Delivering Personal Protected Information (PPI) Remotely

Toolkit for Delivering Services Remotely

A screen shot of a computer

Description automatically generated

Contents

[Overview 1](#_Toc193878702)

[Related Volunteer Risk and Program Management (VRPM) Policies 2](#_Toc193878703)

[What Information Needs Protection? 3](#_Toc193878704)

[How does this apply to grantees? 4](#_Toc193878705)

[Using “Print to Mail” or Fax 5](#_Toc193878706)

[Encrypting Email 5](#_Toc193878707)

[Creating an Adobe Acrobat Password-Protected Document 6](#_Toc193878708)

[Tips for Privacy and Confidentiality: Online vs. Offline 12](#_Toc193878709)

**Interchangeable Terminology Key**

Beneficiary …………………………………………………………………………………………… Client

Staff, Volunteers, Counselors ……………………………………………… Team Members

# Overview

This resource is intended to inform State Health Insurance Assistance Programs (SHIP), Medicare Improvements for Patients and Providers Act (MIPPA), and Senior Medicare Patrol (SMP) grantees of methods that can be used to guard client protected personal information that is being delivered electronically or by other remote means. Choosing which ways work for your organization and/or clients is important. Client program related contact forms and interactions are considered confidential and must be treated as such. The properly trained, screened, and state-certified team member must assure the client that all personal information collected is kept confidential. Remember to review your organization’s current policies and procedures before making your final decisions.

At the national level, SHIPs and SMPs operate under the Volunteer Risk and Program Management (VRPM) policies, some of which address information security. Two of those policies appear in this guide. SHIPs and SMPs have also been provided with Privacy and Confidentiality Training, which are available in the password-protected websites for SHIP and SMP grantees.

# Related Volunteer Risk and Program Management (VRPM) Policies

Grantees take the privacy and confidentiality of the clients served very seriously. VRPM policy 3.94 defines this expectation for SMP and SHIP volunteers, but the same expectation applies to paid staff and any partners that handle proprietary and privileged information.

When handling confidential information in a remote or electronic environment, the VRPM internet protocol policy also applies (excerpted below). Notice that this national policy mandates a protocol, but it does not define the protocol. Specific protocols must be determined by state SHIPs and SMPs[[1]](#footnote-1).

**3.94 Confidentiality [Required]**

*Policy:* Volunteers are responsible for maintaining the confidentiality of all proprietary or privileged information to which they are exposed while serving as a volunteer, whether this information involves a member of staff, a volunteer, a beneficiary or other person, or involves the overall business of the SMP/SHIP.

Volunteers take all steps necessary to safeguard the confidentiality of all SMP/SHIP and beneficiary related information and to prevent personal information of beneficiaries from falling into the possession unauthorized persons.

Volunteers use any information collected or obtained in their course of their SMP/SHIP work only to assist the beneficiary or otherwise fulfill volunteer role responsibilities. No information collected or obtained in the course of SMP/SHIP work is disclosed other than when clearly approved by an authorized SMP/SHIP representative.

There is zero tolerance for breaches of confidentiality in connection with work at the SMP/SHIP.

4.2 **Internet protocol [Required]**

*Policy:* The SMP/SHIP has a protocol for use of the internet, covering email use and appropriate access to web sites.

The SMP/SHIP has in place a protocol and appropriate training for volunteers who use wireless devices to connect to the internet while performing SMP/SHIP work.

The SMP/SHIP has a protocol and appropriate training for volunteers who make use of their personal computers while performing SMP/SHIP work.

# What Information Needs Protection?

When delivering information remotely, using encryption and passwords are the most common methods of protecting information from access by unintended people. This toolkit provides options and ideas for encrypting and password-protecting material you deliver. Obtaining client consent to relay certain information is another form of protection.

We have already talked about the importance of confidentiality, but when it comes to protecting information, it is also important to understand the terms “**individually identifiable health information**,” “**Protected Health Information (PHI)**,”and **“Personal Protected Information (PPI)**.”

* Individually identifiable health information is information, including demographic data, that relates to:
  + an individual’s past, present, or future physical or mental health or condition,
  + providing health care to the individual, or the past, present, or future payment for providing health care to an individual, and
  + identifies the individual or gives a reasonable basis to use in identifying an individual.
* Protected Health Information (PHI) is personal information that must be paired with individually identifiable health information. Here is a definition of PHI, with **important words emphasized**:
  + Individually identifiable **health information** that is explicitly linked to a particular individual, and health information which can allow individual identification. PHI includes many common identifiers (e.g., name, address, birth date, Social Security number) **when they can be associated with** individually identifiable health information.
* Personal Protected Information (PPI) includes both categories above. It is information which can be used to trace an individual’s identity, such as their name, Social Security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as a data and place of birth, mother’s maiden name, etc.

However, protected personal information does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the public. For example, names and addresses are publicly available on voter records.

# How does this apply to grantees?

Examples of information going out to clients or other team members from a grantee that would *NOT* be considered PHI or PPI and would *NOT* need encryption or password-protection include:

* Medicare Plan Finder plan comparisons (without plan details)
* Plan enrollment confirmation
* Brochures about the program or public educational materials

Reminder: When **health** information **is combined with personally** **identifiable** information, protect it. Separating those two components in the delivery process is one way to enhance security.

Information being exchanged between clients, program team members, and a grantee that *WOULD* be considered PHI or PPI include:

* Client Medicare.gov account login information
* Medicare Summary Notices (MSNs) or Explanations of Benefits (EOBs)
* Documents and information needed to refer client complaints/issues/complex interactions to the Centers for Medicare & Medicaid Services (CMS)
* Information requested from volunteers for background checks
* Completed intake forms with client prescription drugs listed
* Medicare Plan Finder plan details that list client prescription drugs

# Using “Print to Mail” or Fax

When a secure internet option is not available, the information or document can be printed out to:

* Mail the information or
* Fax the information, if the person has a fax machine

Another option is to use a company that can “print to mail.” This can be an expensive option. The average Midwest cost is around $2.30 per mailing. Here are some parameters that can be given by a grantee to a “print to mail” service:

* Completed cost comparisons would be emailed to the company, and the average number of pages would be 11 (single-sided)
* Company would also be sent a formatted cover letter that provided client name, address, and key points for the client to review in their cost comparison
* Documents need to be printed, put in an envelope, and mailed first class
* Mailings need to be sent and processed at least twice per week

# Encrypting Email

Emails that include personal information can be encrypted. Encryption is the process of making information into code to prevent others from getting the information that you didn’t send it to. It is important to tell your client before sending an encrypted email. For example:

* Explain that encrypted emails can be sent to junk mail folders, and they may need to check there if the email doesn’t appear in their inbox.
* Ask if they know their email’s file size restriction and be aware of the file size of your attachments.
* Remember to review your organization’s current policies and procedures.

# Creating an Adobe Acrobat Password-Protected Document

You can limit access to a PDF by setting passwords and by restricting certain features, such as printing and editing. However, you cannot avoid saving copies of a PDF. A copy has the same restrictions as the original PDF. Two types of PDF passwords are available:

* **Document Open Password** – (also known as a *user* password) requires a user to type a password to open the PDF.
* **Permissions Password –** (also known as a *master* password) requires a password to change permission settings. Using a permissions password, you can restrict printing, editing, and copying content in the PDF. Recipients don’t need a password to open the document in Reader or Acrobat. They do need a password to change the restrictions you've set.

If the PDF is secured with both types of passwords, it can be opened with either password. However, only the permissions password allows the user to change the restricted features. Because of the added security, setting both types of passwords are often beneficial.

**Note:** You cannot add passwords to a signed or certified document.

### Adobe Acrobat: Creating a Password-Protected PDF Document

1. A screenshot of a computer

   Description automatically generatedOpen the PDF.
2. Click on the “All Tools” tab, then click the “Protect a PDF” button.
3. You will still be in the document. Click the “Protect with password” option on the top left of the screen.

A screenshot of a computer program

Description automatically generated

1. A box will pop up stating “Protect Using Password”. Choose to allow the person with the password to view or edit the document.
2. A screenshot of a computer screen

   Description automatically generatedClick Apply.

### Adobe Acrobat: Creating a Password-Encrypted PDF Document

1. Open the PDF.
2. Click on the “All Tools” tab, click the “Protect a PDF” button, then click the “Encrypt with Password.”
3. It will ask if you would like to change the security on this document. Click “Yes”.

A screenshot of a computer error

Description automatically generated

1. Password Security – Settings will open.
2. Click to require a password to open the document and enter a password.
3. Click any permissions you would like such as restricting editing or printing of the document, the ability to copy text, images, and other content, or enabling text access for screen readers. This will require a different password from the read only password.
4. Click on any options you would like. A good tip is to make sure to click Encrypt all document contents.
5. Save the document to save the security settings.
6. Attach the document to your email. Call the recipient to give them the password(s) over the phone or send them in a separate email.

A screenshot of a computer

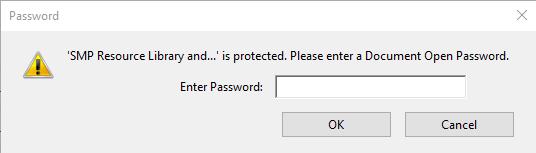
Description automatically generated

**Tip:** For more information on how recipients will open a protected Microsoft Word document, see the [Microsoft Word or Adobe PDF: Receiving a Password-Protected Document](#_Microsoft_Word_or) section and for more information you can visit [adobe.com/Online Tools](https://www.adobe.com/acrobat/online.html).

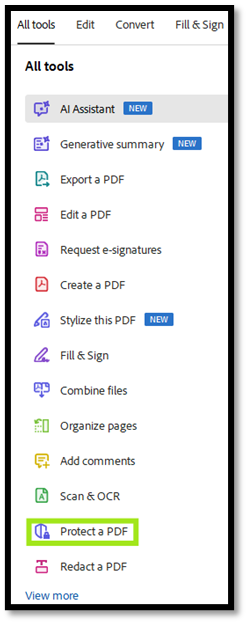
### Adobe Acrobat: Remove Password-Protected Security

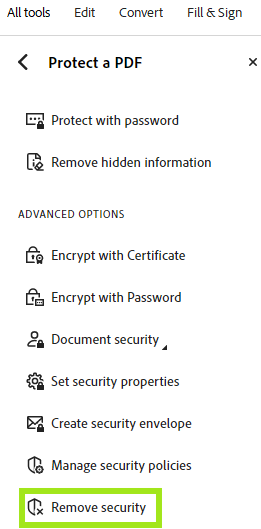
You can remove security from an open PDF if you have permissions to do so. If the PDF is secured with a server-based security policy, only the policy author or a server administrator can change it.

1. Open the PDF.
2. Enter the Document Open Password to access the document and then click “OK.”



1. Click on the “All Tools” tab, then click the “Protect a PDF” button.



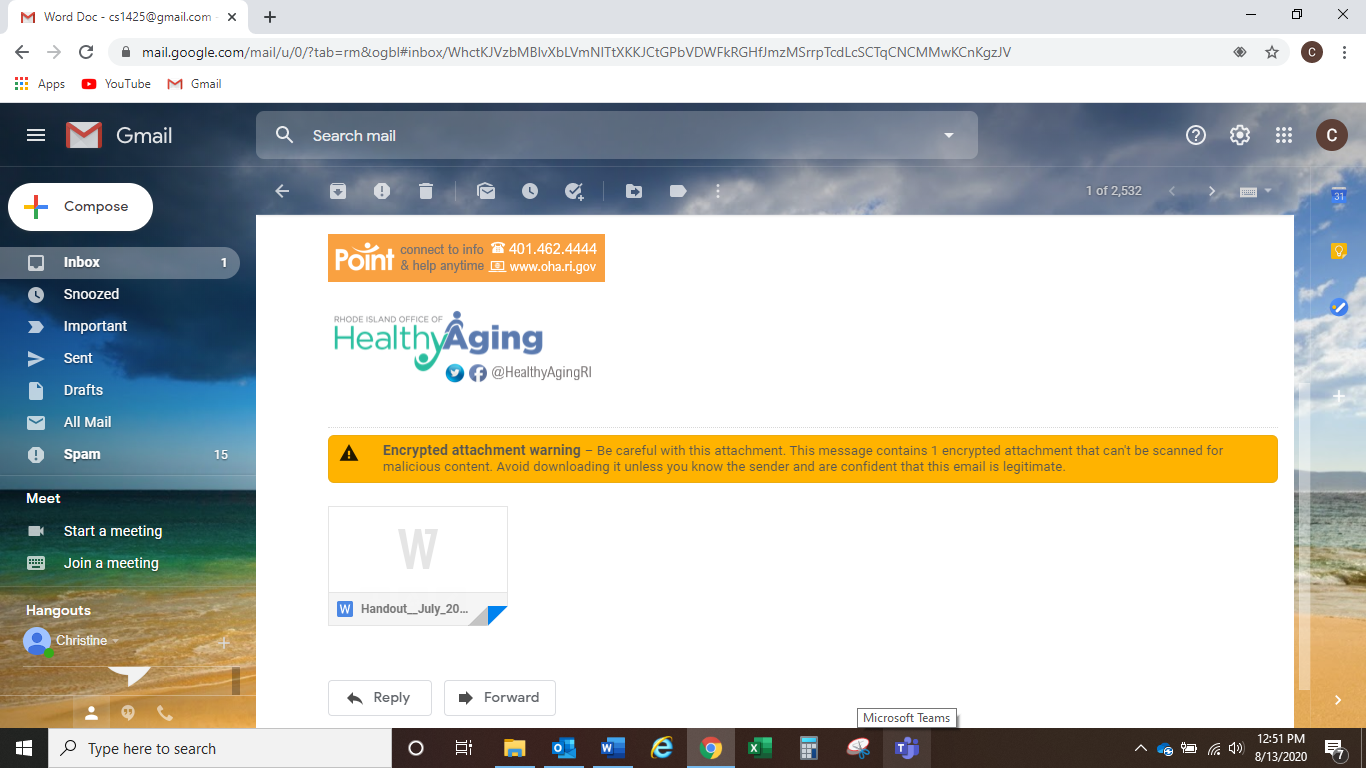
1. Click “Remove Security.”
2. Click “OK” to the pop-up asking if you are sure you want to remove security from the document.
3. If you have a permissions password, you will need to enter the permissions password to delete that password.

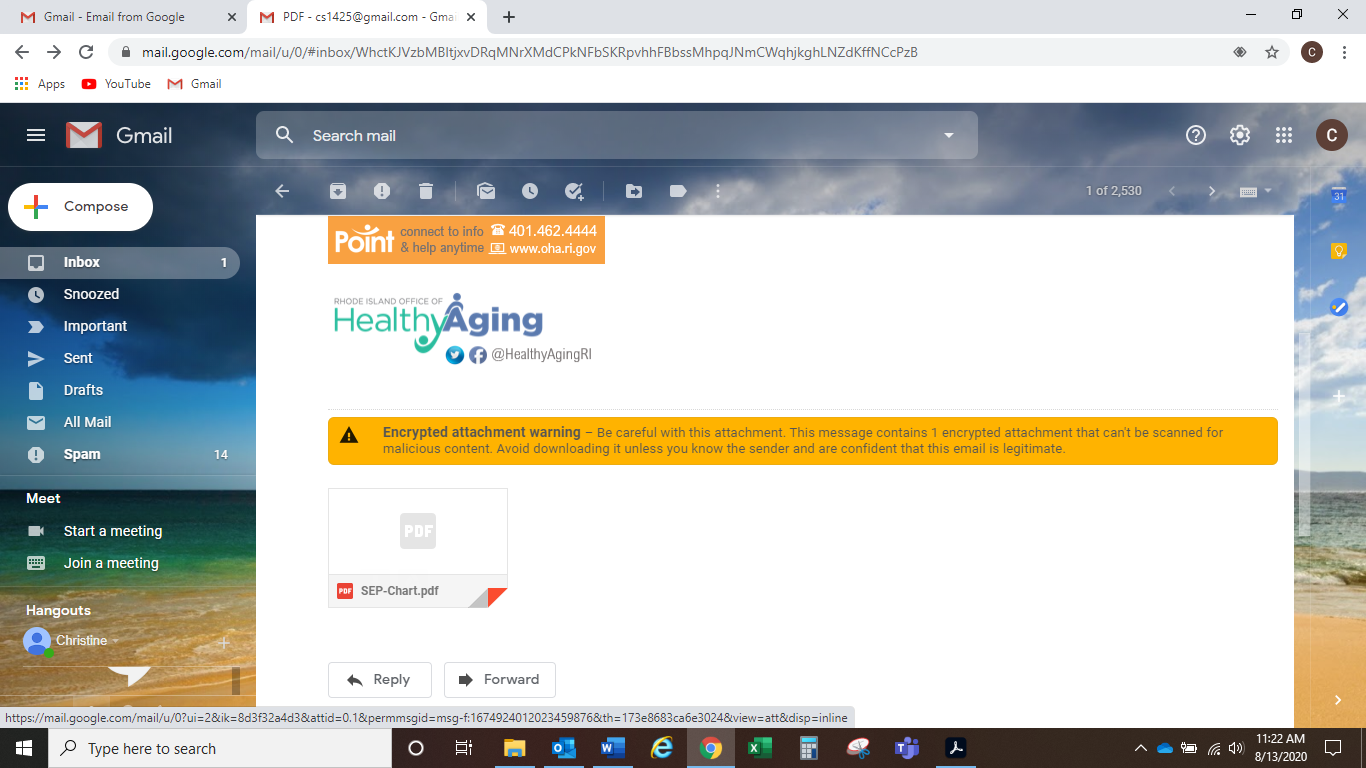
A screen shot of a computer error

Description automatically generated

### 

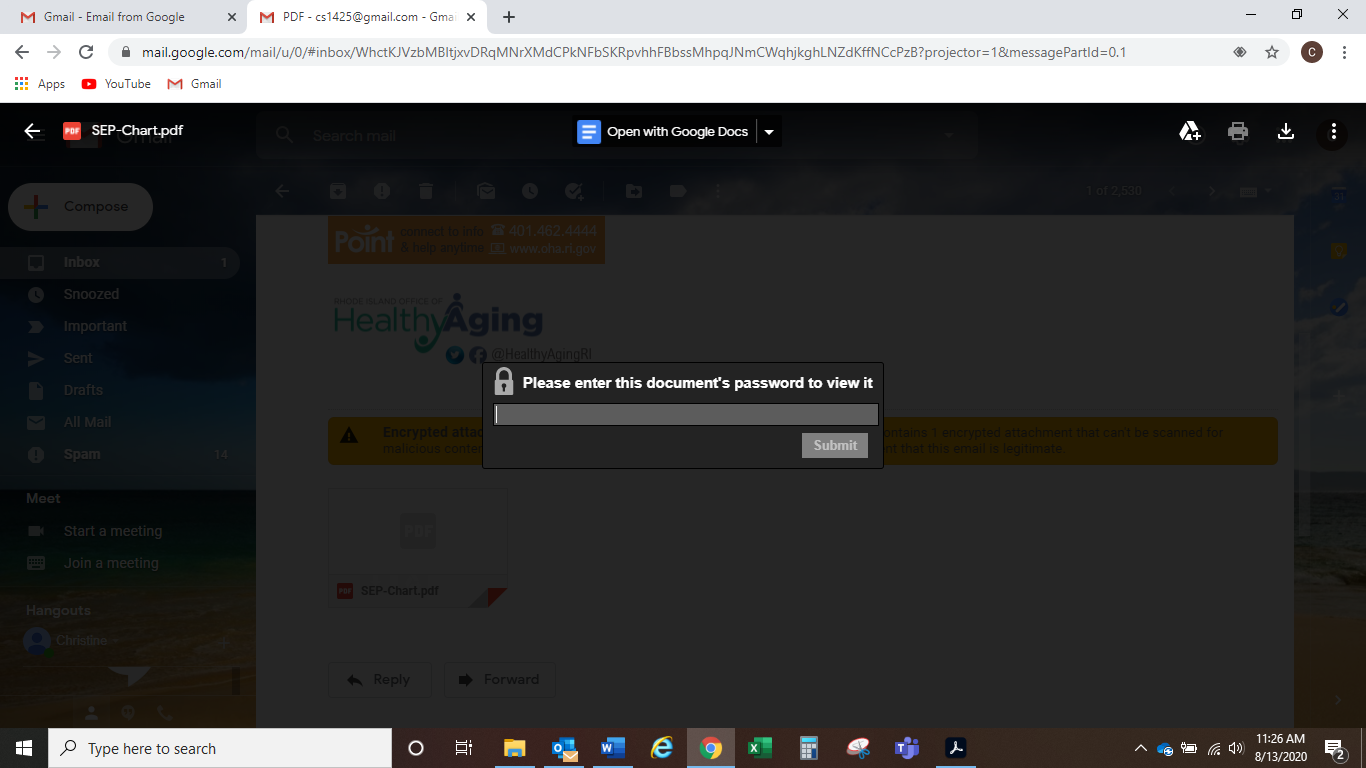
### Microsoft Word or Adobe PDF: Receiving a Password-Protected Document

1. When a team member sends a password-protected Word or PDF document as an attachment to an email, you will see a warning message similar to from the Gmail examples below. This lets you know the attachment is encrypted. 



1. You will need a password to view the attachment. You will receive the password in one of two ways.
   * + The team member will call you and tell you the password over the phone
     + The team member will send you a separate email with the password in it

**Note:** If you do not receive the password, reach out to the team member to have them resend it to you.

1. Once the email is received, open the attached Word document. You will receive the following pop-up. Enter the password in the open field and then click “Submit” to open the Word document.

# Tips for Privacy and Confidentiality: Online vs. Offline

There are tips and questions to consider related to privacy and confidentiality when working online vs. offline in programs where grantees and clients would typically meet face-to-face, in the same physical space.

Allowable or unallowable activities are often detailed in written policies and procedures for volunteers. For example, VRPM Policy 3.94 - Confidentiality is a required policy for SHIPs and SMPs. Volunteers are responsible for maintaining the confidentiality of all proprietary or privileged information to which they are exposed while serving as a volunteer, whether this information involves a member of staff, a volunteer, a beneficiary or other person, or involves the overall business of the SMP/SHIP.

The key to success for providing grantee activities virtually/remotely is to emphasize that the same confidentiality rules apply online as when people are face-to-face in your program. Also note that most of what you need to do online regarding safety and confidentiality involves following procedures, not simply installing or using an app.

### Considerations

* Look at your organization’s current policies and procedures. Do they already cover confidentiality, privacy, and safety? Do they cover permitted and prohibited online activities? Do they cover harassment and complaints processes? Do they need to be revised so that they apply both offline **and** online?
* Describe what a violation of confidentiality would look like, both online **and** offline.
* Describe what a violation of safety policies would look like, both online **and** offline.
* Describe what someone should do, in detail, if they observe a violation of safety or confidentiality.
* Consider whether volunteers should use their personal email account for client interactions or if they should create an email account that is used only for their volunteer work. Can your program provide volunteers with organizational email addresses? Consider requiring they only use a work email account when working for your program.
* Consider prohibiting team members from “friending” a client on social media platforms.
* Describe what a team member should do if a client starts commenting on their personal social media. Consider providing examples of how to diplomatically respond if this situation occurs.
* Consider whether team members should be required to have a password-protected computer or smart phone if they use one for your program. Could you provide guidance or examples on how to do this?
* Consider whether team members should or should not be allowed to use a public wi-fi network, even with a Virtual Private Network (VPN). When reading or responding to clients via email (at an airport, at a coffee shop, at the library, etc.) they should use a VPN and, if so, what would the cost be and will your IT staff be able to help install and support it?
* Consider policies or advice regarding what should be shown in the background on a video call with clients and other team members.
* Consider whether team members should use their own MS Teams, WebEx, GoToMeeting, Zoom account, etc. when working with clients or if your program will need to develop a platform that can be used.

### Tech Tips

* Ask team members if the software and operating systems on their computer, smart phone, and/or tablet automatically and regularly updates. If they are not sure, can an IT person from your program talk to them about their devices and determine the answer? It is important to remember that updating software and operating systems helps improve device security.
* Ask team members if their devices are password-protected and if anyone else has access to those devices. Could an IT person at your program walk them through how to password-protect their devices if needed?
* Ask team members if their home internet access is password-protected, how often they change the password, and how many people have access to their internet. Could an IT person at your program evaluate if they have enough security?

*This resource is supported by the Administration for Community Living (ACL), U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling $2,534,081 with 100% funding by ACL/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by ACL/HHS or the U.S. government.*

1. 1SHIP and SMP leaders can review the Information Technology Checklist in the SHIP and SMP Resource Libraries that was created to assist with developing state protocols. [↑](#footnote-ref-1)