Should you send or receive UNH personally identifiable information by email?
UNH ISS, August 2015

The transmission of personally identifiable information (PII) by email or fax should only be done when no other practical options are available and the communication serves a legitimate business need. Emailing or faxing PII classified as restricted (protection mandated by state or federal laws) should never be done without appropriate protections such as file encryption or use of a secure fax service, for example. Transmission of sensitive PII (protection mandated by university policy or contract) by email or fax is generally not recommended by ISS, however, where this conflicts with established business practices, it is not prohibited. ISS would recommend that departments consider alternative means of sharing data such as through Box@UNH.

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 ISS 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 any person, 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 un-authorized persons to see. Preferably, the receiving party will provide a dedicated fax device in a location not accessible to unauthorized persons for receipt of restricted information.

The question of emailing sensitive data such as a person's date of birth (DOB) is more complicated. While it is not listed as protected PII in current privacy laws, 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. ISS recommends that DOB should be protected in the same way as an SSN where practical, however, transmission of DOB, the USNH ID or other sensitive information via unencrypted email within the University or University System for legitimate business reasons is acceptable. As stated above, ISS urges departments to consider alternative means of sharing data such as through Box@UNH.

Resources:

- The USNH System Access Policy can be read at 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.
- For more information on using encryption to protect restricted and sensitive information, contact UNH ISS at https://itsupport.unh.edu/itsec/.