A picture containing text, clipart

Description automatically generated

**‘Care Share**

**Nov 2024**

The Centers for Medicare & Medicaid Services (CMS) are notifying people whose protected health information or other personally identifiable information may have been compromised in a data breach involving Wisconsin Physicians Service Insurance Corporation. It is one of many organizations in the United States that have been impacted by the MOVEit security vulnerability.

MOVEit is a third-party application used for the transfer of files in providing services to CMS. Similarly, this year there were 40 breaches involving Lash Group in Montana, which partners with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support services, business analytics and technology, and other services. You would have received a letter if you were involved.

Looking at the Montana Department of Justice website, there have been 540 separate data breaches like these in Montana over the past 12 months.

Why is this happening? Data breaches can occur for several reasons, including:  
  
**Hacking:** Cybercriminals exploit vulnerabilities in systems and networks to access sensitive data.

**Phishing:** Deceptive emails or messages trick individuals into providing personal information.

**Malware:** Malicious software can infiltrate systems, leading to data theft.

**Insider Threats:** Employees or contractors may intentionally or unintentionally expose data.

**Poor Security Practices:** Weak passwords, outdated software, and lack of encryption can create opportunities for breaches.

Receiving a data breach letter can be alarming. If this happens to you, here is a guide on what steps to take:

1. **Read the Letter Carefully**: Understand what information was compromised and the entity responsible for the breach. Look for details about the nature of the breach and what data was involved.
2. **Monitor Your Accounts**: Keep a close eye on your bank and credit card statements for any unauthorized transactions. Report any suspicious activity immediately.
3. **Change Passwords**: Update your passwords for affected accounts and any other accounts using the same or similar passwords. Use strong, unique passwords for each account.
4. **Enable Two-Factor Authentication** (2FA): If available, enable 2FA on your accounts to add an extra layer of security.
5. **Consider a Credit Freeze or Fraud Alert**: Placing a credit freeze restricts access to your credit report, while a fraud alert warns creditors to verify your identity before opening new accounts.
6. **Use Identity Theft Protection Services**: Consider enrolling in credit monitoring or identity theft protection services, which can alert you to potential fraud. Often, the letter will offer this for a limited time.
7. **Report Identity Theft**: If you notice any signs of identity theft, report it to the Federal Trade Commission (FTC) at IdentityTheft.gov.
8. **Stay Informed**: Keep an eye on any follow-up communications from the organization that experienced the breach for updates and further instructions.
9. **In the case of your Medicare**, whether you have given it out or it has been accessed through a breach make sure you:
   1. **Contact Medicare**: Call the Medicare helpline at 1-800-MEDICARE (1-800-633-4227) and report the situation.
   2. **Contact MT SMP** at 800-551-3191. They will collect your information and research further, referring your case to the Office of Inspector General.
   3. **Monitor Your Medicare Statements**: Keep an eye on your Medicare Summary Notices (MSNs) or Medicare Advantage EOB’s and call MT SMP to report any unauthorized services or claims you find.
   4. **Change Your Medicare Number** (if necessary): In certain situations, Medicare can issue a new number. Discuss this option with the Medicare representative when you contact them.
   5. **Stay Alert**: Be wary of any unsolicited calls or messages asking for further personal information. Scammers may use your Medicare number to try to obtain more details.

By taking these proactive steps, you can better safeguard your personal information and minimize the impact of a data breach.



**Let’s Talk Data Breaches**

Montana SMP is a program coordinated by Missoula Aging Services and partnered with local Area Agencies on Aging. This project was supported by grant #90MPPG0052 from the U.S. Administration for Community Living, Department of Health and Human Services, Washington D.C., 20201. Points of view or opinions do not necessarily represent official ACL policy.

The Senior Medicare Patrol (SMP) is ready to provide you with the information you need to PROTECT yourself from Medicare fraud, errors, and abuse; DETECT potential fraud, errors, and abuse; and REPORT your concerns. SMPs help educate and empower Medicare beneficiaries in the fight against health care fraud. Your SMP can help you with your questions, concerns, or complaints about potential fraud and abuse issues. It also provides information and educational presentations. To reach Montana Senior Medicare Patrol, call 1-800-551-3191 or visit www.smpresource.org.