resident would be considered public, and we would be required to provide it to anyone who requests it.

Challenges: Because the MN Data Practices Act starts with the presumption that all government data is public, we have seen a patchwork approach to protecting individual privacy rights, particularly personal contact information for individuals at high risk.

After the general administrative provisions of the MGDPA, there are 163 pages that classify data as not public. Additionally, other laws have been implemented protecting individuals in high-risk situations. There is Safe at Home, the Judicial Protection Act, and the anti-doxing laws for elections officials and law enforcement officials. The MN Safe at Home

Office is a great example of the best way to administer these protections. They work closely with individuals seeking these protections to help them understand what they need to do to stay safe and what they can expect of government entities. For other programs, we often receive insufficient information to verify identity making it difficult to confidently apply the protections. There has been less consistency implementing the other statutory protections:

- One of the programs has a form to submit, but for a larger county, if the individual requests protection for family members, the form does not provide us with enough information to verify the identity of the individuals. This is especially problematic for individuals with common names, since we cannot legally provide the protection to every individual with that name. We have reached out to individuals requesting additional information to ensure that we are protecting the correct information, but people do not respond to our requests for clarification. We have also reached out to the entity administering the forms asking them to add additional information and have not received a response.
- Other programs do not require that a form be used to submit a request, so we often do not get adequate information to apply the protections, or that the request be submitted to the government entity's Responsible Authority. Yet there are criminal penalties and civil remedies for violating the protections.
- For both of the anti-doxing laws the protections are to be applied if the information poses an "imminent and serious threat", without any guidance on who is responsible for evaluating that condition.
- Other programs do not require that the protections be reviewed and renewed periodically, regardless of whether there is a change in the individual's circumstances.

Hennepin County offers two solutions:

1) Make personal contact information (home address, email address, and personal phone numbers) presumptively private, unless they are required by law to be public.
2) For individuals/groups seeking additional protections, include provisions that these protections be coordinated by a single entity at the state level (e.g., Safe at Home)

The volume of electronic data that government entities receive continues to increase with society's reliance on computer-based services

Best Practices: In the landscape of increased cybersecurity threats and incidents, Hennepin County seeks to follow industry standards to minimize the amount of personal data that we retain about our residents.
Following are three ways that Hennepin County works to minimize the risk to personal data:

1. We provide direction to staff to move data that is part of an official record to its designated record storage location and to securely dispose of data that is not part of an official record when there is no longer a business need for it.
2. We maintain and dispose of our official records using our official records retention schedule which is approved by the MN Records Disposition Panel.
3. We use the technology available to us to manage our official records. We store records electronically, and we use access management to ensure that only those individuals with the legal authority to access the data do so.

Challenges: The evolving nature of records formats is not adequately supported in the Official Records Act.
When the Official Records Act was enacted, most records were in a physical—often paper—format. Now, most records are created electronically.

The Official Records Act provides examples of formats for official records, including items such as papers, documents, and computer-based data. However, the Official Records Act has never required that government entities maintain all paper or all computer-based data, only those "records necessary to a full and accurate knowledge of their official activities". Taken

together, the Official Records Act and the Records Management Act document retention requirements for official records based on the content of the record, regardless of its format or storage medium.

At the same time, the Official Records Act is prescriptive about the ways government records can be reproduced. Many of the methods outlined in the statute, such as microfilm, photostat, and optical disc imaging are almost obsolete. With changing technology, listing out specific physical forms or storage media creates limitations on how government entities may most effectively and efficiently store government records. For those records that are classified as permanent, current statute is ambiguous about whether these records may be reproduced digitally.

Hennepin County offers the following solution:

1) Update the Official Records Act to permit the digitization of all official records and to allow government entities the flexibility to digitize records without prescribing the storage medium or format.

The challenges that have been identified have an impact on Hennepin County's responsiveness to data practices requests

Hennepin County is a large county with a significant amount of data (see image 1). However, the challenges that we face in responding to data practices requests are not unique to us.

It is very important to understand making a request to a government entity for data is not like performing a Google search. No entity that I am aware of possesses only searchable databases, much less ones that are connected.

Hennepin County uses a data portal to manage its data practices requests. The portal does not use Artificial Intelligence. It is administered and managed by the Compliance Office. In 2024, Hennepin County received 7,741 data requests (see images 2 and 3).

While many requests are focused on specific records, for example, I'd like a copy of the county's contract for on-site shredding or a copy of an accident report, others are more all-encompassing, often requesting "all communications" between certain persons or on a certain topic. Technology has allowed us to search and retrieve this data more efficiently. That said, once retrieved, each document must still be reviewed. In the first 8 months of this year, Hennepin County conducted 51 searches of emails in response to data requests, and staff have needed to review over 107 thousand items to ensure that private data is protected before being released to the requester.

The solutions proposed by Hennepin County allow government entities to better respond to data requests by:

1) Taking a consistent approach in redacting personal contact information, regardless of its context. This also reduces the risk of inadvertently releasing data that is classified as private.
2) Disposing of data that is not part of an official record and for which there is no longer a business need. This helps to support government transparency by providing more timely access to responsive data.
3) Digitizing all government records to ensure that records are readily accessible as required by statute.

Contact

Hennepin County – Compliance Office
Kristi Lahti-Johnson
Hennepin County Responsible Authority and Data Practices Compliance Official
Office: 612-348-4307
Kristi.lahti-johnson@hennepin.us

Website

hennepin.us

Image 1:

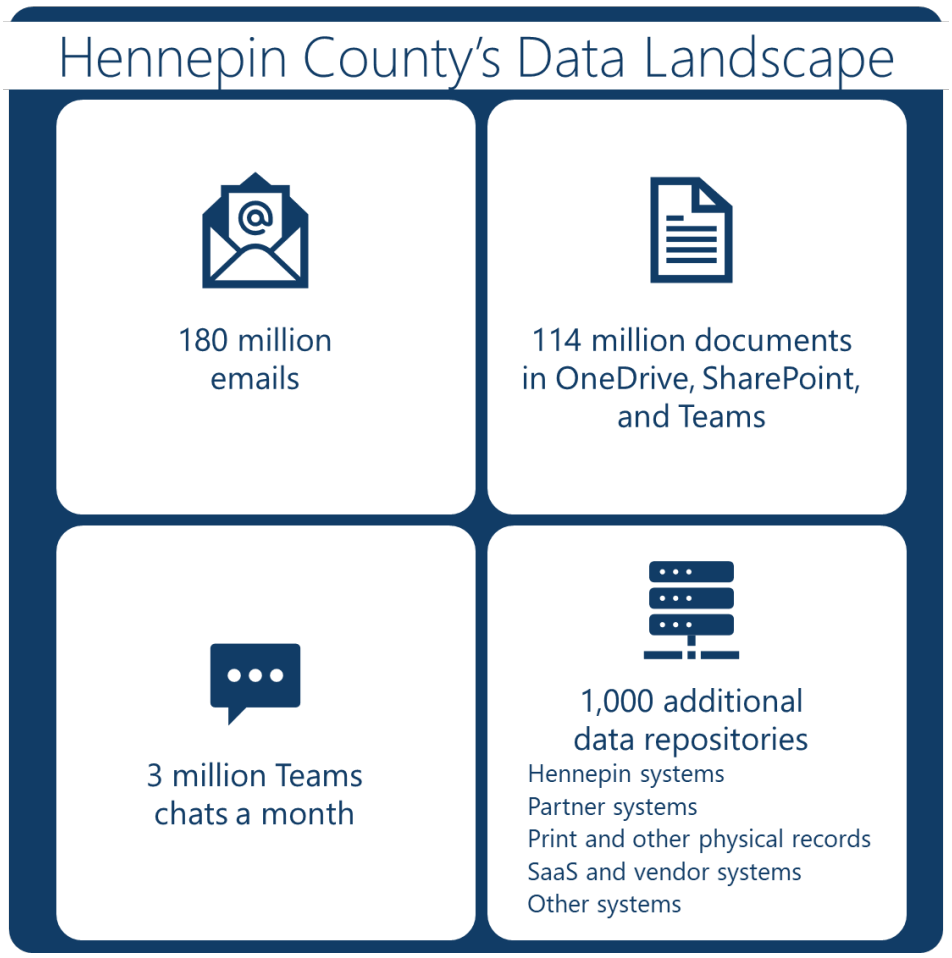


Image 2:

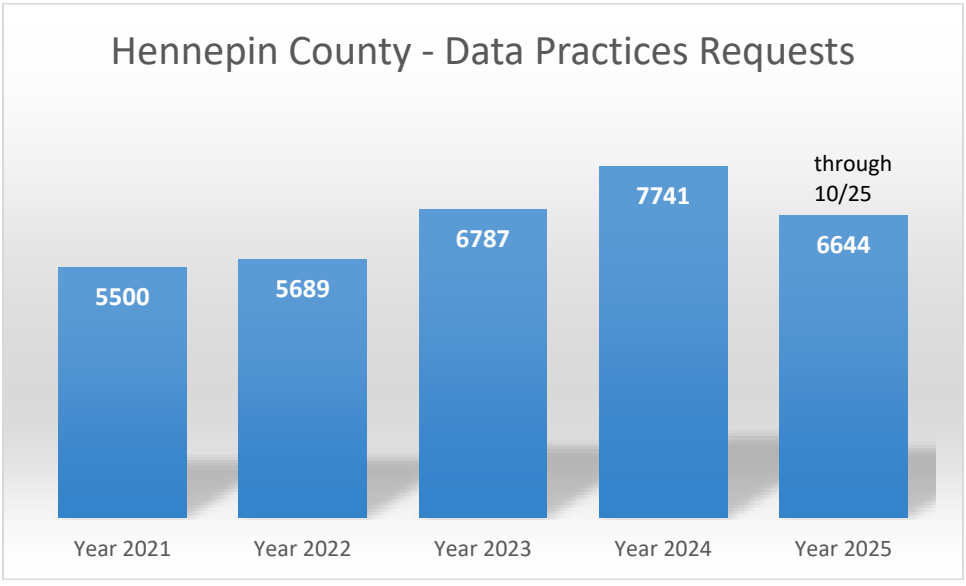
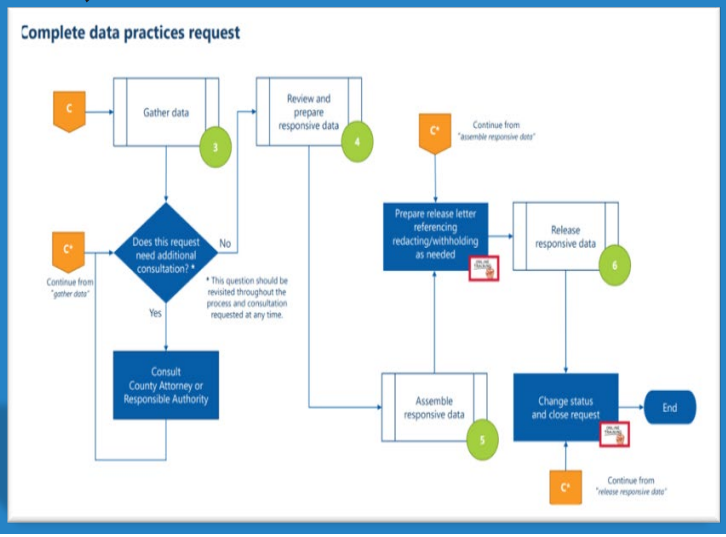


Image 3:

AFTER WE RECEIVE A REQUEST



PROCESSES WITHIN A PROCESS

- **Gather the data:** Where is the data? Who has access to the data? Do we need to do a Purview search for communications or other documents?
- **Review and prepare the data:** Is all the data responsive? Does any of the data need to be withheld or redacted? Do you need County Attorney review? Apply redactions.
- **Assemble and release the data:** Convert the data to a PDF, unless requested in its native format. Upload the data into GovQA, unless requested in another way. Communicate the release of the data, including providing citations for any withholding or redactions.