OVERVIEW OF CHANGES TO THE ACCESS TO PUBLIC RECORDS ACT (APRA)

House Enrolled Act 1360

Public Law 97-2026

Governor Mike Braun signed House Enrolled Act 1360 (HEA 1360) on March 4, 2026, and the new law takes effect on July 1, 2026.

HEA 1360 passed the Indiana House of Representatives with a vote of 95 yeas and 0 nays. It also passed the Indiana Senate with a vote of 48 yeas and 0 nays. The Office of the Public Access Counselor (OPAC) provides this Overview to provide guidance to public agencies and to the public on HEA 1360's changes to Indiana's APRA (Indiana's open records law). Indiana Code (IC) 5-14-3.

Summary

In recent years, public agencies have reported an increasing number of bulk public records requests that appear to originate from automated sources rather than individuals. Additionally, public agencies reported a growth of phishing attempts when reviewing public records requests that have been submitted via email. The increasing number of requests, together with the rise of data scraping and automated systems employed by certain organizations, resulted in significant strain on public agency resources.

To address this growing trend, HEA 1360 makes several significant changes to Indiana's APRA. The changes modernize the public records process and set reasonable limits to protect agency resources. This Overview covers five (5) topics.

First, HEA 1360 authorizes public agencies to establish an electronic portal to receive and acknowledge public records requests. These portals can screen requests and track their sources. For example, a portal may confirm the requester is a real person, verify their address, check Indiana residency, and flag submissions from known sources of phishing (deceptive requests designed to trick staff) or data scraping (automated tools that extract large amounts of data).

Second, HEA 1360 allows agencies to prioritize Indiana resident requests and requests submitted for civic, journalistic, academic, or personal use. Agencies can deprioritize both out-of-state requests and automated requests while charging a supplemental fee for these requests.

Third, HEA 1360 allows agencies to deny suspected data scraping requests, phishing requests, and requests that could compromise the agency's electronic

systems or data, while also mandating that agencies report suspected requests to OPAC.

Fourth, HEA 1360 authorizes agencies to deny requests that are duplicative of the litigation discovery process.

Finally, HEA 1360 requires the public access counselor to coordinate with public agencies and compile information from Indiana's public agencies. Specifically, the counselor must track the number and type of requests received and flag patterns tied to automation, phishing, or data scraping. IC 5-14-4-10(8). To support this, public agencies must report certain information to OPAC throughout the year and submit a full annual report each June.

1. Electronic Public Records Portals

Starting in July 2026, IC 5-14-3-3.3 permits public agencies to set up and maintain an electronic portal to receive and acknowledge public records requests. The portal may include the following features:

1) Incorporate CAPTCHA (a test that confirms the user is a human, not a computer program) or an equivalent mechanism to ensure the requestor is a human;

2) Require verification of the requestor's physical address;

3) Utilize a tool to determine whether the requestor is a resident of Indiana; and

4) Automatically track and report submissions suspected to be automated or that come from known sources of data scraping or phishing.

2. Prioritizing Certain Requests

Starting in July 2026, IC 5-14-3-8.1(a) permits public agencies to give priority to fulfilling public records requests from Indiana residents and requests submitted for civic, journalistic, academic, or personal use. To receive priority, the requestor must clearly state the purpose of the request.

IC 5-14-3-8.1(b) permits public agencies to delay responding to out-of-state requests and automated requests as necessary to prevent disruption of core agency functions.

Below are three suggested questions that agencies might ask requestors during the request submission process.

1. Select one of the following:
   - ☐ I am an Indiana resident.
   - ☐ I am not an Indiana resident.

2. I am making this request on behalf of (select one of the following):
   - ☐ Myself
   - ☐ Another person who is an Indiana resident.
   - ☐ Another person who is not an Indiana resident.
   - ☐ An entity that is based in Indiana.
   - ☐ An entity that is not based in Indiana.

3. Select one of the following, I am making this request for the following purpose:
   - ☐ Civil, philanthropic, journalistic, academic, or personal use.
   - ☐ Commercial use.
   - ☐ Some other use.
   - ☐ Prefer not to say.

Tracking the answers to these questions might aid in:

(1) allowing agencies to make priority determinations under IC 5-14-3-8.1; and

(2) gathering necessary information for the agency's annual reporting to OPAC.

Supplemental Fee for Out-of-State & Automated Requests

Public agencies may collect a supplemental fee when responding to out-of-state requests or automated requests. The fee must be tied to the actual cost of fulfilling the request. It may not exceed $0.25 per page or $25 per hour of staff time. IC 5-14-3-8(n). An agency may waive the fee if the request serves the public interest. IC 5-14-3-8(o). If adopted, agencies must apply the fee consistently to all out-of-state and automated requests.

Reporting Automated Requests

A public agency **must** report to the public access counselor any request received by the agency that the agency suspects of being automated. IC 5-14-3-11. Note, an agency does **not** have discretionary authority to deny a request solely because it is a suspected automated request.

Information on how public agencies can make these mandatory reports to OPAC can be found starting on Page 7.

3. Data Scraping, Phishing, & Cybersecurity Risk Requests

The new law defines “data scraping” and “phishing” for APRA purposes. Both terms describe ways bad actors misuse the records request process.

"Data scraping" means use of an automated system to extract data from websites and other Internet accessible sources. IC 5-14-3-2(d).

"Phishing" means a method of obtaining information through fraud. The sender hides or misrepresents who they are to trick the recipient into sharing information or granting access. IC 5-14-3-2(p).

Cybersecurity risk is not defined in the code, as data scraping and phishing have been.

Handling of Suspected Data Scraping, Phishing, & Cybersecurity Risk Requests

HEA 1360 gives public agencies discretion to deny a public records request if the agency suspects the request to be a data scraping request, a phishing request, or a cybersecurity risk request. But time is of the essence for public agencies handling these requests.

A public agency may deny a request if the agency suspects the request is a:

1) data scraping request,

2) phishing request, or

3) request for electronic transmission that:

   (a) may expose the public agency’s electronic systems or data to unauthorized use or alteration; or

   (b) could otherwise jeopardize the security of the public agency's electronic systems or data.

IC 5-14-3-3.3(b). If the agency declines the request, the agency must notify the public access counselor of the request and the statutory basis for the denial. IC 5-14-3-3.3(c). That notice must be submitted no later than seven (7) days after the agency receives the suspected public records request. IC 5-14-3-3.3(c).

The agency may also fulfill a request that the agency suspects to be data scraping or phishing activity. If the agency responds to such a suspected request, the

agency must report to the public access counselor request that the agency suspects of being data scraping or phishing activity. IC 5-14-3-11(2).

Information on how public agencies can make these mandatory reports to OPAC can be found starting on Page 7.

Below is a suggested written notice that agencies might provide to requestors during the request submission process.

> IC 5-14-3-3.3(b) gives public agencies the authority to deny a request if one or more of the following apply:
>
> (1) The public agency suspects the request to be data scraping or phishing activity.
>
> (2) The public agency suspects that responding to the request electronically may:
>
> (A) expose the public agency's electronic systems or data to unauthorized access or alteration; or
>
> (B) otherwise jeopardize the security of the public agency's electronic systems or data.

Potential Indicators of a Suspicious Public Records Request

The table on the following page presents hypothetical public records requests with indicators that may signal a suspicious public records request. It uses examples from real agency experience to highlight warning signs agencies should watch for. The examples are not exhaustive and new threats are discovered regularly.

Reviewing these examples may help public agencies evaluate requests for potential automation, data scraping, phishing attempts, or other cybersecurity risks.

By way of reminder, a public agency is **not** obligated to create a new document or compile information into a format that does not already exist when responding to a public records request.

Category	Hypothetical Request	Indicators
High-Volume Dataset	"I am formally requesting a spreadsheet containing information on every purchase made from 2021 to the present. Specifically, I request that the spreadsheet include the following details for each transaction: unit pricing, vendor IDs, quantities purchased, total amounts, and any additional relevant fields maintained in your records."	Seeks exhaustive datasets of structured data. Common target for data scraping.
Repetitive Identical Requests Submitted in Bursts	Within a few minutes, the agency receives five versions of the same message: "I request all available public records related to property ownership in your county."	Identical wording sent multiple times. Timing pattern suggest automation.
Script-Generated or Odd Formatting	"I requ3st ALL rec0rds relat3d to REZIDENCE DATA for ALL parc3ls. Pls respond ASAP with d4ta in CSV."	Machine-like formatting, substitutions, or errors suggest automation. Specific request for structured formats used in data scraping.
Sequential Slice Requests	"Please provide property tax records for parcel numbers: 000001–000500; 000501–001000; 001001–001500; [... and so on]."	Typical of bots designed to iterate through numbered datasets.
Phishing Techniques	"I am submitting a public records request under state law. I need all employee contact lists, including direct phone numbers and email login information, for immediate compliance review. To avoid penalties, please upload the files using the secure portal below within 24 hours."	Overbroad request for sensitive data. Urgent language and threats. Includes a fake "secure" link using a deceptive domain. Asks staff to confirm credentials, a major red flag.
Technical or Coded Language	"Please export the court docket database in JSON or XML, including all indexed fields."	Requests a database level export rather than a typical public record. Uses formats aligned with automated ingestion.
Personally Identifiable Information	"Send all records that contain any citizen's name, address, or contact information across any agency departments."	Extremely broad request. Overinclusive PII target typical of data scraping activity.

4. Pending Litigation Denial

Starting in July 2026, a public agency may deny a public records request if the request:

1) is made by a person who is a party to pending or ongoing litigation; and

2) is duplicative of a discovery request the person made in the pending or ongoing litigation.

IC 5-14-3-4(e). Note, there is **no** statutory requirement for an agency contemporaneously report a pending litigation denial to OPAC.

Below is a suggested written notice that agencies might provide to requestors during the request submission process.

> IC 5-14-3-4(e) gives public agencies the authority to deny a request if the request:
>
> (1) is made by a person that is a party to pending or ongoing litigation; and
>
> (2) is duplicative of a discovery request made by the person in the pending or ongoing litigation.

5. Public Agency Reporting to OPAC

HEA 1360 expands the duties of the public access counselor. The counselor must now work with public agencies to track the number and type of records requests they receive. The counselor must also identify patterns of excessive, automated, phishing related, or data scraping requests. IC 5-14-4-10(8).

Additionally, the counselor's annual report to the legislative services agency must now include a summary of public records requests received by public agencies. That summary must include information about requests suspected of being automated, data scraping, or phishing activity. IC 5-14-4-10.

All public agencies will collaborate with OPAC's compilation of this data for the General Assembly in two different ways: 1) contemporaneous reporting and 2) annual reporting.

Contemporaneous Reporting

First, as discussed above, there are instances when a public agency must notify OPAC.

Request Denied due to Suspicion. If the agency denies a request because the agency suspects the request of data scraping, phishing, or a cybersecurity risk, the agency must notify the public access counselor of the request within seven (7) days of receipt of the request. IC 5-14-3-3.3(c).

Suspicion of Fulfilled Request. If the agency fulfills a request that the agency suspects of being automated, data scraping, or phishing activity, IC 5-14-3-11 requires agencies to report each such request to OPAC.

Note, the statute does not establish a deadline for agencies to report a suspicious request that the agency decides to fulfill. OPAC requests that all public agencies submit these Suspicion of Fulfilled Request reports contemporaneously and in the normal course of fulfilling suspect public records requests. Links to online submission forms for both contemporaneous report types will be posted on OPAC's website. A pdf of each form is hyperlinked at the end of this guidance.

Contemporaneous reporting in these two instances will aid in meeting the General Assembly's directive that the public access counselor coordinates with public agencies to identify patterns or sources of excessive, automated, phishing related, or data scraping based public records requests. IC 5-14-4-10(8).

Annual Reporting

Starting in June 2027, public agencies will file a report with OPAC on an annual basis. Each agency's annual reporting will aid in meeting the General Assembly's directive that OPAC coordinate with public agencies to track the volume and nature of public records requests received by public agencies. IC 5-14-4-10(8). The first agency annual report will cover the period from July 1, 2026, through May 31, 2027. Agencies must submit their reporting form to OPAC by June 11, 2027. OPAC will then compile the data for the public access counselor's annual report to the General Assembly, which is due June 30, 2027. IC 5-14-6 & IC 5-14-4-12.

The counselor's annual report will include recommendations based on the analysis of the data collected under the new provisions. These recommendations may include proposed statutory or administrative remedies for excessive, automated, phishing related, or data scraping based public records requests. A link to the online submission form for agency annual reporting will be posted on OPAC's website. A pdf of the annual reporting form is hyperlinked at the end of this guidance.

❖ ❖ ❖

HEA 1360 aims to improve Indiana's public records system by equipping public agencies with tools to address the rising number of automated and out-of-state requests that can strain their resources. The law adds safeguards to keep the process focused on traditional requests and combat technology-driven misuse. Hoosiers should have prompt, transparent access to public information. HEA 1360 aims at ensuring that certain technology-driven requests don't slow down service for everyone.

Thank you, in advance, to all public agencies for their cooperation and collaboration with OPAC.

❖ ❖ ❖

For pdf of the statutory language, click here.

For pdf example of the Request Denied Due to Suspicion Notice, click here. However, to complete the online form, click here.

For pdf example of the Suspicion of Fulfilled Request Notice, click here. However, to complete the online form click here.

For pdf example of the Annual Summary Report form, click here. However, to complete the online form click here.