Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 351-2019

Dr. Rukevwe Ugwumba

July 21, 2021

Summary: The Commissioner received a concern about a possible breach of privacy from the Ministry of Health (Health) involving Dr. Rukevwe Ugwumba. Upon investigation, the Commissioner found that Dr. Ugwumba had no authority to collect the personal health information of some patients from September 3, 2016 to October 11, 2019. In addition, the Commissioner found that Dr. Ugwumba failed to adequately safeguard the personal health information that was in the doctor's custody and control. This includes having appropriate back-ups. The Commissioner recommended Dr. Ugwumba ensure that there is authority to collect personal health information before doing so. Further, that Dr. Ugwumba put appropriate safeguards in place to protect the personal health information that is in the doctor's custody and control. In addition, the Commissioner recommended the College of Physicians and Surgeons of Saskatchewan complete any investigation process that may be ongoing and proceed in accordance with its governing legislation. Also, the Commissioner recommended that Health and eHealth Saskatchewan provide notice of the breach to affected individuals by posting a notice on its website, media advisories and advertisements. Finally, the Commissioner recommended the Minister of Justice and Attorney General consider commencing a prosecution pursuant to subsections 64(1) and 64(1.1) of *The Health Information Protection Act*.

I BACKGROUND

[1] On October 8, 2019, the Ministry of Health (Health) contacted my office to proactively report a possible breach of privacy. Health advised that Dr. Rukevwe Ugwumba, a private practice physician and trustee under *The Health Information Protection Act* (HIPA), may have been inappropriately accessing, obtaining, and using beneficiaries' health services numbers and other personal health information through one or more of the health registration systems to facilitate billing Health's Medical Services Branch for physician

services inappropriately to the publicly funded system. The concern arose from a random audit by the Medical Services Branch. Health made eHealth Saskatchewan (eHealth) aware of the matter because the concern involved eHealth's health registration systems.

[2] On May 22, 2020, my office notified Dr. Ugwumba that it would be investigating the matter. In my office's notification, it requested the following:

- details regarding accesses to the Person Health Registration System (PHRS) Viewer for purposes other than providing care to patients between September 3, 2016 and October 11, 2019;
- details regarding all locations where Dr. Ugwumba was practicing between September 3, 2016 and October 11, 2019 and supporting documentation that showed Dr. Ugwumba saw patients in Saskatchewan since moving to Ontario during this timeframe;
- which section of *The Health Information Protection Act* (HIPA) was relied on for the collection, use and disclosure of personal health information obtained from PHRS Viewer;
- how Dr. Ugwumba took into consideration the 'data minimization' and the 'need-to-know' principles; and
- copies of relevant policies and/or procedures and/or agreements (or plans to develop relevant polices and/or procedures and/or agreements) or any other relevant documentation that supports Dr. Ugwumba's position.

[3] On July 9, 2020, my office received a privacy breach report from legal counsel representing Dr. Ugwumba.

II DISCUSSION OF THE ISSUES

1. Does *The Health Information Protection Act* apply and do I have jurisdiction to conduct this investigation?

[4] HIPA is only engaged if three elements exist: (1) there must be a trustee within the meaning of subsection 2(t) of HIPA; (2) there must also be personal health information within the

meaning of subsection 2(m) of HIPA; and (3) the personal health information must be in the custody or control of the trustee.

[5] To qualify as a trustee, one must be included in the definition at subsection 2(t) of HIPA. According to the privacy breach report provided by Dr. Ugwumba's legal counsel, Dr. Ugwumba is a family physician that operated in the Downtown Physicians Clinic as a solo practice. Subsection 2(t)(xii)(A) of HIPA provides:

> **2** In this Act:
> …
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
> …
> (xii) a person, other than an employee of a trustee, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible;

[6] According to the College of Physicians and Surgeons of Saskatchewan, Dr. Ugwumba received her medical license pursuant to *The Medical Profession Act, 1981*, in August 2003. She still held that license at the time of the matters in question.

[7] Therefore, Dr. Ugwumba is a "trustee" for purposes of HIPA by reason of subsection 2(t)(xii)(A) of HIPA. Therefore, the first element is met.

[8] *Custody* is physical possession with a measure of contorl. *Control* need only be considered if there is no custody by a trustee. At the material time when Dr. Ugwumba or her clinic entered eHealth's PHRS Viewer, Dr. Ugwumba collected and had custody of the personal health information at issue. Therefore, the second element is met.

[9] Subsection 2(m) of HIPA defines personal health information as follows:

> **2** In this Act:
> …
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:

> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> > (A) in the course of providing health services to the individual; or
> >
> > (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;

[10] For purposes of subsection 2(m)(v) of HIPA, "registration information" is defined at subsection 2(q) of HIPA as follows:

> **2** In this Act:
> …
> (q) **"registration information"** means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[11] The type of information contained within the PHRS Viewer and accessed by Dr. Ugwumba is as follows:

- patient's first and last name;
- patient's date of birth;
- patient's health services number; and
- patient's sex.

[12] This information would qualify as registration information and is therefore personal health information pursuant to subsection 2(m)(v) of HIPA. Therefore, the third element is met.

[13] As all three elements have been met, I find that HIPA is engaged on these matters and I have jurisdiction to conduct this investigation.

2. Were the requirements for a HIPA collection satisfied by Dr. Ugwumba?

[14] *Collection* is defined at subsection 2(b) of HIPA. It means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means.

[15] When Dr. Ugwumba (or Dr. Ugwumba's billing clerk) entered the PHRS Viewer as an approved user that was effectively a collection of personal health information by the trustee. Viewing personal health information on a screen, whether or not it is copied or recorded, is a collection within the meaning of HIPA (Investigation Report H-2010-001 at [85])

[16] Section 24 of HIPA provides:

> **24**(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[17] Health advised my office that its Medical Services Branch had concerns about Dr. Ugwumba's billing activity following a random audit. As part of investigating its concerns, it sent letters to patients. Many of the patients who had been contacted denied receiving services billed by Dr. Ugwumba and several indicated that they had never seen Dr. Ugwumba before as a patient. This is troubling.

[18] According to eHealth, Dr. Ugwumba was approved for access to the PHRS Viewer on February 24, 2015. The first time Dr. Ugwumba accessed the PHRS Viewer was on September 10, 2016. eHealth determined through an audit of the PHRS Viewer that the physician accessed the profiles of approximately 5,328 individuals between September 10, 2016 and September 10, 2019. It is unclear how many of these patients received services from Dr. Ugwumba or what the purpose was for these accesses.

[19] Upon learning of Health's investigation, eHealth disabled Dr. Ugwumba's access to all eHealth managed applications on September 19, 2019.

[20] The total dollar amount of inappropriate billings may be very large.

[21] My office asked Dr. Ugwumba for details and supporting documentation regarding accesses to the PHRS Viewer for purposes other than providing care to patients between September 3, 2016 and October 11, 2019.

[22] In the privacy breach report from Dr. Ugwumba's legal counsel, counsel indicated that "the clinic" accessed personal health information in the PHRS Viewer "for the purposes of updating demographic and billing information". Further, that in doing so, the "clinic erroneously accessed" the personal health information of individuals who were not patients of the clinic. Finally, counsel indicated Dr. Ugwumba did not have patient records from September 3, 2016 to October 11, 2019, to substantiate the collection of personal health information. The reason was an apparent malware and backup failure in the clinic's Accuro Electronic Medical Record system. Essentially, all patient records during this timeframe that could support Dr. Ugwumba's billings were allegedly lost and there were no back-ups made. To support this assertion, a copy of a report from Dr. Ugwumba's IT Administrator was provided to my office.

[23] However, as part of Dr. Ugwumba's privacy breach report, 14 pages of severed gynecological cytology reports were provided. The patient names, dates of births, health services numbers and registration numbers were all severed, so I cannot verify if these patients are among the ones who claim they did not receive services. In addition, I cannot

verify which patients Dr. Ugwumba "erroneously accessed" as nothing was provided to identify them. The gynecological cytology reports demonstrate, at best, that Dr. Ugwumba may have had some patients between March 2017 and July 2019.

[24] It appears Dr. Ugwumba cannot substantiate that the collection of personal health information from the PHRS Viewer was compliant with section 24 of HIPA. Supporting documentation could have been records showing Dr. Ugwumba was delivering health care services to the patients whom she looked up in the PHRS Viewer between September 2016 and October 2019. Trustees must have authority to collect personal health information. When a trustee cannot support their authority for collection, I must find that no authority exists.

[25] Therefore, I find that Dr. Ugwumba did not have authority to collect the personal health information of some patients between September 3, 2016 and October 11, 2019. The adequacy of safeguarding the personal health information is clearly an issue that must be addressed in this Report as Dr. Ugwumba appears to have lost control over the personal health information she collected as a result of an alleged malware and backup failure.

3. Did Dr. Ugwumba have policies and procedures in place as required by section 16 of HIPA?

[26] HIPA prescribes that the trustee must establish policies and procedures to maintain administrative, technical and physical safeguards. These safeguards must protect the integrity, accuracy and confidentiality of the information. They must also protect against any reasonably anticipated threat or hazard to the security or integrity of the information; and the loss of, unauthorized access to, use or disclosure of the information. Section 16 of HIPA provides:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;

> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
> (ii) loss of the information; or
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[27] If a trustee fails to achieve satisfactory compliance with HIPA requirements, there is a greatly increased risk that patient's personal health information will fail to be protected from exposure to others who would have no legitimate need-to-know that personal health information. There is also a heightened risk that patient confidence in their health providers will be undermined and that this will negatively impact health care outcomes. Such a lack of confidence could also compromise the effectiveness of the electronic health record system that has rolled out across the province.

[28] In the privacy breach report from Dr. Ugwumba's legal counsel, it indicated that the clinic's electronic medical records system failed on October 11, 2019, such that the clinic has no back-up records to verify which individuals' information was erroneously accessed.

[29] In addition, it appears that Dr. Ugwumba's log-in information was shared with the billing clerk who accessed the PHRS Viewer on occasion using Dr. Ugwumba's log-in information. The clerk should have had their own log-in so that it was clear who was accessing the PHRS Viewer and for what purpose. In order to maintain proper safeguards, authorized users must have their own log-in capabilities. I have addressed this in previous Reports including most recently Investigation Report 413-2019, 414-2019, 415-2019. Dr. Ugwumba has indicated to my office that she takes full responsibility for any errors of her staff and acknowledges the need for separate log-ins.

[30] My office inquired if Dr. Ugwumba had policies and procedures in place to safeguard the personal health information in her custody and control. My office was advised that Dr. Ugwumba had practices in place to protect personal information but they were not in writing. As well, that she had written agreements signed with staff and third parties

respecting confidentiality of personal health information but copies were lost when the back-up failure occurred. Legal counsel for Dr. Ugwumba provided my office with copies of policies and procedures and advised that Dr. Ugwumba implemented the policies and procedures in October 2019. Therefore, they were not in place during the timeframe in question (September 3, 2016 to October 11, 2019). This is unacceptable considering HIPA came into force September 1, 2003.

[31] Based on what has been provided to my office, it is apparent that Dr. Ugwumba did not maintain administrative, technical and physical safeguards to protect the personal health information in her custody and control.

[32] Given the egregious nature of this breach and Dr. Ugwumba's failure to safeguard the personal health information of patients, the offence provision under HIPA is an appropriate provision to consider in this case. Subsections 64(1)(a), (1.1), (1.2) and (2) of HIPA provide:

> **64**(1) No person shall:
>
> (a) knowingly contravene any provision of this Act or the regulations;
>
> …
>
> (1.1) No trustee or information management service provider, or former trustee or information management service provider, shall fail to keep secure the personal health information in its custody or control as required bv this Act.
>
> (1.2) No person shall be found to have contravened subsection (1.1) if that person can establish that he or she took all reasonable steps to prevent the contravention.
>
> (2) Every person who contravenes subsection (1) or (1.1) is guilty of an offence and is liable on summary conviction:
>
> (a) in the case of an individual, to a fine of not more than $50,000, to imprisonment for not more than one year or to both; and
>
> (b) in the case of a corporation, to a fine of not more than $500,000.

[33] It is my office's understanding that the College of Physicians and Surgeons of Saskatchewan and the Regina Police Service are also investigating the matter involving Dr. Ugwumba's conduct.

III FINDINGS

[34] I find that Dr. Ugwumba had no authority to collect the personal health information of some patients from September 3, 2016 to October 11, 2019.

[35] I find that Dr. Ugwumba failed to adequately safeguard the personal health information in her custody and control.

IV RECOMMENDATIONS

[36] I recommend that, if continuing to practice, Dr. Ugwumba should ensure that there is authority to collect personal health information before doing so.

[37] I recommend that if Dr. Ugwumba continues to practice, Dr. Ugwumba put appropriate safeguards in place to protect the personal health information in her custody and control. This includes having appropriate back-ups.

[38] I recommend the College of Physicians and Surgeons of Saskatchewan complete any investigation process that may be ongoing and proceed in accordance with its governing legislation.

[39] I recommend that the Minister of Justice and Attorney General consider commencing a prosecution pursuant to subsections 64(1) and (1.1) of HIPA in respect to multiple breaches documented in this Report.

[40] I recommend that Health and eHealth provide notice of the breach to affected individuals by posting a notice on its website, media advisories and advertisements.

Dated at Regina, in the Province of Saskatchewan, this 21st day of July, 2021.

Ronald J. Kruzeniski, Q.C.
Office of the Saskatchewan Information and Privacy Commissioner