

[Cite as *Eye on Ohio v. Ohio Dept. of Health*, 2020-Ohio-5278.]

EYE ON OHIO, OHIO CENTER FOR
INVESTIGATIVE JOURNALISM

Requester

v.

OHIO DEPARTMENT OF HEALTH

Respondent

Case No. 2020-00279PQ

Special Master Jeff Clark

REPORT AND RECOMMENDATION

{¶1} The Ohio Public Records Act requires that copies of public records be made available to any person upon request, within a reasonable period of time. R.C. 149.43(B)(1). The state policy underlying the Act is that open government serves the public interest and our democratic system. To that end, the public records statute must be construed liberally in favor of broad access, with any doubt resolved in favor of disclosure of public records. *State ex rel. Rogers v. Dept. of Rehab. & Corr.*, 155 Ohio St.3d 545, 2018-Ohio-5111, 122 N.E.3d 1208, ¶ 6. A requester alleging violation of the Act must establish entitlement to relief by clear and convincing evidence. *Hurt v. Liberty Twp.*, 2017-Ohio-7820, 97 N.E.3d 1153, ¶ 27-30 (5th Dist.).

{¶2} In this case, Eye on Ohio, Ohio Center for Investigative Journalism, requests the records of daily hospital bed capacity, medical supplies, and staffing levels compiled by the Ohio Department of Health in its Surgenet data system. Eye on Ohio intends to report this data to the public as “the people’s records” documenting the day-to-day availability of hospital services during the ongoing Covid-19 pandemic.¹ (Complaint at 8-12, 15.)

¹ “The rule in Ohio is that public records are the people’s records, and that the officials in whose custody they happen to be are merely trustees for the people; therefore anyone may inspect such records at any time, subject only to the limitation that such inspection does not endanger the safety of the record, or unreasonably interfere with the discharge of the duties of the officer having custody of the same.” (Citation omitted.) *State ex rel. Patterson v. Ayers*, 171 Ohio St. 369, 371, 171 N.E.2d 508 (1960).

{¶3} Courts recognize that the news media enable an informed public by gathering and reporting information about government operations.

“(I)n a society in which each individual has but limited time and resources with which to observe at first hand the operations of his government, he relies necessarily upon the press to bring to him in convenient form the facts of those operations. Great responsibility is accordingly placed upon the news media to report fully and accurately the proceedings of government, and official records and documents open to the public are the basic data of governmental operations.”

Kallstrom v. City of Columbus, 165 F.Supp.2d 686, 697 (S.D. Ohio 2001), quoting *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 492, 95 S.Ct. 1029, 43 L.Ed.2d 328 (1975). “Thus, the Supreme Court has concluded, ‘an untrammelled press [is] a vital source of public information’, and an informed public the essence of working democracy.” (Citations omitted.) *Id.* at 698. The Public Records Act facilitates ready access to government information for public review. “One of the salutary purposes of the Public Records Law is to ensure accountability of government to those being governed.” *State ex rel. Strothers v. Wertheim*, 80 Ohio St.3d 155, 158, 684 N.E.2d 1239 (1997).

Request for Hospital Reporting Data

{¶4} On March 27, 2020, Eye on Ohio, Ohio Center for Investigative Journalism, made a public records request to respondent Ohio Department of Health (ODH) as follows:

This is a request on behalf of the Ohio Center for Investigative Journalism to inspect the following records:

1. The most recent communication from the Ohio Hospital Association to the Ohio Department of Health relaying data from the OHA Resource Tracker.
2. The most recent Surgenet data available, broken down by facility, on capacity and availability for:
 - A. Adult medical/surgical beds
 - B. Pediatric medical/surgical beds
 - C. Adult critical care beds

- D. Pediatric critical care beds
 - E. Adult airborne isolation beds
 - F. Pediatric airborne isolation beds
 - G. Ventilators
 - H. ECMO machines
3. The most recent Surgenet data, broken down by facility, on the availability of:
- A. N95 respirators
 - B. Face/surgical masks
 - C. Gloves
 - D. Face shields
 - E. Gowns
 - F. Physician staffing
 - G. Nurse staffing
 - H. Ancillary staffing
4. The Ohio Department of Health record-retention schedule.

(Complaint at 2-4.) On April 16, 2020, counsel for ODH responded:

Upon review of your records request dated March 27, 2020, the Ohio Department of Health has determined that the records you are seeking are “security records,” as that term is defined in R.C. 149.433(A). Because security records are not public records, pursuant to RC 149.433(B)(1), they also are not subject to the mandatory release and disclosure requirements found in R.C. 149.43(B)(1).

Given the sensitive nature of the records you have requested, the Department has decided to deny your records request.

(*Id.* at 5.) ODH does not dispute that it gathers, maintains, and can produce the requested records.²

² A requester is entitled to any electronically compiled record that a public office’s data software is programmed to produce (“Database Rule”). *State ex rel. Scanlon v. Deters*, 45 Ohio St.3d 376, 379, 544 N.E.2d 680 (1989); *Naymik v. Northeast Ohio Areawide Coordinating Agency*, Ct. of Cl. No. 2017-

{¶5} On April 29, 2020, Eye on Ohio filed a complaint pursuant to R.C. 2743.75 alleging denial of access to public records in violation of R.C. 149.43(B). Following unsuccessful mediation, ODH filed respondent's reply (Response) on July 6, 2020. On July 28, 2020, Eye on Ohio filed a reply. On October 6, 2020, ODH filed a sur-reply along with copies of a Surgenet user guide, training materials, and screen shots, restricted from public access.

Surgenet

{¶6} Surgenet was first developed by the Greater Dayton Area Health Information Network (GDAHIN). The software was subsequently enhanced to its present "all hazards" function as "a tool to be utilized during an emergency involving the public's health which could severely impact hospital services." (Sur-reply, Webber Aff. at ¶ 4.) "SurgeNet's function is to provide the current status of participating hospitals to respond to crisis events such as bioterrorism attack or pandemic." (*Id.* at ¶ 5.) "SurgeNet is being updated daily at the request of the Regional Healthcare Coordinators (RHC). The primarily [*sic*] purpose is to have a regional view of the current bed availability as well as to be prepared for any mass casualty event that may occur." (*Id.* at ¶ 7.)

Exception Claimed

{¶7} ODH does not dispute that the data outputs of Surgenet are, absent an applicable exception,³ public records kept by a public office. However, ODH claims that the requested Surgenet hospital data is exempt from disclosure as a "security record * * * assembled, prepared, or maintained by a public office * * * to prevent, mitigate, or respond to acts of terrorism." R.C. 149.433(A)(2).

{¶8} The burden to establish the applicability of this exception rests on ODH. *State ex rel. Cincinnati Enquirer v. Pike Cty. Coroner's Office*, 153 Ohio St.3d 63, 2017-

00919PQ, 2018-Ohio-1718, ¶ 31-33, and cases cited therein. Even if ODH were not currently accessing the precise data output requested (see Webber Aff. at ¶ 6), it is still considered to be an existing record.

³ A public records exception is a law prohibiting or excusing disclosure of records that would otherwise be public.

Ohio-8988, 101 N.E.3d 396, ¶ 15. Exceptions to disclosure are strictly construed against the public-records custodian. *State ex rel. Rogers v. Dept. of Rehab. & Corr.*, 155 Ohio St.3d 545, 2018-Ohio-5111, 122 N.E.3d 1208, ¶ 7. A custodian does not meet this burden if it has not proven that the requested records fall squarely within the exception. *State ex rel. Cincinnati Enquirer v. Jones-Kelley*, 118 Ohio St.3d 81, 2008-Ohio-1770, 886 N.E.2d 206, paragraph two of the syllabus. Any doubt should be resolved in favor of disclosure of public records. *State ex rel. James v. Ohio State Univ.*, 70 Ohio St.3d 168, 169, 637 N.E.2d 911 (1994).

Security Records

{¶9} The public records exception asserted by ODH is found in R.C. 149.433(A), which provides:⁴

(A) As used in this section: * * * “Security record” means any of the following:

* * *

(2) Any record assembled, prepared, or maintained by a public office or public body to prevent, mitigate, or respond to *acts of terrorism*, including any of the following:

(a) Those portions of records containing specific and unique vulnerability assessments or specific and unique response plans either of which is intended to prevent or mitigate acts of terrorism, and communication codes or deployment plans of law enforcement or emergency response personnel;

⁴ ODH includes the text of another subsection, once, in its pleadings. (Sur-reply at 2.) Even if this was intentional, ODH offers no argument or evidence that the requested hospital data was being “directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage.” R.C. 149.433(A)(1). Eye on Ohio did not request records disclosing the programming or security configuration of Surgenet. It did not request any password, source code, user guide, or other document that could compromise or provide direct access to the Surgenet system. ODH alleges that “[t]hese records are also used to identify vulnerabilities in the Ohio healthcare system that, if made widely known to the public, could be seized upon by terrorist organizations and others seeking to wreak havoc upon Ohio’s healthcare system in times of pandemic.” (Sur-reply at 2-3.) However, it provides no explanation or expert opinion as to *how* the March 27, 2020 data output could be reverse-engineered or otherwise used to “wreak havoc upon Ohio’s healthcare system.” *Rogers* at ¶ 16-21.

- (b) Specific intelligence information and specific investigative records shared by federal and international law enforcement agencies with state and local law enforcement and public safety agencies;
- (c) National security records classified under federal executive order and not subject to public disclosure under federal law that are shared by federal agencies, and other records related to national security briefings to assist state and local government with domestic preparedness for acts of terrorism.

* * *

(B)(1) A record kept by a public office that is a security record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

(Emphasis added.)

{¶10} As a threshold matter, ODH complains that Eye on Ohio is “focused on the specific records sought, while Respondent is looking at the system itself.” (Sur-reply at 2.) However, the Public Records Act is focused solely on records, and not on systems.⁵ ODH argues that “*the security record SurgeNet* is not a public record” (*Id.*), but provides no legal precedent for the notion that an entire computer system is a “record.” Computer systems are repositories of records. Computer software is a means of access to records, without itself meeting the definition of a “record.” *State ex rel. Recodat Co. v. Buchanan*, 46 Ohio St.3d 163, 165, 546 N.E.2d 203 (1989). An office may keep records *about* a computer system, such as user guides and training materials, but the Surgenet system itself is not a single record. ODH must prove that the actual “records” requested – hospital resource availability data used to respond to the Covid-19 pandemic – were maintained on that date to mitigate or respond to acts of terrorism.

Requested Hospital Data Was Not Related to Acts of Terrorism

{¶11} ODH admits that, at the time of the request, the Surgenet system was gathering and generating Eye on Ohio’s requested records in response to a pandemic.

⁵ “‘Public record’ means records kept by any public office, * * *.” R.C. 149.43(A)(1). See R.C. 149.011(G) for the definition of “records” as used in R.C. Chapter 149.

ODH seeks to invoke the terrorism exception only by asserting that Surgenet *could* be used *if* the state is faced with acts of terrorism in the future. Eye on Ohio counters that ODH is required to prove application of the terrorism exception to the data on the date it is requested, not how it might apply to future hospital data under different circumstances.

{¶12} To meet the burden of proof regarding alleged security records, ODH must offer more than its own conclusory labeling:

The department and other agencies of state government cannot simply label a criminal or safety record a “security record” and preclude it from release under the public-records law, without showing that it falls within the definition in R.C. 149.433.

State ex rel. Plunderbund Media, L.L.C. v. Born, 141 Ohio St.3d 422, 2014-Ohio-3679, 25 N.E.3d 988, ¶ 29. Even records produced by a designated security system or law enforcement security protection operation must individually meet the statutory definition. *State ex rel. Rogers v. Dept. of Rehab. & Corr.*, 155 Ohio St.3d 545, 2018-Ohio-5111, 122 N.E.3d 1208, ¶ 21 (video from a security camera system did not meet the definition); *State ex rel. Miller v. Pinkney*, 149 Ohio St.3d 662, 2017-Ohio-1335, 77 N.E.3d 915, ¶ 1-4 (dated, innocuous, and unfounded reports of threats against official were “not security records.” See Appendix.); *Shaffer v. Budish*, Ct. of Cl. No. 2017-00690PQ, 2018-Ohio-1539, ¶ 21-24 (video from jail’s internal security camera). “As we made clear in *Plunderbund*, every record claimed under the security-record exception to disclosure must be considered separately.” *Rogers* at ¶ 21. “And when a public office claims an exception based on risks that are not apparent within the records themselves, the office must provide more than conclusory statements in affidavits to support its claim. See *State ex rel. Besser v. Ohio State Univ.*, 89 Ohio St.3d 396, 400-401, 2000-Ohio-207, 732 N.E.2d 373 (2000).” *Rogers* at ¶ 15.

{¶13} The standard of proof is strictly applied against the public records custodian. *Rogers* at ¶ 7. Even where a document has previously qualified as a security

record, that status ceases if the threat to which it responded has abated. *State ex rel. Ohio Republican Party v. FitzGerald*, 145 Ohio St.3d 92, 2015-Ohio-5056, 47 N.E.3d 124, ¶¶ 6-8, 24; *Rogers* at ¶¶ 20-21; *Gannett GP Media, Inc. v. Ohio Dept. of Pub. Safety*, Ct. of Cl. No. 2017-00051PQ, 2017-Ohio-4247, ¶ 32. Proof that information is a security record is often provided through affidavits and expert testimony establishing that the records meet the statutory elements. In *Plunderbund*, respondent provided the detailed testimony of several law-enforcement and telecommunications experts connecting the disclosure of the requested information to future risks. *Plunderbund* at ¶¶ 22-31. The evidence offered by ODH falls short of this standard, more closely resembling the evidence found to be insufficient in *Rogers*:

First, the evidence it offers to support the applicability of the claimed exception pales in comparison to the evidence we considered in *Plunderbund*. Here, DRC has provided only two affidavits, one of which merely concludes that “it is [DRC] policy that security videos within correction institutions are not public records, and are therefore not disclosed in response to public records requests.” The Bobby affidavit contains more information regarding the applicability of the exception, yet even his testimony is general and insufficient to meet DRC’s burden in this case. Beyond these bare allegations, DRC has not attempted to explain how the video recording at issue * * * was “assembled, prepared, or maintained by a public office * * * to prevent, mitigate, or respond to acts of terrorism.” R.C. 149.433(A)(1) and (2).

Rogers at ¶ 19. The single affidavit submitted by ODH does not attempt to connect the March 27, 2020 hospital data requested by Eye on Ohio with prevention, mitigation, or response to any pending or anticipated act of terrorism.

{¶14} The additional, unsworn assertions in ODH’s pleadings also fail to establish the elements of the exception. First, ODH relates that

On March 26, 2020, ODH and local health partners received a verbal warning from Special Agent Bryan Seamour of the Federal Bureau of Investigation of credible threats from foreign terrorist organization [sic] directing followers to attack healthcare infrastructure within the United States.

(Sur-reply at 1.) A general warning that a terrorist organization is directing followers to attack unnamed healthcare infrastructure anywhere within the United States is not the type of specific, credible, current threat required to prove any exception based on risk. See *Gannett* at ¶¶ 28-33, *Narciso v. Powell Police Dept.*, Ct. of Cl. 2018-01195PQ, 2018-Ohio-4590, ¶¶ 35-38, *State ex rel. Quolke v. Strongsville City Sch. Dist. Bd. of Educ.*, 142 Ohio St.3d 509, 2015-Ohio-1083, 33 N.E.3d 30, ¶¶ 30. Nor, even were a specific terrorism threat identified with high confidence, does ODH explain how the snapshot of Surgenet hospital data existing on March 27, 2020 was assembled to prevent, mitigate or respond to that terrorist threat – the essential element of the exception asserted.

Second, ODH asserts a policy preference to not disclose the data:

The strength of SurgeNet depends entirely on how candid participating healthcare providers are when providing information. Webber Affidavit, Paragraph 5. Most of the information that could be in SurgeNet (inventories, bed availability, readiness) are not topics hospitals prefer to discuss in open forums. See, generally, Webber Affidavit, Exhibit A.

Even assuming, *arguendo*, that some hospitals would rather not disclose their bed and resource availability, it is well-settled that public offices may not withhold records merely because of a policy preference for confidentiality. *State ex rel. Consumer News Serv., Inc. v. Worthington City Bd. of Edn.*, 97 Ohio St.3d 58, 2002-Ohio-5311, 776 N.E.2d 82 at ¶¶ 46, 54. *Accord State ex rel. WBNS TV, Inc. v. Dues*, 101 Ohio St.3d 406, 2004-Ohio-1497, 805 N.E.2d 1116, ¶¶ 37; *Snyder-Hill v. Ohio State Univ.*, Ct. of Cl. No. 2020-00308PQ, 2020-Ohio-4957, ¶¶ 8-13.

“[I]n enumerating very narrow, specific exceptions to the public records statute, the General Assembly has already weighed and balanced the competing public policy considerations between the public’s right to know how its state agencies make decisions and the potential harm, inconvenience or burden imposed on the agency by disclosure.”

James v. OSU, 70 Ohio St.3d 168, 172, 637 N.E.2d 911 (1994). In the absence of proof that they meet the statutory definition, a public office’s mere policy of not disclosing certain documents is insufficient to show they are “security records.” *Rogers* at ¶¶ 19.

{¶15} Under the Public Records Act, it generally does not matter whether a record *could be* used by an office for some purpose, but only whether it *is* so used. *Narciso v. Powell Police Dept*, Ct. of Cl. 2018-01195PQ, 2018-Ohio-4590, ¶ 35-38, and cases cited therein (the bare assertion that records “could be used to target and victimize” persons was not supported by the evidence); *State ex rel. Beacon Journal Publ. Co. v. Whitmore*, 83 Ohio St.3d 61, 63, 697 N.E.2d 640 (1998) (an item is not a record just because the office “could have” used it). In the absence of expert testimony or other competent evidence that the requested data is being used in the context of acts of terrorism, the mere assertion of potential nefarious use is not sufficient to prove the data falls squarely within the security records exception. *Rogers* at ¶ 16-18. Although the Surgenet system could be used to mitigate or respond to acts of terrorism at some future time, and ODH may be able then to justify the security records exception, its daily hospital bed and resource records were not being so used on the date of this request.

{¶16} I conclude that ODH has failed to meet its burden to prove that on the date of the request the listed data fell squarely under the exception for records “assembled, prepared, or maintained * * * to prevent, mitigate, or respond to acts of terrorism.”

Conclusion

{¶17} Accordingly, I recommend the court order respondent to provide requester with copies of the requested records.⁶ I recommend the court order that requester is entitled to recover from respondent the amount of the filing fee of twenty-five dollars and any other costs associated with the action that it has incurred. I recommend costs be assessed to respondent.

{¶18} Pursuant to R.C. 2743.75(F)(2), *either party may file a written objection with the clerk of the Court of Claims of Ohio within seven (7) business days after receiving this report and recommendation. Any objection shall be specific and state with*

⁶ A requester is entitled to copies of electronic public records in any format that the public office’s equipment is programmed to export. See *Parks v. Webb*, Ct. of Cl. No. 2018-00995PQ, 2018-Ohio-1578, ¶ 10-17, and cases cited therein. See also R.C. 149.43(B)(6).

particularity all grounds for the objection. A party shall not assign as error on appeal the court's adoption of any factual findings or legal conclusions in this report and recommendation unless a timely objection was filed thereto. R.C. 2743.75(G)(1).

JEFF CLARK
Special Master

Filed October 20, 2020
Sent to S.C. Reporter 11/13/20