

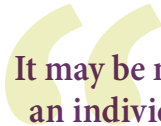


OPEN RECORDS REQUESTS: AN INTRODUCTION

How to accommodate the public's right to know while complying with state and local laws.

By Christine Massengale and Ron Ginn

The release of information from any government entity, including emergency communication centers (ECCs), is often a responsibility full of complications and legal challenges. Every state has variations of open records laws, sometimes called sunshine laws, which are typically derived from federal Freedom of Information Act (FOIA) laws. Since 1967, FOIA has ensured public access to federal records, intended to provide transparency about how the government operates and prevent misconduct and waste. Similarly, state and local governmental agencies have laws and rules to provide records to the public.



It may be necessary to allow an individual to view files or listen to recordings even though they cannot take possession of the file or data.

The most common open records requests for ECCs are audio recordings of phone and/or radio traffic as well as computer-aided dispatch (CAD) records from calls for service and responder activity logs. For police departments, records requests are usually from insurance companies and individuals for incident reports such as car crashes or burglaries.

One of the first complications for these requests is, who owns the records? An ECC that is contractually holding the records, i.e., managing the storage, access and dissemination of such records, may not be the owner. Rather, the request may be routed to the client-agency served by the ECC for approval of release or a decision on the redaction of protected information.

Next, what is considered a record? Aside from recordings and police reports, how is work product defined and what makes it “discoverable” or subject to an open records request? The answer may vary by state, but any written communication may be considered work product, including email, instant message (IM) chat logs, CAD documentation, paper logs, and even scratch notes or sticky notes attached to files. This may also include files associated with internal processes such as financial activities, policies and procedures, personnel files, and even hiring practices.

Audio recordings may include emergency and non-emergency calls, as well as personal calls placed from a business line that is recorded. What about security camera footage, center recordings and even business activity handled by a personally owned electronic device, such as a cell phone? Are text messages subject to open records requests even if sent from a personal device? Maybe. There are cases where sunshine laws were challenged due to an individual’s use of their personal cell phone during a public meeting to surreptitiously discuss business in a private side conversation.

That’s a lot of data available for public consumption, so are there any protections for victims or ways to ensure privacy, especially for first responders? Yes and no. While most states have very generous open records laws, certain pieces of data are protected from release through redaction or exemptions. Redaction may be used to hide or omit pieces of an overall report, such as names of juveniles, medical information, personally identifiable information (PII) or other details that may

pose a threat to an individual or entity, such as home address or personal phone numbers.

There may be other records unavailable to the public, including those considered safety-sensitive such as building schematics that would jeopardize site security, continuity of operations plans (COOPs) and other details about infrastructure, like radio tower sites. Those requesting the information may be required to verify their identity and be specific about the request to limit “fishing” or requesting large volumes of overly broad records. In some instances, open records requests have been deemed malicious attempts to overburden an agency by asking for thousands of documents at a time or for several years of archival data. In such cases, an agency may not be required to provide such a large volume of documents, especially if it is not reasonable to do so with their available resources.

What is the retention period for records? It depends on the type of record and any specific state laws, agency rules, standards compliance or limitations of data storage capabilities. For example, an agency might store audio recordings for one year, but CAD records are retained five years (or even indefinitely or for the life of the system). Individual agency policy may encourage employees to discard written scrap notes in the shred box at the end of every shift, while shift briefing logs (written or digital) might be kept for a week, a month, a year or indefinitely, depending on the agency’s storage capabilities and policy. Video files such as quality assurance screen capture require enormous storage capacity, even for a short period of time, and an agency may opt to allow the files to drop off after 10 to 30 days. Internal agency practices may also be protected from open records requests, but depending on state laws, that may be open to interpretation.

How are the records released or reviewed? Many agencies maintain records digitally, and the systems used to archive the data may create digital file formats protected by encryption or verification keys that limit the file type used for dissemination. What processes are in place to allow the public to view a record

rather than take possession of it as a copy of the original? It may be necessary to allow an individual to view files or listen to recordings even though they cannot take possession of the file or data. This means allowing the individual access to a room or office where the data can be seen, heard or accessed with supervision by agency personnel.

Finally, when a copy of a record is provided to a requestor, what changes, if any, can be levied to recoup the expense to the agency? This is defined by each state’s law, and agency policy should align closely with that. A few sheets of printed paper in a police report or audio files transferred to a CD may seem like negligible expenses to an agency, but when hundreds are disseminated over the course of a year, the expense may be significant. Some agencies provide copies of reports through an online process, which allows the requestor to save the file in a digital format or take responsibility for printing a hard copy for themselves. One of the most important issues is that any charges should only recoup the expense of reproducing the record.

State laws vary, but these guidelines may help keep your agency from running afoul of the laws:

- Know your state’s statutes and agency policy on records retention and any variances for file types.
- Verify who owns the record, and ensure there are no provisions preventing its release.
- Identify what constitutes a record, what is subject to release and what is protected under exemptions or redaction.
- Design and implement a consistent method of records release, according to a variety of file types (paper logs, digital files, audio files, etc.).
- Respond to requests within the time frame required by law or, if necessary, ask for an extension.
- Cite exemptions or redaction laws that would protect records from release.
- Design a process for documenting requests, logging completion of assignments and method of dissemination.
- If fees are levied for records, ensure proper fiscal accountability for auditing purposes.
- If in doubt, do not send it out — consult with your agency’s legal counsel before disseminating records, but provide an update to the requestor that it is being actively reviewed.

In this digital media era, the public's right to know coupled with the desire for data on-demand make it more important than ever to ensure your agency stays up to date on the requirements surrounding open records releases. ●

Christine Massengale, ENP, RPL, is the Dispatch Coordinator for the Tennessee Highway Patrol's four consolidated dispatch centers and the Chair of the APCO Editorial Committee.

Ron Ginn began his career as a police officer in 1989, retiring with the rank of Patrol Sergeant. He returned to law enforcement in 2013 before transitioning to public safety communications in 2016 and currently serves as the Deputy Director of the Stone County Missouri 9-1-1 Center.

CDE EXAM #58170

- | | | |
|--|---|---|
| <p>1) The Freedom of Information Act (FOIA) was created in:</p> <ol style="list-style-type: none"> a. 1969 b. 1972 c. 1967 d. 2012 <p>2) Data that may be considered “discoverable” or subject to an open records request might include:</p> <ol style="list-style-type: none"> a. Private social media account log-on information b. Business messages conducted over a privately owned electronic device c. Names of juveniles d. Information associated with an individual and communicable diseases <p>3) When seeking guidance about what information should not be released, review these rules or laws:</p> <ol style="list-style-type: none"> a. Redaction and exemptions b. Policy and procedure c. Terms and conditions d. Citizen's right to know <p>4) Which of the following records would not be subject to an open records request:</p> <ol style="list-style-type: none"> a. IM chat logs in CAD b. Employee social security numbers c. Paper logs on call activity d. Scratch notes associated with employee interviews | <p>5) Often, the intent of a fishing expedition is to:</p> <ol style="list-style-type: none"> a. Confuse the records clerk b. Over burden the agency's ability to respond to the request c. Give the records clerk something meaningful to do d. Gain access to unauthorized data <p>6) What fees is an agency authorized to charge for the release of records?</p> <ol style="list-style-type: none"> a. As much as it deems appropriate b. No more than 10% profit over the expense c. Only what is necessary and reasonable to recoup the expense of reproducing the record d. There are no guidelines for charging fees <p>7) The retention period for records:</p> <ol style="list-style-type: none"> a. Depends on an individual state's statutes b. Is guided by an agency's policies or standards compliance c. May depend on the capability of the agency to store the file type d. All of the above | <p>8) A particular complication that ECCs may encounter in dealing with open records requests is:</p> <ol style="list-style-type: none"> a. Determining who owns the record and is responsible for authorizing its release b. How the data will be made available to the requestor c. How to hire a records clerk d. Both b and c e. Both a and b <p>9) If in doubt about an open records request, complete the request and provide it anyway.</p> <ol style="list-style-type: none"> a. True b. False <p>10) The process for documenting open records requests should include:</p> <ol style="list-style-type: none"> a. Any fees that were charged for the release of records b. A detailed description of the person making the request c. How the person intends to use the records d. None of the above |
|--|---|---|

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.
2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).
3. Add/upload your CDE article information and certificate of achievement in the “My Classes Taken” section of APCO’s Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online!

To receive a complimentary certificate of completion, you may take the CDE exam online. Go to <http://apco.remote-learner.net/login/index.php> to create your username and password. Enter CDE in the search box, and click on the “2021 Public Safety Communications CDE Magazine Article Exams,” then click on “enroll me” and choose “Open Records Requests (58170)” to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.