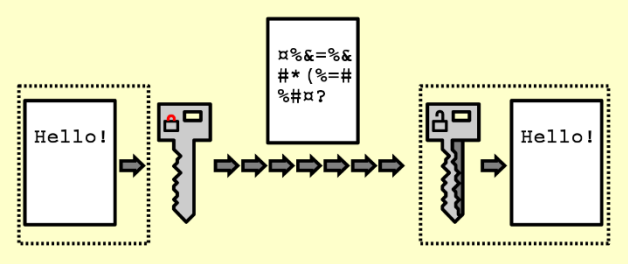
DATA ENCRYPTION – WV BIRTH TO THREE



Data Encryption in and of itself is a very large and involved topic that involves tech jargon and expertise. I will attempt to provide you some basic information to help you understand what encryption is and its importance when sending documents via the internet.

- **First, let's define data encryption.**

Data encryption translates information into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it.

- **What data should be encrypted? As a program our priority is protecting Personally Identifiable Information (PII).**

In broad terms, there are two types of data you should encrypt: personally identifiable information and confidential business intellectual property.

- *Personally Identifiable Information (PII)*
- *Confidential Business & Intellectual Property.*

Using secure, *encrypted email* is our answer to meet WVDHHR, HIPPAA, and FERPA requirements for sharing confidential information through the world-wide-web. This is our best defense for preventing data loss and possibly creating harm for our children and families.

The simplest way of sending an email that contains private information is to *password protect* the document. This is a type of encryption that the sender must provide the receiver a password so they may open a document. To use this method, you would complete a document and password protect it when you save the document to your files. (**Make sure to note the password**. You will not be able to open the document later without it and unless you pay for a special program, your document will remain forever locked!) In a separate email, you send your receiver the password that will allow them access to the document. They will then be able to open the document, print, save, and store as necessary.

Best practice is to use *email encryption.* Email encryption "disguises" the content of your email to protect sensitive information from being read by someone other than the receiver. Encryption renders content of your emails unreadable as they travel through cyberspace from home to destination.

Personally Identifiable Information (PII) – as a program under the WV Department of Health and Human Resources (WVDHHR) we are required to send emails securely that may contain information on our children and or families. You may have noticed that in many cases our emails contain perhaps initials or the child's ID number when we are sending or sharing information with you via an email message. This information is only privy to those who use it and if hacked does not provide enough information to do a child or family harm. However, any documents that are sent as attachments are sent via an encrypted format to your attention OR in the manner of a password protected document with the password sent separately.

As providers of services through WVBTT, you are also required to carry out the protection of PII when using email.

While this list is NOT all inclusive, here are some weblinks to access encryption through your email and or your Windows program.

https://mailvelope.com/en - Mailvelope will provide you with information on how to add it as an "add-on" to different web browsers i.e., Chrome, MS Edge, and Firefox. The site also offers tutorial and additional safety information.

Virtru – Gmail Encryption – Provides information on Google's add-on for encryption services. Dependent upon your operating system, you may be able to set this up at no additional cost.

Microsoft Office 365 – changes are coming soon to MS Office 365 and their encryption use. Visit this link to learn more about it!

PassLok for Email – this link will provide you with information on the encryption add-on for Firefox.

As always, do your research!! If you have a browser that you are using for your internet access and email that is not listed above, check to see if there is something that has been provided for you to use.

SAFELY SHARE INFORMATION BY USING ENCRYPTION!!