NORTH DAKOTA
UNIVERSITY SYSTEM
CORE TECHNOLOGY SERVICES

GLBA Compliance and the SafeGuards Rule

3/31/23

Brad Miller, Director, Information Security

Gramm-Leach-Bliley Act (GLBA)

Act

- Dear Colleague Letter (Safeguarding Against Data Breaches)
- Gramm-Leach-Bliley Act (GLBA)
- FACTA Red Flags Rule
- Family Educational Rights and Privacy Act (FERPA)
- Student Aid Internet Gateway (SAIG) Enrollment Agreement
- Contractual Agreements (Third-Party liability)
- Protected Controlled Unclassified Information (CUI): NIST SP 800-171
- Higher Education Act (HEA)
- Federal Information Security Management Act (FISMA): NIST SP 800-53 Revision 4

GLBA, also known as the Financial Services Modernization Act of 1999 requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

HIGHER EDUCATION AND GLBA

GLBA applies to any business engaging in financial activities.

FINANCIAL ACTIVITY IN HIGHER EDUCATION

- Student loans
  (Including receiving application information)
- Grants
- Federal work-study program
- Financial advisory services (like 401K programs)
- Debt collections
- Check cashing services
- Career counseling services
- Health insurance provisioning

COMMONLY AFFECTED DEPARTMENTS

- Administration
- Financial Aid
- Student Services
- Information Technology
- Student Information Management

GLBA has also been added to the FAFSA Participation Agreement and the Federal Student Aid Handbook.

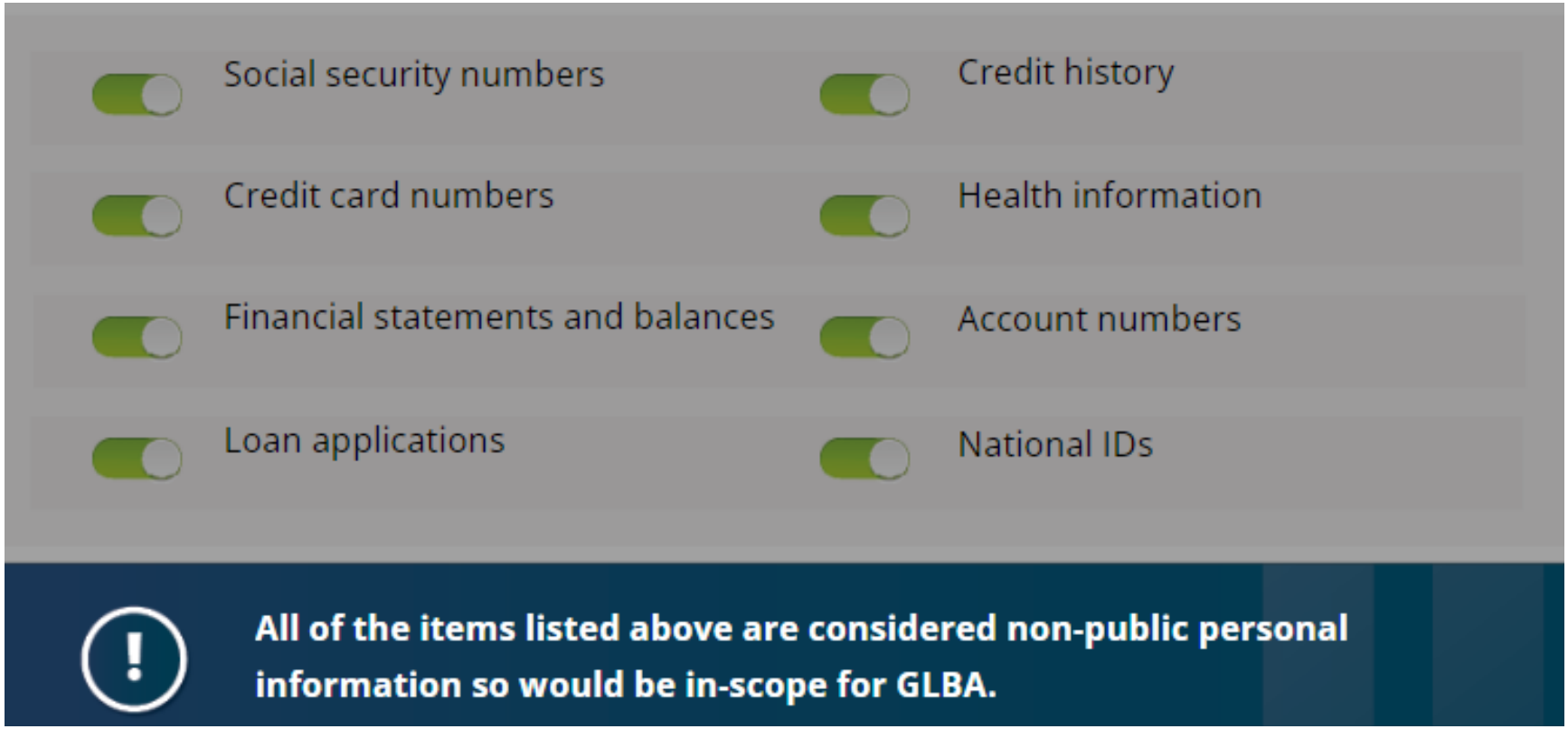
In recent years, the Department of Education has issued two OCR Dear Colleague Letters reminding institutions of their legal obligations to protect student information and FSA's enforcement through annual compliance audits.

The compliance supplement for the federal single audit process includes the audit objective for the Safeguards Rule. Auditors are checking to see if institutions have:

- **Appointed a coordinator for the institution's information security program**
- **Performed a risk assessment addressing employee training and management, network and systems, and incident response**
- **Implemented safeguards for all risks identified**

If FSA documents an audit finding, they refer that audit to the FTC, who then determines what action may be needed as a result.

Institutions are ultimately responsible to the FTC for complying with the Safeguards Rule, but a determination by FSA that an institution is not complying with the Safeguards Rule can affect its Title IV eligibility, and therefore the ability of the students enrolled at the institution to get federal student loans and financial aid.


Social security numbers
Credit history
Credit card numbers
Health information
Financial statements and balances
Account numbers
Loan applications
National IDs
All of the items listed above are considered non-public personal information so would be in-scope for GLBA.

COMMON RISKS

Privacy and security risks to sensitive information can come from a variety of possible gaps, which is why it is so important for organizations to perform ongoing risk assessments and identify and prioritize risks accordingly.

- Unauthorized Disclosures
- Overheard Conversations
- Information on Paper
- Inappropriate Access
- System Misconfiguration
- Insecure Storage Facilities
- Failure to Classify Data
- Personal Devices
- Viruses/Malware
- Failed Software Updates
- Email Security/Phishing

SAFEGUARDS RULE

There are no exceptions to the Safeguards Rule, and the FTC requires all institutions to develop an information security program to protect customer information.

1. Develop, implement, and maintain a ***written information security program***.
2. ***Designate a program*** coordinator.
3. ***Identify and assess risks*** to customer information.
4. ***Design and implement*** a ***safeguards program*** (including policies and procedures to manage and control risks).
5. ***Regularly test and monitor*** the effectiveness of all safeguards.
6. Select and oversee ***third-party service providers*** who implement and maintain appropriate safeguards.
7. ***Periodically evaluate and update the security program*** to account for changes in technology, as well as new threats.


New Requirements
Data Inventory and Classification
Written Risk Assessments
Designation of Qualified Individual
Written Reports to the Board of Directors
Access and Authentication Controls
System Monitoring
Data Retention and Disposal
Encryption of customer information at Rest and in Transit
Multifactor Authentication for all individuals
Penetration Testing and Vulnerability Scanning
Secure Development Practices
Change Management Procedures
Incident Response Plan
Employee Training
Vendor Management

Security Best Practices
Physical Security

- Securely destroy paper containing NPI
- Secure all stored NPI in locked desks or file cabinets (do not keep sensitive files on your desk)

Security Best Practices

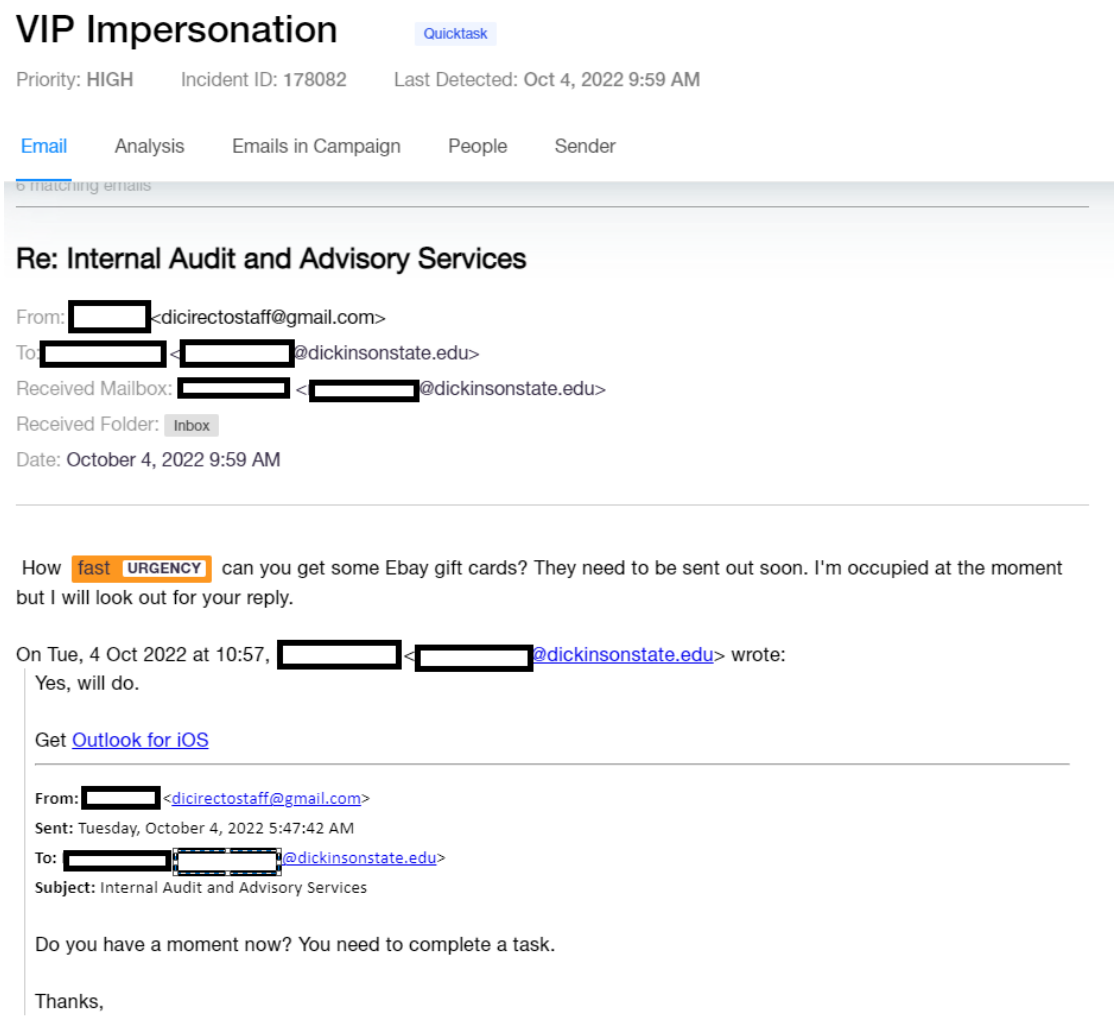
Email Security

- Do not email NPI
- Be aware of email scams, fraud, and phishing – never click on links or attachments in suspicious emails.

NORTH DAKOTA UNIVERSITY SYSTEM

Security Best Practices

Email Security



VIP Impersonation Quicktask

Priority: HIGH Incident ID: 178082 Last Detected: Oct 4, 2022 9:59 AM

Email Analysis Emails in Campaign People Sender

6 matching emails

Re: Internal Audit and Advisory Services

From: [redacted] <dicirectostaff@gmail.com>

To: [redacted] <[redacted]@dickinsonstate.edu>

Received Mailbox: [redacted] <[redacted]@dickinsonstate.edu>

Received Folder: Inbox

Date: October 4, 2022 9:59 AM

How fast URGENCY can you get some Ebay gift cards? They need to be sent out soon. I'm occupied at the moment but I will look out for your reply.

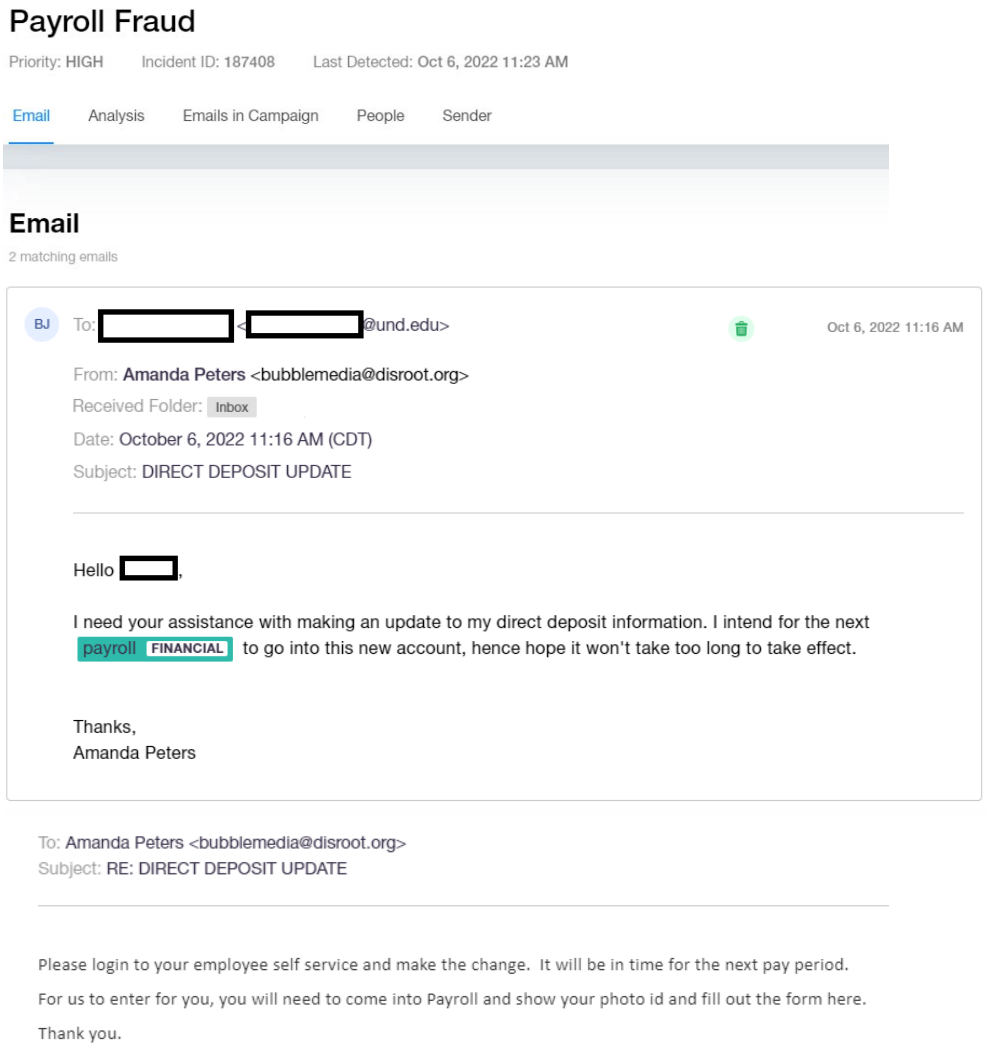
On Tue, 4 Oct 2022 at 10:57, [redacted] <[redacted]@dickinsonstate.edu> wrote:

> Yes, will do.
>
> Get Outlook for iOS
>
> **From:** [redacted] <dicirectostaff@gmail.com>
> **Sent:** Tuesday, October 4, 2022 5:47:42 AM
> **To:** [redacted] <[redacted]@dickinsonstate.edu>
> **Subject:** Internal Audit and Advisory Services
>
> Do you have a moment now? You need to complete a task.
>
> Thanks,

NORTH DAKOTA UNIVERSITY SYSTEM

Security Best Practices

Email Security



Payroll Fraud

Priority: HIGH Incident ID: 187408 Last Detected: Oct 6, 2022 11:23 AM

Email Analysis Emails in Campaign People Sender

Email

2 matching emails

BJ To: [redacted] <[redacted]@und.edu> Oct 6, 2022 11:16 AM

From: Amanda Peters <bubblemedia@disroot.org>
Received Folder: Inbox
Date: October 6, 2022 11:16 AM (CDT)
Subject: DIRECT DEPOSIT UPDATE

Hello [redacted],

I need your assistance with making an update to my direct deposit information. I intend for the next payroll FINANCIAL to go into this new account, hence hope it won't take too long to take effect.

Thanks,
Amanda Peters

To: Amanda Peters <bubblemedia@disroot.org>
Subject: RE: DIRECT DEPOSIT UPDATE

Please login to your employee self service and make the change. It will be in time for the next pay period.

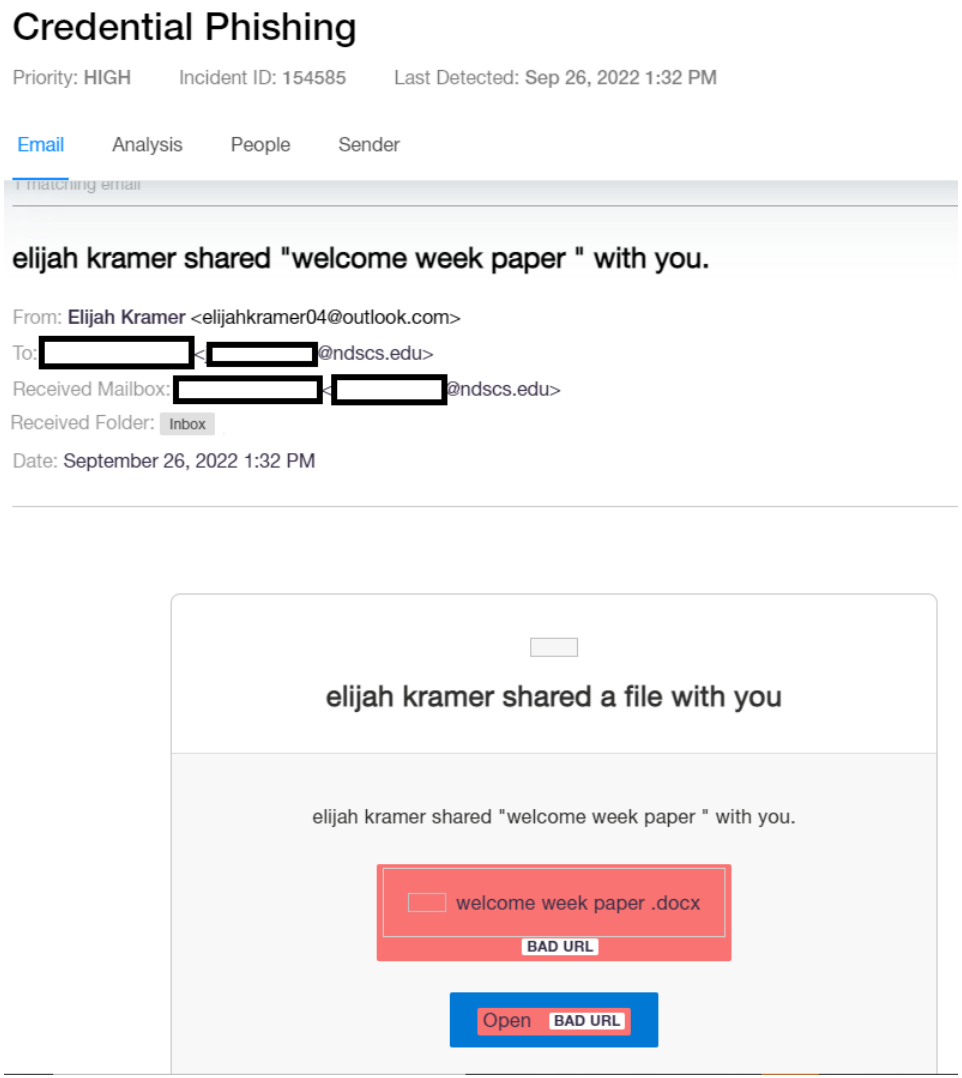
For us to enter for you, you will need to come into Payroll and show your photo id and fill out the form here.

Thank you.

NORTH DAKOTA UNIVERSITY SYSTEM

Security Best Practices

Email Security



Security Best Practices

Don't send NPI in email

https:\\sendfiles.ndus.edu

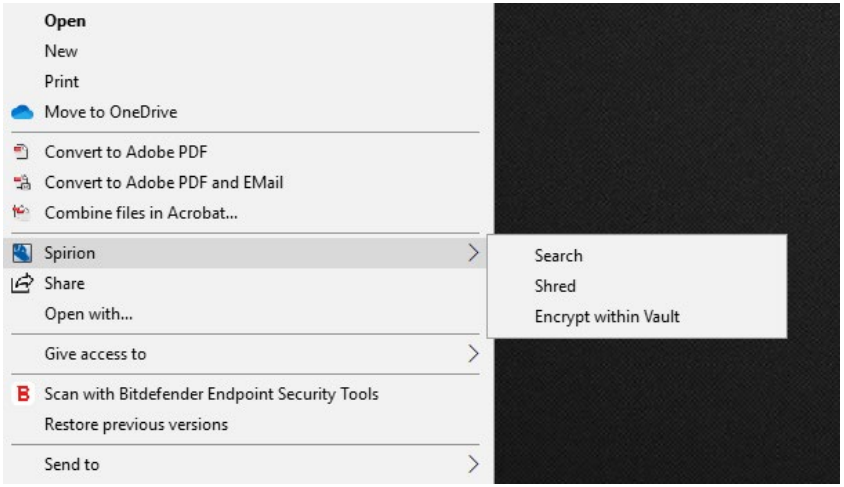
NORTH DAKOTA UNIVERSITY SYSTEM

Security Best Practices

Minimize Storage of NPI

Store on authorized devices, delete whenever you can

- Secure erase (Shred)
- Store on file shares/servers

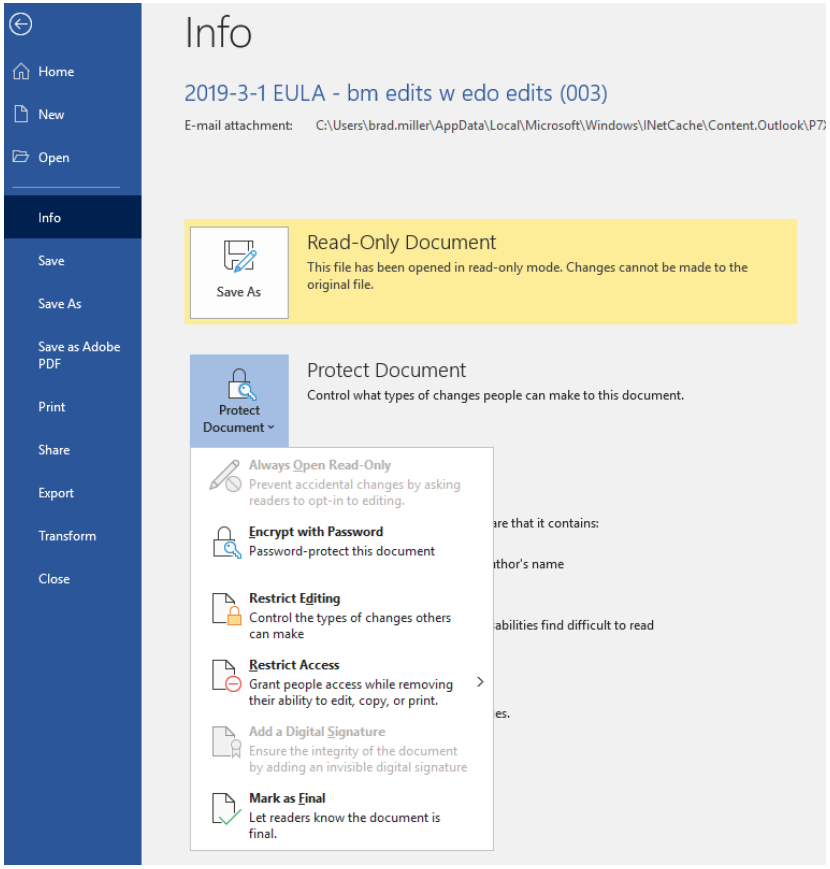


NORTH DAKOTA UNIVERSITY SYSTEM

Security Best Practices

Protect NPI Data

- Encrypt – Full Disk, File/Folder – Office



NORTH DAKOTA UNIVERSITY SYSTEM

Security Best Practices

Account Security

Use Multifactor Authentication

Do not share accounts with other users

GOOGLE AUTHENTICATOR

Microsoft Authenticator

Security Best Practices

Protect Passwords

- Use a strong password
- Use a Password Safe/Vault

LastPass •••|

1Password

KEEPER®

Security Best Practices

Recognize and report suspicious activities immediately

BEST PRACTICES

Use the following three simple rules regarding sensitive data:

Collect only what you need.

Keep it safe.

Dispose of it securely.

QUESTIONS?