Should you send or receive UNH personally identifiable information by email?

The transmission of personally identifiable information (PII) by email or FAX should never be done without the use of appropriate data protection. This includes UNH data classified as restricted (protection mandated by state or federal laws) as well as sensitive (protection mandated by university policy or contract).

As an example of restricted data protection, the USNH System Access Policy specifically prohibits sending social security numbers (SSN) through email, unless they are encrypted or reduced to the last four digits. UNH IT Security urges that even the last four digits should not be sent by email un-encrypted, because identity thieves can reconstruct SSNs from the last four digits in combination with other obtainable information.

When anyone, any service provider or agency sends you an email with SSNs, alerting them to not do so is the most appropriate response. You should delete the message immediately and purge it from the deleted folder; the sender should also be urged to delete and purge it from their sent folder. Both parties should delete and purge any other copies they may have in email.

All service providers and agencies should have in their publicly available privacy policy a warning about not sending to the service provider any SSNs or other legally protected information by unprotected email. The statement could be displayed on the service provider's website; for example: "We do not accept, and ask that you not send us by email, legally protected information, such as SSNs, unless the information is properly protected from unauthorized viewing through mechanisms that include encryption. Please contact us by telephone to make appropriate arrangements before sending such information." Service providers and agencies that routinely need to receive such information as part of their business can post additional detailed information about how to do so safely.

When sending such information by FAX, it is important to ensure that it is a secure FAX transaction. At minimum, the sending party should ensure that the recipient is expecting it and will ensure that the document does not stay on the receiving fax machine for unauthorized persons to see.

The question of emailing sensitive data such as a person’s date of birth (DOB) is more complicated. Technically it is not listed as protected PII in current privacy laws; however, the DOB is often used for changing or recovering passwords, setting up bank accounts or gaining access to accounts and medical services. Many individuals consider it highly sensitive for personal reasons. IT Security recommends that DOB should be protected the same way that the SSN is, however the SSN has the additional burden that protection is required by policy and law. The consequence of a breach of an SSN includes reporting such to the attorney general’s office (ex. NH, Mass, CA…) and to the person whose SSN was breached.

Finally, UNH IT Security does not agree with any claim that email is secure. Email is insecure because it is subject to malware, phishing, accidental sending or forwarding a message to the wrong person, and copies of messages remain in the originating and receiving system for extended periods of time. For example, with the UNH Identity Finder initiative, significant amounts of protected information have been found in email messages from more than a decade ago. The risks associated with this situation potentially exceed millions of dollars – as well as damage to the university’s reputation - if those messages or email accounts are compromised.

Resources:

- The USNH System Access Policy can be read at [http://www.usnh.edu/olpm/USY/VI.Prop/F.htm#5.7](http://www.usnh.edu/olpm/USY/VI.Prop/F.htm#5.7)
- The UNH University Identifier Policy which includes handling of SSN’s and other restricted PII can be read at [http://www.usnh.edu/olpm/UNH/VI.Prop/F.htm#4.5](http://www.usnh.edu/olpm/UNH/VI.Prop/F.htm#4.5).
- For more information on using encryption to protect restricted and sensitive information, contact IT Security at [https://itsupport.unh.edu/itsec/](https://itsupport.unh.edu/itsec/).