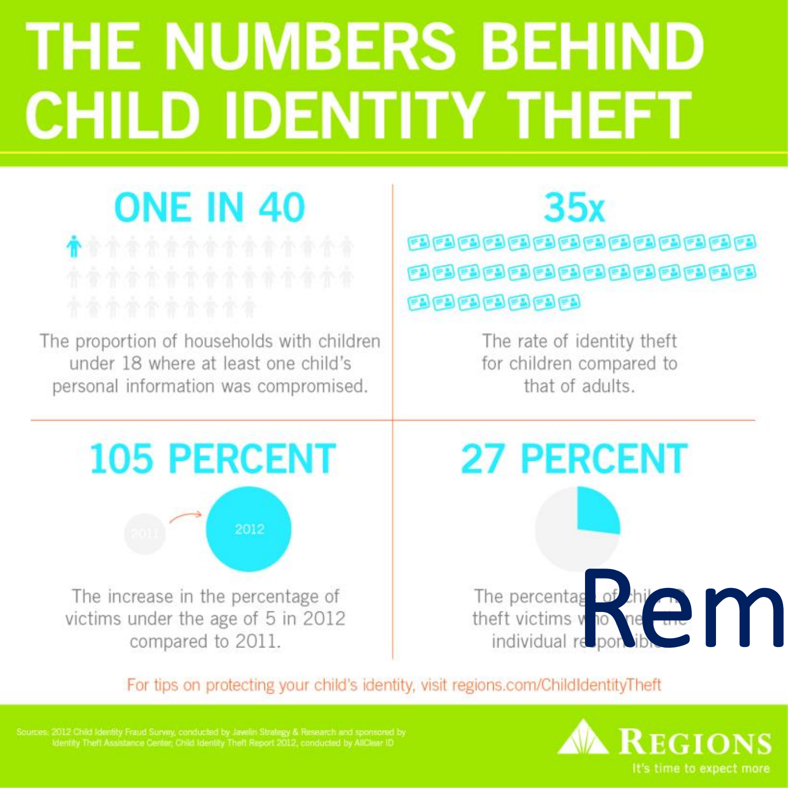

THE NUMBERS BEHIND CHILD IDENTITY THEFT

ONE IN 40

The proportion of households with children under 18 where at least one child's personal information was compromised.

35x

The rate of identity theft for children compared to that of adults.

105 PERCENT

The increase in the percentage of victims under the age of 5 in 2012 compared to 2011.

27 PERCENT

The percentage of child ID theft victims who knew the individual responsible.

For tips on protecting your child's identity, visit regions.com/ChildIdentityTheft

Sources: 2012 Child Identity Fraud Survey, conducted by Javelin Strategy & Research and sponsored by Identity Theft Assistance Center; Child Identity Theft Report 2012, conducted by AllClear ID

REGIONS
It's time to expect more

Data Privacy

in the

Remote Learning Environment

Ryan Wassink

GST BOCES E-Learning Coordinator

April 19, 2021

I owe $23,000 on my credit cards,
my condo's in foreclosure and
I turn 4 on Friday.

Description

- NYS Ed Law 2d and the accompanying Part 121 Regulations have been put in place to protect sensitive student and teacher data. FERPA, COPPA, CIPA, and HIPAA laws exist for very similar reasons. Combined, these regulations and laws create a framework that all educators need to follow when designing lessons. Without strategically planning for this, managing these requirements becomes harder in online, distance, blended, or hybrid models of learning.

Disclaimer

- The content of this slideshow is not to be referenced or trusted as “legal advice”. It is for informational purposes only.

- Please discuss any potential legal issue with the proper school administrator or attorney. *I am not a law expert.*

Why does data privacy matter?

- Child Identity Theft is one of the fastest growing segments of fraud.
  - Social Security Numbers can be used to open credit cards or other money-making enterprises. https://www.youtube.com/watch?v=-5aGWPRpHSI
- Social networking data, browsing data, and other related data can determine the likes and habits of anyone, leading to all sorts of potentially nefarious acts. https://www.youtube.com/watch?v=fHhNWAKw0bY (some NSFW language)
- Health-related data can be used to harass or deny service to someone with certain characteristics.
- Data surrounding your voting habits or political/religious/moral beliefs can be used for many reasons. https://www.youtube.com/watch?v=iX8GxLP1FHo

Definitions

- PII (pii)
- Directory Information
- De-Classified Data
- Educational Record

What is PII?

- Personally Identifiable Information (PII) – the term includes, but is not limited to,
  - Student's name
  - Name of the student's parent or family members
  - Address of the student or student's family
  - Personal identifier, such as the student's social security number, student number, or biometric record
  - Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name
  - Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty,
  - information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates

What data is considered “Directory Information”?

- Directory Information – This information can be released without consent, and does not include social security numbers or student ID numbers
    - Student’s name
    - Address
    - Telephone number
    - Date and place of birth
    - Honors and awards
    - Sports and activities
    - Dates of attendance

What is de-identified data?

- Schools may disclose deidentified data without prior parental consent. Deidentification requires
  - Removal of all personally identifiable information (PII)

    -- and --

  - A reasonable determination that a student's identity is not personally identifiable
  - De-identified education records may be disclosed for education research purposes, provided the school attaches a code to the de-identified data to allow the recipient of the data to match information received from the same source. The code must not be based on the student's social security number of other personal information, nor should it contain any information that would allow the recipient to identify a student based on the code.

What data is considered “Educational Record”?

- Education Records are those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

- Audio & Video:
  - As with any other “education record,” a photo or video of a student is an education record, subject to specific exclusions, when the photo or video is: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution. (20 U.S.C. 1232g(a)(4)(A); 34 CFR § 99.3 “Education Record”)[1]

https://www.youtube.com/watch?v=yrjT8m0hcKU&t=1s

Family Educational Rights and Privacy Act (FERPA)

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

- FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students.“

Family Educational Rights and Privacy Act (FERPA)

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

Family Educational Rights and Privacy Act (FERPA)

- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;
  - Organizations conducting certain studies for or on behalf of the school;
  - Accrediting organizations;
  - To comply with a judicial order or lawfully issued subpoena;
  - Appropriate officials in cases of health and safety emergencies; and
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

- Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

Family Educational Rights and Privacy Act (FERPA)

- Federal Law enacted in 1974
- Accountability is tied to federal funding
- Relevant for all K-12 students under the age of 18

- Other regulations under this act, effective starting January 3, 2012, allow for greater disclosures of personal and directory student identifying information and regulate student IDs and e-mail addresses. For example, schools may provide external companies a student's personally identifiable information without the student's consent. Conversely, tying student directory information to other information may result in a violation, as the combination creates an education record.

- http://spaces.gstboces.org/board/policies/5000%20Student%20Policies/5500%20FERPA.pdf

- https://www.fordham.edu/download/downloads/id/1850/09_-_dos_and_donts_for_teachers.pdf

Children’s Internet Protection Act
(CIPA)

- *The law states:*
  - CIPA requires K-12 schools and libraries using E-rate discounts to operate "a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors". Such a technology protection measure must be employed "during any use of such computers by minors". The law also provides that the school or library "may disable the technology protection measure concerned, during use by an adult, to enable access for *bona fide* research or other lawful purpose".

Children’s Internet Protection Act (CIPA)

- Federal Law enacted in December, 2000
- accountability is tied to federal funding (e-rate telecommunication funds)
- meant for public libraries and K-12 schools

- Many libraries (over 30%) have chosen to no longer apply for these E-rate funds so that they do not need to comply with this filtering requirement.

- The Supreme Court heard a case regarding the 1st amendment rights to information in a public setting and upheld the constitutionality of this act specifically because it did allow for adults to bypass security measures for bona fide purposes.
- Many institutions have additional policies regarding this – most schools do not allow classroom teachers or building administrators to bypass content filtering due to the need to protect staff from liability in case indecent materials appear after the filter is bypassed.

- http://spaces.gstboces.org/board/policies/4000%20Instruction/4527%20Internet%20Protection%20Policy.pdf

Children's Internet Protection Act (CIPA)

- As of July 1, 2012, as part of their CIPA certification, schools also certify that their internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

  https://www.usac.org/e-rate/applicant-process/starting-services/cipa/

Health Insurance Portability and Accountability Act (HIPAA)

- Federal law passed in 1996 (Dept of Health & Human Services)
- Relevant to Healthcare Providers, Health Plans, Healthcare Clearinghouses, and Business Associates.
- 2 parts:
    - Privacy Rule
        - The Privacy Rule standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities." The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.
    - Security Rule
        - *Deals with electronically-transmitted information*
            - Ensure the confidentiality, integrity, and availability of all electronic protected health information
            - Detect and safeguard against anticipated threats to the security of the information
            - Protect against anticipated impermissible uses or disclosures
            - Certify compliance by their workforce

Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA does not usually apply to educators in public schools, as this information is protected under FERPA.
    - Since FERPA only applies to schools that receive funds from the Dept of Education, it does not always cover records in private schools. Those schools should protect student data following FERPA guidelines but are not required to.
    - *https://www.hipaajournal.com/does-hipaa-apply-to-schools/*
    - *https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html*

FR
iPad Giv aw ay
Pass

Children’s Online Privacy Protection Act (COPPA)

- Federal law passed in 1998 (Federal Trade Commission)
- Only relevant for students younger than 13 years of age
- This rule is meant for technology providers, but school districts get involved when using their software.
- COPPA requires operators (online service providers, website operators, etc.) to
  - Provide notice to parents
    - Wishes to collect personal information from an individual child
    - Type of information it wishes to collect
    - Purpose of information collection
    - Means by which parents can provide and revoke consent
  - Obtain <u>verifiable parental consent</u> before they begin collecting, using or disclosing information from children under age 13
    - COPPA permits a school to obtain parental consent on the operator’s behalf, as long as the operator uses the information only on behalf of the school pursuant to the agreement between the school and the operator.
    - An operator must obtain consent directly from the parents if it wants to use the data collected from the school for its own commercial purposes

Children’s Online Privacy Protection Act (COPPA)

- NYS Ed Law 2d and Regulations 121 cover many of these same needs in much greater detail; however –
  - Opting-out is not recommended for COPPA compliance. According to the rules, a school needs verifiable parent permission to use their software before agreeing to use that software with those students. This includes any commercial software that uses ads, tracking cookies, or collects any data on users who are under the age of 13.
  - Teachers who click “agree” on click-through agreements stating that they have parental permission to add students to an app or site are, in fact, committing forgery if permission has not specifically been granted.
  - Teachers should never agree to these terms without the documented consent of a technology director and/or school attorney.

NYS Ed Law 2d

- state law went into effect April 2014
- Applicable to all New York public K-12 schools
- The student data protected under the statute consists of the same elements as are protected pursuant to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232-g.

- Also: Ed Law 2d regulates the Individuals with Disabilities Education Act (IDEA), 20 U.S.C. § 1400 *et seq*., as PII, with regard to IDEA eligible students, that is: a list of personal characteristics or other information that would make it possible to identify the child with reasonable certainty. 34 CFR § 300.32.

- Teacher data or principal data, defined as PII from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

NYS Ed Law 2d

- Teachers who intentionally circumvent the law (intentional negligence) may be subject to administrative or legal penalties including lawsuits, fines, or job loss. Since all school employees are required to attend an annual training, it will be hard to claim non-negligence in many cases.

- Oftentimes a lawsuit or fine would be directed at the school entity

Part 121 Regulations

- Education Commissioner’s regulations went into effect October 2020
- Applies to all public K-12 schools

- Build onto the original Ed Law 2d in many ways

- https://riconedpss.org/resources

This slide – and the next – could be outdated and Kahoot! may now be compliant. It can be used to show that even heavily-used sites that are thought of as "educational sites" aren't always compliant with data privacy laws.

Kahoot Privacy Policy

- **CROSS-BORDER TRANSFER**
  Your Personal Information may be stored and processed in any country where we have facilities or in which we engage service providers, and by using the Services you understand that your information will be transferred to countries outside of your country of residence, which may have data protection rules that are different from those of your country.
- If you are located in the European Economic Area (“EEA”): Some of the non-EEA countries are recognized by the European Commission as providing an adequate level of data protection according to EEA standards (the full list of these countries is available **here**). For transfers from the EEA to countries not considered adequate by the European Commission, we have put in place adequate measures, such as standard contractual clauses adopted by the European Commission to protect your Personal Information. You may obtain a copy of these measures by contacting us (see below under Contacting Us).

What can I do?

1. Never use unauthorized apps, sites, or programs that are even questionable. Err on the side of caution 100% of the time.
2. Protect all data as strongly as possible both with physical safeguards and technological best-practices and encourage others to do the same.
3. Pre-plan! Looking for a “good resource to share with my students” the night before the lesson can lead to mistakes being made.
4. Report anything that you find suspicious; your action may stop an entire chain of events from unfurling.

1: Never use unauthorized apps, sites, or programs that are even questionable. Err on the side of caution 100% of the time.

- The Technology Director and/or DPO are trained to evaluate and identify resources that can (or cannot) be used with students
- Be honest – circumventing these rules intentionally may lead to disciplinary actions.
- Never click on a click-through agreement without having documented proof that you can do so.
- If you share your resources with other educators, always suggest that they ask their Tech Director or DPO before using it in a classroom. Just because it is compliant at GST BOCES doesn’t make it compliant elsewhere.

2: Protect all data as strongly as possible both with physical safeguards and technological best-practices and encourage others to do the same.

- Protect your physical computer and any backup drives.
  - Lock your computer when you walk away! Windows & L key
- Device encryption is mandatory – if you are not savvy enough to enable this, reach out to someone who can help.
  - Your hard drive should already be encrypted on your laptop.
  - If you have a phone or tablet with BOCES accounts on it, you will need to maintain a security measure to unlock the device.
  - Backup hard drives and USB drives are often unencrypted – do not place PII on these devices!
  - Do NOT email data with PII to non-GST BOCES email accounts and do NOT save protected data on personal computers that are not secured properly.
- Keep your devices updated regularly.

3: Pre-plan! Looking for a “good resource to use with my students” the night before the lesson can lead to mistakes being made.

- Websites are generally okay to use for research so long as they do not require any PII be entered.
  - Surveys are one of the most-exploited things on the internet. “Fill out this survey to determine what your career should be” and then require an email address and name to send the results to. Students love taking surveys.
- Did you find a cool app that works 100% perfect for what you want to do? Talk to your DPO or Tech Director!
  - Their goal is to get data privacy agreements in place so you can use it! They are not trying to limit you to “terrible sites only”

4: Report anything that you find suspicious; your action may stop an entire chain of events from unfurling.

- Never plug in an unknown USB device as it may contain viruses.
  - see: USB Drop Attacks
- Learn how to properly spot phishing emails, hyperlinks, and websites.
  - see: Phishing
- If you see someone you don’t know in an area with access to sensitive data, verify their identity or ask an administrator to do so. This includes people using WiFi from a vehicle.
  - See: Wardriving and Social Engineering
- Watch out for others; the organization’s security = your security