"All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information." -- https://www.ala.org/advocacy/intfreedom/librarybill

What sort of safeguarding? What is being threatened & by what?

First thing most folks think of is: **Intellectual safety**—what materials or topics patrons are checking out.

- Censorship -- Between July 2021 and the end of March 2022, an astounding 1,586 book bannings took place in 86 school districts in 26 states, according to a comprehensive PEN America study.
- Politics – both parties looking for "dirt" on local candidates. Especially at the local level. Small town gossip.

This is indeed important, but it is the tip of the iceberg. There is also **Digital Safety** to be concerned about…

- Junkmail/scams
- Identity theft.
- Shared email accounts.

As software moves web-based and becomes more mobile, more opportunities for others to see patron info. Shared email accounts, family of staff working from home, etc.

Lastly we need to think about the patron's **Physical safety**. There are patrons in our database who have a "safe address" through a governmental program. They are literally in hiding, but want to use the library.

Another factor is not so much "safety" but confidentiality and courtesy. It isn't anyone's business (except the patron's and the 1 library staff person at time of contact) if they owe $$, have lost materials, what they are checking out, or where they live. Yes, there are times when some of that info needs to get passed along—*but that should be the exception, not SOP.*

ALA's statement says "including personally identifiable information" (PII). The Winnefox shared automation system (AKA ILS) definitely contains data that is considered PII.

The State of Wisconsin considers the following to be PII (I highlighted info that our database contains):

▯ Name.
▯ Address.
▯ Telephone number.
▯ Driver's license number.
▯ Social Security number
▯ Employer or place of employment
▯ Employee identification number
▯ Mother's maiden name
▯ Financial account numbers
▯ Taxpayer identification number

⬚ DNA profile

<mark>⬚ Any number or code that can be used alone or with an access device to obtain money, goods, services, or any other thing of value</mark>

⬚ Unique biometric data, including a fingerprint, voice print, retina or iris image, or any other unique physical representation

<mark>⬚ Any other information or data that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled</mark>

<mark>⬚ Any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.</mark>

When we think of improper disclosure of patron PII we tend to think of getting hacked—either the database itself, or staff email containing patron information. But there is also the tendency for staff to share patron info with each other, perhaps not being as careful as we ought to be. There is the tendency in library administration to think "the more info we have about a patron, the better we can meet their needs."

There is also the potential for staff to abuse/misuse patron PII, from as mild as using the database to look up the birthday of a friend, to using it to find a patron's address and then stalk and harass them. Both are real-life examples at Winnefox libraries. Both are breaches of patron confidentiality.

State statute is pretty explicit about to whom patron info may be released:

1) No one
    a. "Records of any library which is in whole or in part supported by public funds, including the records of a public library system, indicating the identity of any individual who borrows or uses the library's documents or other materials, resources, or services may not be disclosed…"
2) Except
    a. by court order or
    b. to persons acting within the scope of their duties in the administration of the library or library system,
    c. to persons authorized by the individual to inspect such records,
    d. to custodial parents or guardians of children under the age of 16 under sub. (4),
    e. to libraries under subs. (2) and (3),
    f. to law enforcement officers under sub. (5).
3) And [43.30(6)] delinquent/overdue information "limited to the individual's name, contact information, and the amount owed to the library. " may be disclosed
    a. To a collection agency
    b. A law enforcement agency, but only if the dollar value of the individual's delinquent account is at least $50.

When we think of all the reports and emails we send as part of our daily library jobs, reports with patron's name, ID, contact info, last activity, birthdate, sometimes what they have checkedout or overdue. A lot falls under "persons acting within the scope of their duties in the administration of the

library or library system" but we need to be mindful of the patron's rights to have their personal information protected.

The American Library Association urges all libraries to:

- Limit the degree to which personally identifiable information is collected, monitored, disclosed, and distributed; and
- Avoid creating unnecessary records; and
- Limit access to personally identifiable information to staff performing authorized functions; and
- Dispose of library usage records containing personally identifiable information unless they are needed for the efficient and lawful operation of the library, including, but not limited to data-related logs, digital records, vendor-collected data, and system backups; and
- Ensure that the library work with its organization's information technology unit to ensure that library usage records processed or held by the IT unit are treated in accordance with library records policies; and
- Ensure that those records that must be retained are secure; and
- Avoid library practices and procedures that place personally identifiable information on public view; and
- Assure that vendor agreements guarantee library control of all data and records; and
- Conduct an annual privacy audit to ensure that information processing procedures meet privacy requirements by examining how information about library users and employees is collected, stored, shared, used, and destroyed

My goals for 2022 are
1) to try and raise privacy awareness among staff and our member libraries and their staff;
2) to modify and secure the automation system and surrounding procedures to better meet the ALA recommendations above.