REQUIRED CONTENT: 42 CFR 422.2265(B) – Health Info

## Policy Statement: Protecting the Privacy and Security of Health Information

Health information is highly sensitive and personal. Individuals are encouraged to take proactive measures to safeguard their health information and make informed decisions when sharing it in any form. Below are recommended steps and considerations to help protect the privacy and security of your health information:

### 1. Understand the Purpose and Use of Your Information

- Research the Recipient: Investigate the organization or individual requesting your health information. Understand how your information will be used and whether it will be shared with third parties.
- Ask Questions: Inquire about the necessity of providing specific details and the potential uses of your information beyond the stated purpose.

### 2. Evaluate Privacy Practices

- Access Privacy Policies: Ensure the organization or service provides a clear, detailed, and accessible privacy policy or explanation of their data-handling practices.
- Assess Data Usage: Confirm that the stated practices explicitly explain how your data will be collected, used, stored, and shared.
- Check for Third-Party Sharing: Identify whether your data will be shared with third parties and for what purposes (e.g., advertising, research, or other uses).

### 3. Verify Security Measures

- Data Protection: Confirm that measures such as encryption are used to protect your digital information.
- Secure Transmission: For digital exchanges, ensure the website uses secure protocols (e.g., HTTPS) and for physical exchanges, verify the use of secure handling procedures.
- Breach Notification: Verify that there is a clear protocol for notifying individuals in the event of a data breach.

### 4. Consider Data Ownership and Portability

- Data Ownership: Understand whether you retain ownership of your data or if it becomes the property of the organization.
- Data Deletion: Confirm that you can request the deletion of your data and that it will be permanently removed upon request.

**5. Monitor Secondary Uses of Data**

- Unintended Uses: Be cautious of your data being used for purposes beyond its original intent, such as targeted advertising or unrelated research.
- Opt-Out Options: Understand whether you have the option to opt-out of certain uses, such as inclusion in marketing or aggregate data analysis.

**6. Assess Legal and Regulatory Compliance**

- HIPAA Compliance: For entities in the U.S., check if they comply with the Health Insurance Portability and Accountability Act (HIPAA) if applicable.

**7. Limit Data Sharing**

- Share Only Necessary Information: Avoid providing more information than is required for the stated purpose.
- Review Permissions: When sharing data digitally, review and manage any permissions granted, such as access to personal or sensitive details.

**8. Stay Informed**

- Review Practices Regularly: Periodically revisit the privacy practices of organizations handling your information for any updates or changes.
- Monitor News: Stay alert to news about the organization's reputation and any reported security concerns.
- Maintain Records: Keep copies of any forms or communications for reference if questions arise later.

By taking these steps, individuals can better protect their health information and minimize potential risks to their privacy and security. Being vigilant about the practices and safeguards of any entity entrusted with sensitive data is critical to maintaining control over personal health information.