OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS

Kwame Raoul
ATTORNEY GENERAL

December 29, 2021

RE: Social Security Number Protection Task Force Member/Designated Recipient

Dear Designated Task Force Recipient,

In accordance with 20 ILCS 4040/10, attached for your review and records is a copy of the Social Security Number Protection Task Force Report for 2021.

Thank you.

Best Regards,

Matthew W. Van Hise

Matthew W. Van Hise, CIPP/US
Chief Privacy Officer
Task Force Chair
Assistant Attorney General
Illinois Attorney General's Office

Enclosure: 2021 Task Force Report.

Social Security Number Protection Task Force

Report to Governor J.B. Pritzker, Attorney General Kwame Raoul,
Secretary of State Jesse White, and Illinois General Assembly
December 29, 2021

CONTENTS

TASK FORCE BACKGROUND

The Social Security Number (SSN) remains the key piece of sensitive personally identifiable information that identity thieves use to commit fraud. The SSN was intended to be used solely to distribute Social Security benefits, but in the years since its inception in 1935, it has been also used as a unique identification number. The SSN is therefore not only tied to an individual's credit report, financial records, and Social Security earnings with the federal government, but is also present in employment, educational, health, insurance, and criminal records. The wide dissemination of SSNs increases the likelihood that the numbers can be accessed and subsequently used for fraudulent purposes.

Consumers are therefore encouraged to limit their exposure to identity theft by protecting their SSNs. Businesses are also encouraged to do their part by taking necessary steps to limit the collection of SSNs, protect SSNs in their possession, and dispose of documents containing SSNs in a manner that renders them unusable. Local and state government agencies also have a role in protecting SSNs they maintain and reducing their continued widespread dissemination. Government agencies have the larger task of maintaining a system of open records for the public, while taking measures to reduce the amount of sensitive personally identifiable information in those records.

The General Assembly created the Social Security Number Protection Task Force (Task Force) through Public Act 93-0813 in 2004. The Task Force is charged with examining the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN when the State requires the individual to provide that number to an officer or agency of the State. The Task Force also is required to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs by State and local governments for identification and record-keeping purposes. In 2007, the General Assembly amended the law governing the Task Force by Public Act 95-0482. The Office of the Attorney General is charged with chairing and administering the activities of the Task Force.

MEMBERSHIP OF THE TASK FORCE –

- Two members representing the House of Representatives, appointed by the Speaker of the House – ***Awaiting Additional Member Appointment Confirmation*****, Representative Ann Williams**
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – **Representative Dan Ugaste, Representative Randy Frese**
- Two members representing the Senate, appointed by the President of the Senate – **Senator Jacqueline Collins,** ***Awaiting Additional Member Appointment Confirmation***
- Two members representing the Senate, appointed by the Minority Leader of the Senate **-** ***Awaiting Additional Member Appointment Confirmation*****,** ***Awaiting Additional Member Appointment Confirmation***
- One member representing the Office of the Attorney General – **Matthew W. Van Hise, Task Force Chair**
- One member representing the Office of the Secretary of State – **Micah Miller**

- One member representing the Office of the Governor – ***Awaiting Member Appointment Confirmation***
- One member representing the Department of Natural Resources – **John "J.J." Pohlman**
- One member representing the Department of Healthcare and Family Services – **Elizabeth Festa**
- One member representing the Department of Revenue – **Angela Hamilton**
- One member representing the Department of State Police – **Captain Felix Canizares**
- One member representing the Department of Employment Security – **Joseph Mueller**
- One member representing the Illinois Courts – **James Morphew**
- One member representing the Department on Aging – **Jessica Klaus**
- One member representing Central Management Services – **Jake Altman**
- One member appointed by the Executive Director of the Board of Higher Education – **Dr. Eric Lichtenberger**
- One member appointed by the Secretary of Human Services – **Katelyn Nassin**
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- One member representing the Office of the State Comptroller – **Ben Haley**
- One member representing school administrators, appointed by the State Superintendent of Education – **Sara Boucek**

PART I: PROTECTION OF SSNS IN THE PUBLIC RECORD

The first statutory requirement of the Social Security Number Protection Task Force Act is to examine the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN.

IDENTITY PROTECTION ACT

One way to limit the unauthorized disclosure of SSNs is to limit their collection in the first place. If fewer entities collect and use SSNs, fewer entities are capable of disclosing those numbers improperly.

The Identity Protection Act, 5 ILCS 179/1 *et seq.*, prohibits certain collections, uses and disclosures of an individual's SSN by any person, or State or local government agencies. Specifically, the Act, with several exceptions, prohibits a person, or State or local government agency from collecting, using, or disclosing a SSN unless: (1) required to do so under state or federal law or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the agency's duties and responsibilities; (2) the need and purpose for the SSN is documented before the request; and (3) the SSN collected is relevant to the documented need and purpose. The need and purpose for the collection and use of SSNs must be documented in a written Identity-Protection Policy.

Each local government agency must file a written copy of its policy with the governing board of the unit of local government within 30 days after approval of the policy. Under Section 37(b), "each State agency must provide a copy of its identity-protection policy to the Social Security

Number Protection Task Force within 30 days after the approval of the policy." State agencies were reminded of this requirement on August 24, 2011. Policies can be submitted to the Task Force by mailing a copy to:

Illinois Attorney General
Social Security Number Protection Task Force
c/o: Chief Privacy Officer Matthew W. Van Hise
500 S. Second Street
Springfield, IL 62701

As part of the implementation of the policies, local and state agencies will require that all employees identified as having access to SSNs in the course of performing their duties be trained to protect the confidentiality of SSNs. Training should include instructions on the proper handling of information that contains SSNs from the time of the collection of the information through its destruction.

Identity-Protection Policies were to have been implemented within 12 months of the date of approval and a copy was to have been sent to the Task Force no later than June 1, 2012. For reference, an Identity-Protection Policy and Statement of Purpose(s) template can be found in Appendixes A and B.

Updated and/or amended Identity-Protection Policies may be sent electronically to SSNPolicy@ilag.gov. Submissions shall occur as soon as practicable or within the calendar year in which the updated amendment was implemented. An acknowledgement of receipt and record will be provided by a duly authorized representative of the Task Force chairperson.

(Template Identity-Protection Policy – Appendix A)
(Template Statement of Purpose(s) – Appendix B)

NEW DEVELOPMENTS IN LAWS AND REGULATIONS TO PROTECT SOCIAL SECURITY NUMBERS:

The State of Illinois is continually updating and modifying its laws and regulations to meet the continual and emerging threats to the Protection of Personal Identifiable Information; specifically safeguarding Social Security Numbers.

The Student Online Personal Protection Act (SOPPA) (105 ILCS 85) became law on August 24, 2017, as a response to data breaches involving schools and student data to ensure that school districts protect student data when collected by educational technology companies and that the data's use is for beneficial purposes only.

Starting on July 1, 2021, SOPPA amendments now require school districts to provide additional safeguards of student data. School districts are now required to: (1) enter into written agreements with operators to ensure student data remains confidential; and (2) and take steps to minimize data breaches and their potential impact. Some of the specific written agreement requirements include:

- A list of the categories or types of covered information provided to the operator.
- A statement of the product or service provided to the school by the operator.
- A statement that the operator must delete or transfer to the school all covered information if the information is no longer needed for the purpose of the written agreement and to specify the time period in which the information must be deleted or transferred once the operator is made aware that the information is no longer needed for the purposes of the written agreement.

Section 105 ILCS 85/15(1) now requires operators to implement and maintain reasonable security and practices *that otherwise meet or exceed industry standards* designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure. This new requirement to meet or exceed industry standards replaces the language *appropriate to the nature of the covered information* and provides a bit more guidance to schools, school districts and operators.

The Identity Protection Act (IPA) (5 ILCS 179) became effective June 1, 2010 to protect the privacy and rights of the individual in regards to Social Security Numbers and to properly train employees to protect the information. The IPA requires each local and state government to have an identity protection policy to ensure the confidentiality and integrity of Social Security Numbers. The Act requires local and state government agencies to reassess their personal information (PI) data practices and take whatever steps necessary to protect such information.

Consistent with the IPA, Illinois law was updated, effective June 25, 2021, by adding section 20 ILCS 1005/1005-55 which specifically prohibits the Department of Employment Security from disclosing an individual's entire social security number by physical mail, unless otherwise required by State or federal law. The Department of Employment Security is also required to develop and implement a process to replace the use of an individual's Social Security Number with other identifying information to use for mail correspondence. This amendment will help strike a balance between the need to identify applicants and recipients and the need to protect their identity.

The continued updating of laws and regulations is necessary to combat identity fraud and theft, and safeguard personal information, while also ensuring users access to personal information when necessary and appropriate.

(P.A. 101-516; P.A. 102-26 – Appendix C)

PART II: SSNS AS INTERNAL IDENTIFIERS

The second requirement of the Task Force is to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs for identification and record-keeping purposes by State and local governments. State and local government agencies continue to internally assess the collection and use of SSNs. Such an assessment was critical in drafting Identity-Protection Policies.

MINIMIZING THE USE OF SOCIAL SECURITY NUMBERS

Social security numbers have become both an identifier and an authenticator. Partly due to the proliferation of data breaches exposing consumer SSNs, minimizing use of SSNs has become increasingly important. Certain industries, including healthcare, require the collection of SSNs to perform essential services and have a high burden of responsibility to keep patients' sensitive personal information safe under the Illinois Consumer Protection Acts, the Illinois Personal Information Protection Acts, as well as the federal HIPAA Privacy and Security Rule. For industries where the collection of SSNs is essential, enforcement actions must certify that proper precautions are implemented to safeguard the personal information as well as ensure any unauthorized access to sensitive personal information is discovered quickly, remediated, and followed by prompt and concise consumer notification if necessary. When the collection and retention of SSNs is necessary, limiting or minimizing access to this information can reduce the risk to consumers.

On October 8, 2020, Illinois and a bipartisan coalition of 28 states was part of a $5 million dollar settlement with Community Health Systems Inc. (CHS), an operator of acute care hospitals and outpatient care centers. With more than 339,000 impacted Illinois residents, the Illinois Attorney General secured $611,000 as well as a detailed settlement to implement a comprehensive information security program.

In 2014, CHS's computer network was the target of an external cyber-attack that allowed hackers to gain access to personal information, including patient SSNs. As part of the settlement, CHS has agreed to not only implement and maintain a comprehensive information security program to safeguard personal information, but additionally must implement policies to quickly address a security incident such as a breach of personal information.

For CHS to comply with the settlement, CHS is required to conduct an annual risk assessment of the CHS network and develop a plan to address any risks discovered, utilize multi-factor authentication to limit access to the network to only authorized individuals, develop and maintain policies and procedures to encrypt sensitive data, and provide regular security and privacy training for employees who come into contact with sensitive patient data. Additionally, CHS must require third parties that provide services to CHS that involve sensitive data to take appropriate precautions to protect the data.

(*Attorney General Raoul Announces $5 Million Settlement with Community Health Systems for Data Breach* – Appendix D)

TASK FORCE APPOINTMENTS & UPDATES

The Task Force awaits calendar year 2021 Appointment and Confirmations for the following currently vacant membership seats:

- (1) Member representing the House of Representatives, Appointed by the Speaker of the House;
- (1) Member representing the Senate, Appointed by the President of the Senate;
- (2) Members representing the Senate, Appointed by the Minority Leader of the Senate; and
- (1) Member representing the Office of the Governor;

CONCLUSION

Identity-Protection Policies at local and state government agencies throughout Illinois continue to be implemented according to the requirements of the Identity Protection Act. Over the course of the last year the Task Force has continued to monitor state-level discussions regarding further contemplated protections for Illinois individuals' Social Security numbers, and has also monitored federal bills involving the protections and restrictions associated with using Social Security numbers as individual identifiers. The Task Force will continue to monitor state and federal activities, recommending updates as needed and will continue to work together with all stakeholders to identify the best ways to protect SSNs in public records and limit the use of SSNs as internal identifiers.

APPENDIX A – Template Identity-Protection Policy

[AGENCY]
IDENTITY-PROTECTION POLICY

The [AGENCY] adopts this Identity-Protection Policy pursuant to the Identity Protection Act. 5 ILCS 179/1 *et seq*. The Identity Protection Act requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy to ensure the confidentiality and integrity of Social Security numbers agencies collect, maintain, and use. It is important to safeguard Social Security numbers (SSNs) against unauthorized access because SSNs can be used to facilitate identity theft. One way to better protect SSNs is to limit the widespread dissemination of those numbers. The Identity Protection Act was passed in part to require local and State government agencies to assess their personal information collection practices, and make necessary changes to those practices to ensure confidentiality.

Social Security Number Protections Pursuant to Law

Whenever an individual is asked to provide this Office with a SSN, [AGENCY] shall provide that individual with a statement of the purpose or purposes for which the [AGENCY] is collecting and using the Social Security number. The [AGENCY] shall also provide the statement of purpose upon request. That Statement of Purpose is attached to this Policy.

The [AGENCY] shall not:

1) Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the general public.
2) Print an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity.
3) Require an individual to transmit a Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.
4) Print an individual's Social Security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the Social Security number to be on the document to be mailed. SSNs may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the Social Security number. A Social Security number that is permissibly mailed will not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

In addition, the [AGENCY] shall not[1]:

[1] These prohibitions do not apply in the following circumstances:

(1) The disclosure of Social Security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees,

1) Collect, use, or disclose a Social Security number from an individual, unless:
    i. required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the [AGENCY]'s duties and responsibilities;
    ii. the need and purpose for the Social Security number is documented before collection of the Social Security number; and
    iii. the Social Security number collected is relevant to the documented need and purpose.
2) Require an individual to use his or her Social Security number to access an Internet website.
3) Use the Social Security number for any purpose other than the purpose for which it was collected.

Requirement to Redact Social Security Numbers
The [AGENCY] shall comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's Social Security number. The [AGENCY] shall redact social security numbers from the information or documents before allowing the public inspection or copying of the information or documents.

When collecting Social Security numbers, the [AGENCY] shall request each SSN in a manner that makes the SSN easily redacted if required to be released as part of a public records request. "Redact" means to alter or truncate data so that no more than five sequential digits of a Social Security number are accessible as part of personal information.

Employee Access to Social Security Numbers
Only employees who are required to use or handle information or documents that contain SSNs will have access. All employees who have access to SSNs are trained to protect the confidentiality of SSNs.

---

contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's Social Security number will be achieved.

(2) The disclosure of Social Security numbers pursuant to a court order, warrant, or subpoena.

(3) The collection, use, or disclosure of Social Security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.

(4) The collection, use, or disclosure of Social Security numbers for internal verification or administrative purposes.

(5) The disclosure of Social Security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.

(6) The collection or use of Social Security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

APPENDIX B – Template Statement of Purpose(s)

What does the [AGENCY] do with your Social Security Number?
Statement of Purpose for Collection of Social Security Numbers
Identity-Protection Policy

The Identity Protection Act, 5 ILCS 179/1 *et seq*., requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy that includes a statement of the purpose or purposes for which the agency is collecting and using an individual's Social Security number (SSN). This statement of purpose is being provided to you because you have been asked by the [AGENCY] to provide your SSN or because you requested a copy of this statement.

Why do we collect your Social Security number?

You are being asked for your SSN for one or more of the following reasons:
[THE FOLLOWING PURPOSES MAY NOT APPLY; IDENTIFY PURPOSES APPROPRIATE FOR YOUR AGENCY]

- Complaint mediation or investigation;
- Crime victim compensation;
- Vendor services, such as executing contracts and/or billing;
- Law enforcement investigation;
- Child support collection;
- Internal verification;
- Administrative services; and/or
- Other:_____

What do we do with your Social Security number?

- We will only use your SSN for the purpose for which it was collected.
- We will not:
    - Sell, lease, loan, trade, or rent your SSN to a third party for any purpose;
    - Publicly post or publicly display your SSN;
    - Print your SSN on any card required for you to access our services;
    - Require you to transmit your SSN over the Internet, unless the connection is secure or your SSN is encrypted; or
    - Print your SSN on any materials that are mailed to you, unless State or Federal law requires that number to be on documents mailed to you, or unless we are confirming the accuracy of your SSN.

Questions or Complaints about this Statement of Purpose

Write to the [AGENCY]:
[CONTACT INFORMATION]

APPENDIX C— Section 5 of Public Law No: 101-0516

SEC. 5. STUDENT ONLINE PERSONAL PROTECTION ACT- The Student Online Personal Protection Act is amended by changing Sections 5, 10, and 30 and by adding Sections 26, 27, 28, and 33 as follows:

(105 ILCS 85/5)

Sec. 5. Definitions. In this Act:

"Breach" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of covered information maintained by an operator or school. "Breach" does not include the good faith acquisition of personal information by an employee or agent of an operator or school for a legitimate purpose of the operator or school if the covered information is not used for a purpose prohibited by this Act or subject to further unauthorized disclosure.

"Covered information" means personally identifiable information or material or information that is linked to personally identifiable information or material in any media or format that is not publicly available and is any of the following:

(1) Created by or provided to an operator by a student or the student's parent ~~or legal guardian~~ in the course of the student's or~~,~~ parent's, ~~or legal guardian's~~ use of the operator's site, service, or application for K through 12 school purposes.

(2) Created by or provided to an operator by an employee or agent of a school or school district for K through 12 school purposes.

(3) Gathered by an operator through the operation of its site, service, or application for K through 12 school purposes and personally identifies a student, including, but not limited to, information in the student's educational record or electronic mail, first and last name, home address, telephone number, electronic mail address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, a social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

"Interactive computer service" has the meaning ascribed to that term in Section 230 of the federal Communications Decency Act of 1996 (47 U.S.C. 230).

"K through 12 school purposes" means purposes that are directed by or that customarily take place at the direction of a school, teacher, or school district; aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or are otherwise for the use and benefit of the school.

"Longitudinal data system" has the meaning given to that term under the P-20 Longitudinal Education Data System Act.

"Operator" means, to the extent that an entity is operating in this capacity, the operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K through 12 school purposes and was designed and marketed for K through 12 school purposes.

"Parent" has the meaning given to that term under the Illinois School Student Records Act.

"School" means (1) any preschool, public kindergarten, elementary or secondary educational institution, vocational school, special educational facility, or any other elementary or secondary educational agency or institution or (2) any person, agency, or institution that maintains school student records from more than one school. Except as otherwise provided in this Act, "school" ~~"School"~~ includes a private or nonpublic school.

"State Board" means the State Board of Education.

"Student" has the meaning given to that term under the Illinois School Student Records Act.

"Targeted advertising" means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred ~~over time~~ from that student's online behavior, usage of applications, or covered information. The term does not include advertising to a student at an online location based upon that student's current visit to that location or in response to that student's request for information or feedback, without the retention of that student's online activities or requests over time for the purpose of targeting subsequent ads.

(Source: P.A. 100-315, eff. 8-24-17; 101-516, eff. 7-1-21.)

(105 ILCS 85/10)

Sec. 10. Operator prohibitions. An operator shall not knowingly do any of the following:

(1) Engage in targeted advertising on the operator's site, service, or application or target advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application for K through 12 school purposes.

(2) Use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a student, except in furtherance of K through 12 school purposes. "Amass a profile" does not include the collection and retention of account information that remains under the control of the student, the student's parent ~~or legal guardian~~, or the school.

(3) Sell or rent a student's information, including covered information. This subdivision (3) does not apply to the purchase, merger, or other type of acquisition of an operator by another entity if the operator or successor entity complies with this Act regarding previously acquired student information.

(4) Except as otherwise provided in Section 20 of this Act, disclose covered information, unless the disclosure is made for the following purposes:

(A) In furtherance of the K through 12 school purposes of the site, service, or application if the recipient of the covered information disclosed under this clause (A) does not further disclose the information, unless done to allow or improve operability and functionality of the operator's site, service, or application.

(B) To ensure legal and regulatory compliance or take precautions against liability.

(C) To respond to the judicial process.

(D) To protect the safety or integrity of users of the site or others or the security of the site, service, or application.

(E) For a school, educational, or employment purpose requested by the student or the student's parent ~~or legal guardian~~, provided that the information is not used or further disclosed for any other purpose.

(F) To a third party if the operator contractually prohibits the third party from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibits the third party from disclosing any covered information provided by the operator with subsequent third parties, and requires the third party to implement and maintain ~~reasonable~~ security procedures and practices as required under Section 15.

Nothing in this Section prohibits the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application.

(Source: P.A. 100-315, eff. 8-24-17; 101-516, eff. 7-1-21.)

(105 ILCS 85/15)

Sec. 15. Operator duties. An operator shall do the following:

(1) Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards ~~appropriate to the nature of the covered information and~~ designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(2) Delete, within a reasonable time period, a student's covered information if the school or school district requests deletion of covered information under the control of the school or school district, unless a student or his or her parent ~~or legal guardian~~ consents to the maintenance of the covered information.

(3) Publicly disclose material information about its collection, use, and disclosure of covered information, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

(4) Except for a nonpublic school, for any operator who seeks to receive from a school, school district, or the State Board in any manner any covered information, enter into a written agreement with the school, school district, or State Board before the covered information may be transferred. The written agreement may be created in electronic form and signed with an electronic or digital signature or may be a click wrap agreement that is used with software licenses, downloaded or online applications and transactions for educational technologies, or other technologies in which a user must agree to terms and conditions before using the product or service. Any written agreement entered into, amended, or renewed must contain all of the following:

(A) A listing of the categories or types of covered information to be provided to the operator.

(B) A statement of the product or service being provided to the school by the operator.

(C) A statement that, pursuant to the federal Family Educational Rights and Privacy Act of 1974, the operator is acting as a school official with a legitimate educational interest, is performing an institutional service or function for which the school would otherwise use employees, under the direct control of the school, with respect to the use and maintenance of covered information, and is using the covered information only for an authorized purpose and may not re-disclose it to third parties or affiliates, unless otherwise permitted under this Act, without permission from the school or pursuant to court order.

(D) A description of how, if a breach is attributed to the operator, any costs and expenses incurred by the school in investigating and remediating the breach will be allocated between the operator and the school. The costs and expenses may include, but are not limited to:

(i) providing notification to the parents of those students whose covered information was compromised and to regulatory agencies or other entities as required by law or contract;

(ii) providing credit monitoring to those students whose covered information was exposed in a manner during the breach that a reasonable person would believe that it could impact his or her credit or financial security;

(iii) legal fees, audit costs, fines, and any other fees or damages imposed against the school as a result of the security breach; and

(iv) providing any other notifications or fulfilling any other requirements adopted by the State Board or of any other State or federal laws.

(E) A statement that the operator must delete or transfer to the school all covered information if the information is no longer needed for the purposes of the written agreement and to specify the time period in which the

information must be deleted or transferred once the operator is made aware that the information is no longer needed for the purposes of the written agreement.

(F) If the school maintains a website, a statement that the school must publish the written agreement on the school's website. If the school does not maintain a website, a statement that the school must make the written agreement available for inspection by the general public at its administrative office. If mutually agreed upon by the school and the operator, provisions of the written agreement, other than those under subparagraphs (A), (B), and (C), may be redacted in the copy of the written agreement published on the school's website or made available at its administrative office.

(5) In case of any breach, within the most expedient time possible and without unreasonable delay, but no later than 30 calendar days after the determination that a breach has occurred, notify the school of any breach of the students' covered information.

(6) Except for a nonpublic school, provide to the school a list of any third parties or affiliates to whom the operator is currently disclosing covered information or has disclosed covered information. This list must, at a minimum, be updated and provided to the school by the beginning of each State fiscal year and at the beginning of each calendar year.

(Source: P.A. 100-315, eff. 8-24-17; 101-516, eff. 7-1-21.)

(105 ILCS 85/26 new)

Sec. 26. School prohibitions. A school may not do either of the following:

(1) Sell, rent, lease, or trade covered information.

(2) Share, transfer, disclose, or provide access to a student's covered information to an entity or individual, other than the student's parent, school personnel, appointed or elected school board members or local school council members, or the State Board, without a written agreement, unless the disclosure or transfer is:

(A) to the extent permitted by State or federal law, to law enforcement officials to protect the safety of users or others or the security or integrity of the operator's service;

(B) required by court order or State or federal law; or

(C) to ensure legal or regulatory compliance.

This paragraph (2) does not apply to nonpublic schools.

(Source: P.A. 101-516, eff. 7-1-21.)

(105 ILCS 85/27 new)

Sec. 27. School duties.

(a) Each school shall post and maintain on its website or, if the school does not maintain a website, make available for inspection by the general public at its administrative office all of the following information:

(1) An explanation, that is clear and understandable by a layperson, of the data elements of covered information that the school collects, maintains, or discloses to any person, entity, third party, or governmental agency. The information must explain how the school uses, to whom or what entities it discloses, and for what purpose it discloses the covered information.

(2) A list of operators that the school has written agreements with, a copy of each written agreement, and a business address for each operator. A copy of a written agreement posted or made available by a school under this paragraph may contain redactions, as provided under subparagraph (F) of paragraph (4) of Section 15.

(3) For each operator, a list of any subcontractors to whom covered information may be disclosed or a link to a page on the operator's website that clearly lists that information, as provided by the operator to the school under paragraph (6) of Section 15.

(4) A written description of the procedures that a parent may use to carry out the rights enumerated under Section 33.

(5) A list of any breaches of covered information maintained by the school or breaches under Section 15 that includes, but is not limited to, all of the following information:

(A) The number of students whose covered information is involved in the breach, unless disclosing that number would violate the provisions of the Personal Information Protection Act.

(B) The date, estimated date, or estimated date range of the breach.

(C) For a breach under Section 15, the name of the operator.

The school may omit from the list required under this paragraph (5): (i) any breach in which, to the best of the school's knowledge at the time of updating the list, the number of students whose covered information is involved in the breach is less than 10% of the school's enrollment, (ii) any breach in which, at the time of posting the list, the school is not required to notify the parent of a student under subsection (d), (iii) any breach in which the date, estimated date, or estimated date range in which it occurred is earlier than July 1, 2021, or (iv) any breach previously posted on a list under this paragraph (5) no more than 5 years prior to the school updating the current list.

The school must, at a minimum, update the items under paragraphs (1), (3), (4), and (5) no later than 30 calendar days following the start of a fiscal year and no later than 30 days following the beginning of a calendar year.

(b) Each school must adopt a policy for designating which school employees are authorized to enter into written agreements with operators. This subsection may not be construed to limit individual school employees outside of the scope of their employment from entering into agreements with operators on their own behalf and for non-K through 12 school purposes, provided that no covered information is provided to the operators. Any agreement or contract entered into in violation of this Act is void and unenforceable as against public policy.

(c) A school must post on its website or, if the school does not maintain a website, make available at its administrative office for inspection by the general public each written agreement entered into under this Act, along with any information required under subsection (a), no later than 10 business days after entering into the agreement.

(d) After receipt of notice of a breach under Section 15 or determination of a breach of covered information maintained by the school, a school shall notify, no later than 30 calendar days after receipt of the notice or determination that a breach has occurred, the parent of any student whose covered information is involved in the breach. The notification must include, but is not limited to, all of the following:

(1) The date, estimated date, or estimated date range of the breach.

(2) A description of the covered information that was compromised or reasonably believed to have been compromised in the breach.

(3) Information that the parent may use to contact the operator and school to inquire about the breach.

(4) The toll-free numbers, addresses, and websites for consumer reporting agencies.

(5) The toll-free number, address, and website for the Federal Trade Commission.

(6) A statement that the parent may obtain information from the Federal Trade Commission and consumer reporting agencies about fraud alerts and security freezes.

A notice of breach required under this subsection may be delayed if an appropriate law enforcement agency determines that the notification will interfere with a criminal investigation and provides the school with a written request for a delay of notice. A school must comply with the notification requirements as soon as the notification will no longer interfere with the investigation.

(e) Each school must implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure. Any written agreement under which the disclosure of covered information between the school and a third party takes place must include a provision requiring the entity to whom the covered information is disclosed to implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure. The State Board must make available on its website a guidance document for schools pertaining to reasonable security procedures and practices under this subsection.

(f) Each school may designate an appropriate staff person as a privacy officer, who may also be an official records custodian as designated under the Illinois School Student Records Act, to carry out the duties and responsibilities assigned to schools and to ensure compliance with the requirements of this Section and Section 26.

(g) A school shall make a request, pursuant to paragraph (2) of Section 15, to an operator to delete covered information on behalf of a student's parent if the parent requests from the school that the student's covered information held by the operator be deleted, so long as the deletion of the covered information is not in violation of State or federal records laws.

(h) This Section does not apply to nonpublic schools.

(Source: P.A. 101-516, eff. 7-1-21; 102-558, eff. 8-20-21.)

(105 ILCS 85/28 new)

Sec. 28. State Board duties.

(a) The State Board may not sell, rent, lease, or trade covered information.

(b) Except for an employee of the State Board or a State Board official acting within his or her official capacity, the State Board may not share, transfer, disclose, or provide covered information to an entity or individual without a contract or written agreement, except for disclosures required by State or federal law.

(c) At least once annually, the State Board must publish and maintain on its website a list of all of the entities or individuals, including, but not limited to, operators, individual researchers, research organizations, institutions of higher education, or government agencies, that the State Board contracts with or has written agreements with and that hold covered

information and a copy of each contract or written agreement. The list must include all of the following information:

(1) The name of the entity or individual. In naming an individual, the list must include the entity that sponsors the individual or with which the individual is affiliated, if any. If the individual is conducting research at an institution of higher education, the list may include the name of that institution and a contact person in the department that is associated with the research in lieu of the name of the researcher. If the entity is an operator, the list must include its business address.

(2) The purpose and scope of the contract or agreement.

(3) The duration of the contract or agreement.

(4) The types of covered information that the entity or individual holds under the contract or agreement.

(5) The use of the covered information under the contract or agreement.

(6) The length of time for which the entity or individual may hold the covered information.

(7) A list of any subcontractors to whom covered information may be disclosed under Section 15 or a link to a page on the operator's website that clearly lists that information.

If mutually agreed upon by the State Board and the operator, provisions of a contract or written agreement, other than those pertaining to paragraphs (1) through (7), may be redacted on the State Board's website.

(d) The State Board shall create, publish, and make publicly available an inventory, along with a dictionary or index of data elements and their definitions, of covered information collected or maintained by the State Board, including, but not limited to, both of the following:

(1) Covered information that schools are required to report to the State Board by State or federal law.

(2) Covered information in the State longitudinal data system or any data warehouse used by the State Board to populate the longitudinal data system.

The inventory shall make clear for what purposes the State Board uses the covered information.

(e) The State Board shall develop, publish, and make publicly available, for the benefit of schools, model student data privacy policies and procedures that comply with relevant State and federal law, including, but not limited to, a model notice that schools must use to provide notice to parents and students about operators. The notice must state, in general terms, the types of student data that are collected by the schools and shared with operators under this Act and the purposes of collecting and using the student data. After creation of the notice under this subsection, a school shall, at the beginning of each school year, provide the notice to parents by the same means generally used to send notices to them. This subsection does not apply to nonpublic schools.

(Source: P.A. 101-516, eff. 7-1-21.)

(105 ILCS 85/30)

Sec. 30. Applicability. This Act does not do any of the following:

(1) Limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or under a court order.

(2) Limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.

(3) Apply to general audience Internet websites,

general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.

(4) Limit service providers from providing Internet connectivity to schools or students and their families.

(5) Prohibit an operator of an Internet website, online service, online application, or mobile application from marketing educational products directly to parents if the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this Act.

(6) Impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this Act on those applications or software.

(7) Impose a duty upon a provider of an interactive computer service to review or enforce compliance with this Act by third-party content providers.

(8) Prohibit students from downloading, exporting, transferring, saving, or maintaining their own student data or documents.

(9) Supersede the federal Family Educational Rights and Privacy Act of 1974, ~~or rules adopted pursuant to that Act or~~ the Illinois School Student Records Act, or any rules adopted pursuant to those Acts.

(10) Prohibit an operator or school from producing and distributing, free or for consideration, student class photos and yearbooks to the school, students, parents, or individuals authorized by parents and to no others, in accordance with the terms of a written agreement between the operator and the school.

(Source: P.A. 100-315, eff. 8-24-17; 101-516, eff. 7-1-21.)

(105 ILCS 85/33 new)

Sec. 33. Parent and student rights.

(a) A student's covered information shall be collected only for K through 12 school purposes and not further processed in a manner that is incompatible with those purposes.

(b) A student's covered information shall only be adequate, relevant, and limited to what is necessary in relation to the K through 12 school purposes for which it is processed.

(c) Except for a parent of a student enrolled in a nonpublic school, the parent of a student enrolled in a school has the right to all of the following:

(1) Inspect and review the student's covered information, regardless of whether it is maintained by the school, the State Board, or an operator.

(2) Request from a school a paper or electronic copy of the student's covered information, including covered information maintained by an operator or the State Board. If a parent requests an electronic copy of the student's covered information under this paragraph, the school must provide an electronic copy of that information, unless the school does not maintain the information in an electronic format and reproducing the information in an electronic format would be unduly burdensome to the school. If a parent requests a paper copy of the student's covered information, the school may charge the parent the reasonable cost for copying the information in an amount not to exceed the amount fixed in a schedule adopted by the State Board, except that no parent may be denied a copy of the information due to the parent's inability to bear the cost of the copying. The State Board must adopt rules on the methodology and frequency of requests under this paragraph.

(3) Request corrections of factual inaccuracies contained in the student's covered information. After receiving a request for corrections and determining that a factual inaccuracy exists, a school must do either of the following:

(A) If the school maintains or possesses the

covered information that contains the factual inaccuracy, correct the factual inaccuracy and confirm the correction with the parent within 90 calendar days after receiving the parent's request.

(B) If the operator or State Board maintains or possesses the covered information that contains the factual inaccuracy, notify the operator or the State Board of the correction. The operator or the State Board must correct the factual inaccuracy and confirm the correction with the school within 90 calendar days after receiving the notice. Within 10 business days after receiving confirmation of the correction from the operator or State Board, the school must confirm the correction with the parent.

(d) Nothing in this Section shall be construed to limit the rights granted to parents and students under the Illinois School Student Records Act or the federal Family Educational Rights and Privacy Act of 1974.

(Source: P.A. 101-516, eff. 7-1-21.)

(105 ILCS 85/35)

Sec. 35. Enforcement. Violations of this Act shall constitute unlawful practices for which the Attorney General may take appropriate action under the Consumer Fraud and Deceptive Business Practices Act.

Section 10 of Public Law No: 102-0026

SEC. 10 DEPARTMENT OF EMPLOYMENT SECURITY LAW OF THE CIVIL ADMINISTRATIVE CODE OF ILLINOIS:

(20 ILCS 1005/1005-55 new)

Sec. 1005-55. Social security numbers; disclosure prohibited. Except as required under state or federal law, the Department shall not disclose an individual's entire social security number in any correspondence physically mailed to an individual or entity. The Department shall develop a process that allows for identifying information other than an individual's entire social security number to be used in correspondence. This Section does not apply to electronic data sharing pursuant to a written agreement containing appropriate security and confidentiality provisions or to an individual's or entity's secure account in the Department's databases.

APPENDIX D – Attorney General Raoul Announces $5 Million Settlement with Community Health Systems…

https://www.illinoisattorneygeneral.gov/pressroom/2020_10/20201008.html

ATTORNEY GENERAL RAOUL ANNOUNCES $5 MILLION SETTLEMENT WITH COMMUNITY HEALTH SYSTEMS FOR DATA BREACH

Data Breach Compromised More Than 339,000 Illinois Patients' Personal Information

Chicago — Attorney General Kwame Raoul today announced a $5 million settlement with Community Health Systems Inc. (CHS) resulting from a 2014 data breach that impacted approximately 6.1 million patients nationwide. Attorney General Raoul, along with Tennessee Attorney General Herbert Slatery III and Texas Attorney General Ken Paxton, led a bipartisan coalition of 28 states that reached the settlement with CHS and its subsidiary, CHSPSC LLC.

In 2014, CHS confirmed that its computer network was the target of an external cyber attack that allowed hackers to gain access to patient names, birthdates, Social Security numbers, phone numbers and addresses. More than 339,000 impacted patients were Illinois residents. Raoul filed a lawsuit and a settlement today requiring CHS to pay states $5 million, more than $611,000 of which will go to Illinois. CHS has also agreed to implement and maintain a comprehensive information security program to safeguard personal information and implement policies to quickly identify and address future breaches.

"When patients provide sensitive personal information such as Social Security numbers and birthdates, they are trusting that it will be kept safe and confidential," Raoul said. "This settlement requires CHS to enact procedures to better protect patients' information, and to develop plans to react quickly if another breach occurs. I will continue working to hold companies responsible for not doing enough to protect consumers' personal information from data breaches."

The settlement requires CHS to take a number of steps to prevent future breaches, such as developing an incident plan so that the company will know what to do if a breach occurs. The settlement also requires CHS to employ additional policies to protect sensitive patient information, such as:

- Developing and implementing a written information security program.
- Developing a plan to ensure that any needed software patches are detected and applied in a timely manner to avoid allowing security gaps.
- Maintaining strict control over access to CHS' accounts and network, and implementing measures such as multi-factor authentication to limit access only to authorized individuals.
- Providing regular security and privacy training for all employees who handle or come into contact with sensitive patient data.
- Developing and maintaining policies and procedures to encrypt sensitive data when appropriate.
- Conducting an annual risk assessment of the CHS network, and developing a plan for addressing those risks and protecting data.

- Requiring any third-party companies that provide services to CHS involving the handling or storage of sensitive patient data to agree to take certain precautions to protect the data.
- Implementing and maintaining policies to track and protect all company computers, phones and other devices that have access to or transmit sensitive patient data.
- Engaging a third-party assessor to evaluate CHS' compliance with the terms of the judgment and the handling of sensitive patient data.

Privacy Unit Chief Matt Van Hise, Consumer Fraud Bureau Chief Beth Blackston, and Assistant Attorneys General Carolyn Friedman and Ronak Shah handled the settlement for Raoul's Consumer Fraud Bureau.

Joining Attorneys General Raoul, Slatery and Paxton in today's settlement are the attorneys general of Alaska, Arkansas, Connecticut, Florida, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Michigan, Mississippi, Missouri, Nebraska, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Utah, Vermont, Washington and West Virginia.