Keeping Payroll and Benefits Data Safe – Top Ten Tips

We all rely on the internet for key functions such as payroll processing (PrimePay) and benefits administration (BAS/MyEnroll), especially now that many of us work from home due to the pandemic. While steps are taken by the RCAB to audit security protocols that PrimePay and BAS have in place for their websites, data security risks still exist at the user level that must be addressed. Both Massachusetts and federal laws impose a duty on the users of these systems to protect certain data, such as SSNs, banking information, and driver's license/other state-issue ID numbers, which are commonly stored in PrimePay and/or MyEnroll. Please keep in mind your obligation to protect this data as you review the following tips:

1. **Limit administrator access** to PrimePay and MyEnroll to those staff/priests who are actually using these systems. Having a login and password issued to a person who will never log in is an unnecessary risk that should not be taken.
2. **Do not share logins or passwords**. Similar to point #2, if an individual needs access to one or both systems, he/she must be issued credentials that tie to him/her. Links to these access forms can be found at catholicbenefits.org/admins/admins.htm#adminforms.
3. Notify the Benefits Department ASAP when a staff member with access to these systems ends service so that **access can be revoked.**
4. When accessing PrimePay and MyEnroll outside the office, **do not use unsecured internet connections**, such as those provided at coffee shops or libraries.
5. Ensure any **laptops or portable devices** on which you access or store data from PrimePay or MyEnroll have **access passwords/PINS/encryption programs. Manually lock devices** when you will be away from them. If a device is lost or stolen, contact Risk Management and/or the Benefits Department ASAP.
6. Use **secure email** to send information between parishes or schools and/or to the Pastoral Center. If available, use an RCAB-provided email account. You may also send a secure email to the Benefits Department through MyEnroll (contact the Benefits Department for instructions).
7. **Do not take protected information outside of a secured area** unless absolutely necessary. Leave hard copies of this information at the office, where it should be securely stored in a locked room and/or cabinet where unauthorized staff members, parishioners, parents/students, are not permitted.
8. **Do not save files to your desktop or hard drive** if they contain protected data. Save to a network drive that has proper security safeguards in place.
9. If you must print sensitive information, store it in a secure area and/or **dispose of through cross-cut shredding** when no longer needed.
10. Any devices that are no longer used should be **sent to RCAB IT for destruction** if ever used to access protected data through PrimePay, MyEnroll, etc.

Finally, contact **Risk Management, IT, General Counsel's Office, and the Benefits Department ASAP** if a data breach occurs or if you need additional information/support for compliance with these requirements.