

Dolphin Management Protected Trust Integration

March 2017

Patterson Dental Supply, Inc. *dba* Dolphin Imaging and Management Solutions
9200 Oakdale Avenue, Suite 500
Chatsworth, CA 91311
USA

Toll Free: 800.548.7241
Office: +1.818.435.1368
Fax: +1.818.435.1369

© 2016-2017 Dolphin Imaging and Management Solutions. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from Dolphin Imaging and Management Solutions.

The information furnished herein is believed to be accurate and reliable. However, no responsibility is assumed by Dolphin Imaging and Management Solutions for its use, nor for any infringements of patents or other rights of third parties resulting from its use. The operations of the program are subject to change without notice.

Dolphin is a trademark of Dolphin Imaging and Management Solutions. Microsoft, MS, MS-DOS, Windows, Microsoft Word, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Adobe, Acrobat, and Acrobat Reader are registered trademarks of Adobe Systems, Inc.

All other trademarks are the property of their respective owners.

Table of Contents

Introduction	5
Get Credential from Protected Trust	5
Dolphin Management Email Setup	7
Setting Message Policies	10
Default	11
Patient	12
Billing Party	13
Doctor	13
Sending Secured Email	14
What the Recipient Sees	14

Introduction

This guide describes how to set up and use Dolphin Management's integration with Protected Trust.

Protected Trust is a 3rd party email security system that when integrated with Dolphin Management, version 8, routes emails through a secure encrypted SMTP gateway. The recipient (patient, doctor, billing party, etc.) receives an email that provides a link to Protected Trust, where they can register for an account (if they don't already have one), enter in verification data, and view the message.

You can customize the security rules email recipients use for verifying their identity to Protected Trust. You can change these rules at any time, but the rules that go with the message stay with that message. In other words, if you send an email using one set of verification rules, then change the rules and send a new message, the new message uses the new rules, and the old message uses the rules in place when that message was sent. The recipient does not need to be aware of this because each message includes verification instructions.

Before using Dolphin's integration with Protected Trust, you must:

- Get an API Access Credential for your practice. (You get this from the Protected Trust WEB site, and it includes an access ID/user name and an access key/password.)
- Ensure that each user in your practice has an email address associated with that API Access Credential.
- Set up Message Policies in Protected Trust.

You have two options for using Protected Trust integration:

- Activate the integration in Dolphin, but use the message policy settings (verification rules for message recipients) already defined in your Protected Trust account.
- Activate the integration in Dolphin, and set up the message policies in Dolphin, which override what is defined in your Protected Trust account whenever you send an email from Dolphin.

Note: *You can also use Protected Trust with Dolphin Imaging, but there is no set up to perform in the Dolphin Imaging product. Protected Trust has a Microsoft Outlook-add-in that works with Dolphin Imaging.*

Get Credential from Protected Trust

If your practice does not have an account with Protected Trust, you can sign up at <https://www.protectedtrust.com/partners/Dolphin/>.

Once you have set up an account for your practice, you should have acquired the API Access Credential, user name and password, as shown in the example below:

Get Credential from Protected Trust

The screenshot shows the Dolphin Management interface. The top navigation bar includes 'Invite', 'Home', 'Compose', 'Inbox', 'Sent', and 'My Dashboard'. The user is logged in as 'Dustin Sprick'. The breadcrumb trail is 'My Dashboard > User List > API & SMTP Settings'. The main content area is titled 'API & SMTP Settings' and contains a link to 'Go to API & SMTP Documentation'. Below this is a section for 'Access Credentials' with a table of credentials.

Name	Access ID / Username	Access Key / Password	Created	Expires	
Daring Dolphin	Sw01X1110MR1DcrB	r113aPu163qkFTR164QY	1/20/2017	Never	Edit Delete

Keep the Access ID/User name and Access Key/Password handy because you need it to configure your employees' emails from Dolphin Management.

To set up Protected Trust message policies for integration with Dolphin Management:

- 1 From the **Settings** menu, navigate to **Message Policies**, as shown in the example below:

The screenshot shows the 'Message Policies' page in the Dolphin Management interface. The breadcrumb trail is 'My Dashboard > Settings > Message Policies'. The main content area is titled 'Message Policies' and contains a table of policies.

Icon	Name	
	Required Registration (Default) Enabled for All Users	Edit ↓
	Custom Message Policy 1 Enabled for All Users	Edit ↑

Note: Multiple policies and custom icons are supported by the web portal and the Outlook Add-in (version 4.4.5.0) and higher. Other applications (such as the iOS app and Virtual Printer) will use the default policy.

- 2 Click the **Edit** button for **Required Registration (Default)**.
- 3 On the **Message Security Settings** screen, complete the settings as shown for **Unregistered Recipient Identity Verification**:

Message Security Settings

Allow File Attachments	[Use System Default]	Edit
Allow Embedded Images	[Use System Default]	Edit
Encrypt Subject Line	[Use System Default]	Edit
Encrypted Subject Text	[Use System Default]	Edit
Unregistered Recipient Identity Verification	<p>This setting controls which identity verification methods are available to choose from when sending a message using this policy.</p> <p><input checked="" type="checkbox"/> Customize this setting</p> <p>Options</p> <p><input checked="" type="checkbox"/> Shared secret question & answer</p> <p><input checked="" type="checkbox"/> Phone verification</p> <p><input checked="" type="checkbox"/> No verification</p> <p>Default</p> <p>Require user to register ▼</p>	Done
Shared Secret Question	[Use System Default]	Edit
Shared Secret Answer Complexity	[Use System Default]	Edit
Message Expiration	[Use System Default]	Edit
Receipt Notification	[Use System Default]	Edit

Save Changes

- 4 Click **Save Changes**.

Dolphin Management Email Setup

To set up Dolphin's Protected Trust integration:

- 1 Log in to Dolphin Management and select **SMS/Email Manager** from the **Tools** menu.

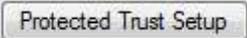
- 2 Select **Email Options** from the  pull-down menu.

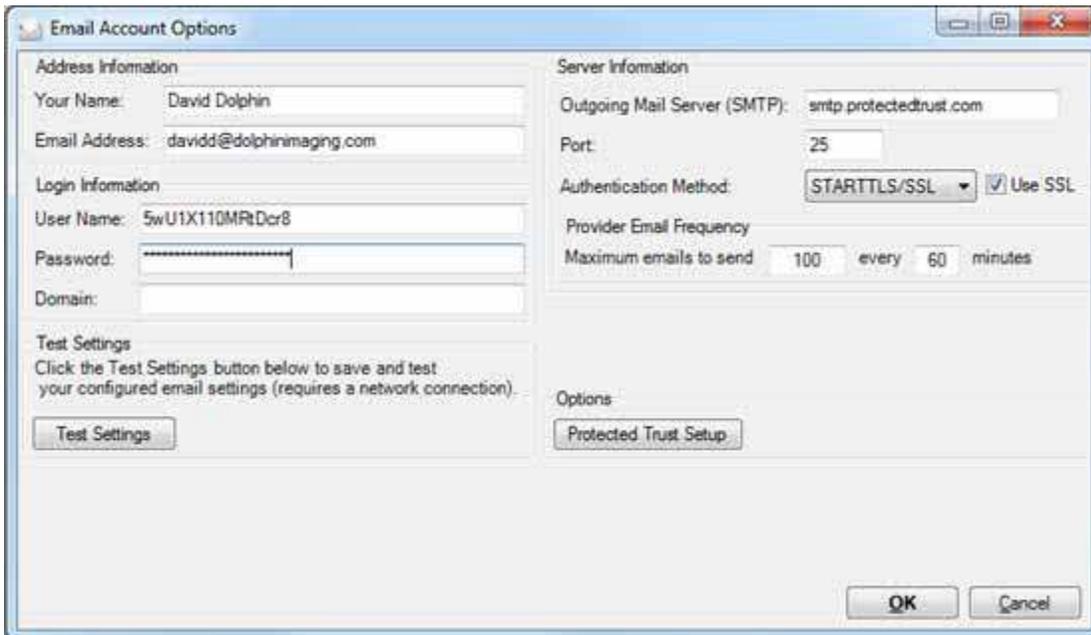
3 Complete the fields as follows:

- 4 In the **Address Information** group box, enter your name and email address.
- 5 In the **Login Information** group box, **User Name** field, enter the Protected Trust API Access ID.
- 6 In the **Password** field, enter the Protected Trust Access Key.
- 7 In the **Server Information** group box, complete the fields as follows:
 - a For **Outgoing Mail Server (SMTP)**, enter **smtp.protectedtrust.com**.

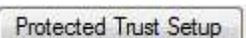
Dolphin Management Email Setup

- b For **Port**, enter **587**.
- c Select **STARTTLS/SSL** from the **Authentication Method** drop-down menu.
- d Click the **Use SSL** check box.

This causes the  button to appear.



The **Provider Email Frequency** is set to send a maximum of 100 emails every 60 minutes, but you can change this if you want.

- 8 Click the  button.

The first time you do this, the **Protected Trust Policy** message box opens. This reminds you to confirm that the following are correct on your Protected Trust account:

- The first policy under **Message Policies** is set to **Required Registration**.
- The following Message Security Settings option, Unregistered Recipient Identity Verification settings are checked: **Customize this setting, Shared secret question & answer, Phone verification, No verification, and Require user to register**. See “Get Credential from Protected Trust” on page 3-5 for more information.

- 9 Optional: Click the **Don't show me this again** check box
- 10 Click **OK** on the **Protected Trust Policy** message box.

The **Protected Trust Email Options** dialog box opens:

Protected Trust Email Options

Use Dolphin Management to Determine Policy Settings

Number of Days Until Message Expires: 0

Send Email When Recipient Views Message

Policy by Recipient Type:

- Default
- Patient
- Billing Party
- Doctor

Reset All to Default

Verification Options for Each Recipient Type:

No Verification

Registration Required

Phone Verification

Shared Secret Question and Answer

Secret Question Based on Recipient's Stored Data: Custom answer?

Secret Question Text:

Secret Answer: A1B2C3

OK Cancel

11 Do one of the following:

- Click **OK** to have Dolphin use the policy settings defined in Protected Trust.

There is nothing more you need to set up. Continue with “Sending Secured Email” on page 3-14 and “What the Recipient Sees” on page 3-14.

- To customize the message policies in Dolphin, and have Dolphin’s settings override what is in your Protected Trust account, click the **Use Dolphin Management to Determine Policy Settings** check box.

This activates the additional fields on [Protected Trust Email Options](#) dialog box:

The screenshot shows the 'Protected Trust Email Options' dialog box. It has a title bar with a shield icon and standard window controls. The main area contains several settings:

- Use Dolphin Management to Determine Policy Settings:** A checked checkbox.
- Number of Days Until Message Expires:** A spinner box set to '0'.
- Send Email When Recipient Views Message:** An unchecked checkbox.
- Policy by Recipient Type:** A list box with 'Default' selected. Other options are 'Patient', 'Billing Party', and 'Doctor'. A 'Reset All to Default' button is to the right.
- Verification Options for Each Recipient Type:** Four radio button options: 'No Verification', 'Registration Required' (selected), 'Phone Verification', and 'Shared Secret Question and Answer'.
- Secret Question Based on Recipient's Stored Data:** A dropdown menu set to 'Custom answer?'.
- Secret Question Text:** A text area containing 'Secret Question?'.
- Secret Answer:** A text box containing '123'.

At the bottom right, there are 'OK' and 'Cancel' buttons.

- Optional: Enter a value for [Number of Days Message Expires](#), or leave it at 0, which means use Protected Trust's message expiration policy.

Note: *Protected Trust's message expiration policy is based on the user's retention period after which the user can no longer access the message. Message retention periods vary depending upon what you purchase from Protected Trust. For more information, contact Protected Trust.*

- If you want to receive an email when the recipient views the message, click the [Send Email When Recipient Views Message](#) check box.
- Continue with [Setting Message Policies](#).

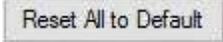
Setting Message Policies

Message policies describe how you want the primary email recipient to verify his or her identity before he or she can read an email sent via Protected Trust.

In Dolphin Management you can set up message policies for the following recipient types: Default, Patient, Billing Party, and Doctor. You must have at least a Default message policy configured, which Dolphin

Management sets to require registration with Protected Trust. If you keep that setting and configure nothing else, all email recipients (patient, billing party, doctor, or unknown) will be required to sign up with Protected Trust (or log in to Protected Trust, if they already have an account) before being able to view the email.

The following sections describe how to set up customized message policies for each recipient type, including Default.

Note: Click the  button if you want to reset the default policy settings for all email recipients (Registration Required).

Default

The default recipient type refers to the message policy Protected Trust uses for all recipients other than the primary recipient. Protected Trust also uses the default message policy when it cannot determine whether the email recipient is a patient, a billing party, or a doctor, or if you have not defined any other message policy.

To set the default message policy:

- 1 On the [Protected Trust Email Options](#) dialog box, [Policy by Recipient Type](#) list box, select **Default**.
- 2 Under [Verification Options for Each Recipient Type](#), select one of the following radio buttons:

No Verification

The email recipient can click on a link and read the secure email without having to verify his or her identity.

Registration Required

The email recipient must sign up with Protected Trust to view the secure email. This is the setting Dolphin Management uses if you do not specify a different option.

Shared Secret Question and Answer

The practice provides the email recipient with a question and answer that he or she can use to verify his or her identity.

When you select this option, the next three options become active.

Secret Question Based on Recipient's Stored Data

The only option available is **Custom answer**.

Secret Question Text

Enter the text you want to use when prompting the email recipient to enter the secret answer.

Secret Answer:

Enter the secret answer, which must have a minimum of 4 characters.

Patient

This section describes how to set up the message policy to use when the primary recipient is a patient. When you send a secure email to a patient, and you carbon copy other recipients as well, those other recipients identify themselves to Protected Trust using the Default policy, described in [Default](#) above. The patient, however is prompted based on the Patient message policy.

To set a patient message policy:

- 1 On the [Protected Trust Email Options](#) dialog box, [Policy by Recipient Type](#) list box, select **Patient**.

Note: *If you already completed the options for recipient type, Default, and then select Patient, the Default settings are automatically saved.*

- 2 Under [Verification options by recipient type](#), select one of the following radio buttons:

No Verification

The email recipient can click on a link and read the secure email without having to verify his or her identity.

Registration Required

The email recipient must sign up with Protected Trust to view the secure email. This is the setting Dolphin Management uses if you do not specify a different option.

Phone Verification

Send a verification code via voice or text to the email recipient. The recipient can then use this code to verify his or her identity and access the secure email.

If you select this option, when the primary recipient receives the email, he or she clicks on the link in the email to be prompted whether Protected Trust should send a verification code via text or voice to the phone number stored in Dolphin Management. After receiving the code, the recipient enters it to open the secure email.

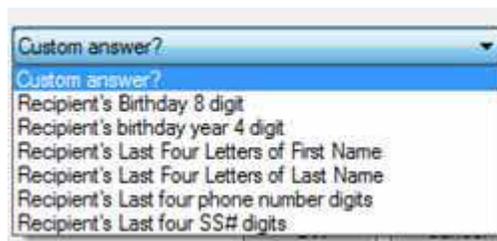
Shared Secret Question and Answer

The practice provides the email recipient with a question and answer that he or she can use to verify his or her identity.

When you select this option, the next three options become active.

Secret Question Based on Recipient's Stored Data

Select from one of the following options:



Secret Question Text

This field is completed for you based on the selection you make for **Secret Question Based on Recipient's Stored Data** above, however you can change it.

For example:

The image shows a screenshot of a web form. At the top, there is a dropdown menu with the text '8-digit Birthday' and a downward-pointing arrow. Below the dropdown is a text input field with the placeholder text 'When were you bom? MMDDYYYY' and an example '(Example: 01151980)'. The input field has small upward and downward arrows on its right side, indicating it is a text input.

Secret Answer:

Activated only if you select **Custom answer?** above, enter the secret answer, which must have a minimum of 4 characters.

The shared secret answer would be the same for all recipients of the type you are defining here.

For example, for all patient recipients, the secret answer might be: ***lflosstwicedaily***. Your practice can define a different custom secret answer for each policy recipient type.

Billing Party

This section describes how to set up the message policy to use when the primary recipient is a billing party. When you send a secure email to a billing party, and you carbon copy other recipients as well, those other recipients identify themselves to Protected Trust using the Default policy, described in [Default](#) above. The billing party, however is prompted based on the Billing Party message policy.

To set a billing party message policy:

- 1 On the [Protected Trust Email Options](#) dialog box, [Policy by Recipient Type](#) list box, select **Billing Party**.
Note: *If you already completed the options for recipient type, Patient, and then select Billing Party, the Patient settings are automatically saved.*
- 2 Follow the directions for this step under “Patient” on page 3-12.

Doctor

This section describes how to set up the message policy to use when the primary recipient is a doctor. When you send a secure email to a doctor, and you carbon copy other recipients as well, those other recipients identify themselves to Protected Trust using the Default policy, described in “Default” on page 3-11 above. The doctor, however, is prompted based on the Doctor message policy.

To set a doctor message policy:

- 1 On the [Protected Trust Email Options](#) dialog box, [Policy by Recipient Type](#) list box, select **Doctor**.
Note: *If you already completed the options for recipient type, Billing Party, and then select Doctor, the Billing Party settings are automatically saved.*

Sending Secured Email

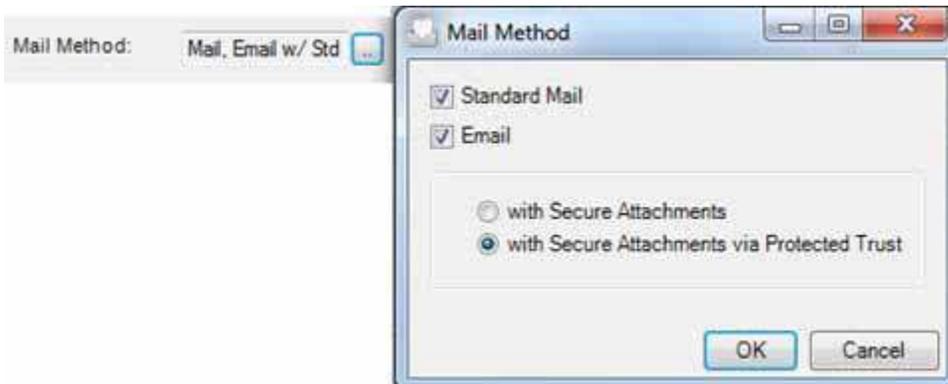
- 2 Follow the directions for this step under “Patient” on page 3-12.

Sending Secured Email

Once the integration with Protected Trust has been set up, you can send secure emails to everyone in your database.

For each entity in your database:

- 1 Open the [Mail Method](#) dialog box:



The option, [with Secure Attachments via Protected Trust](#) should already be selected providing you have set up the integration correctly.

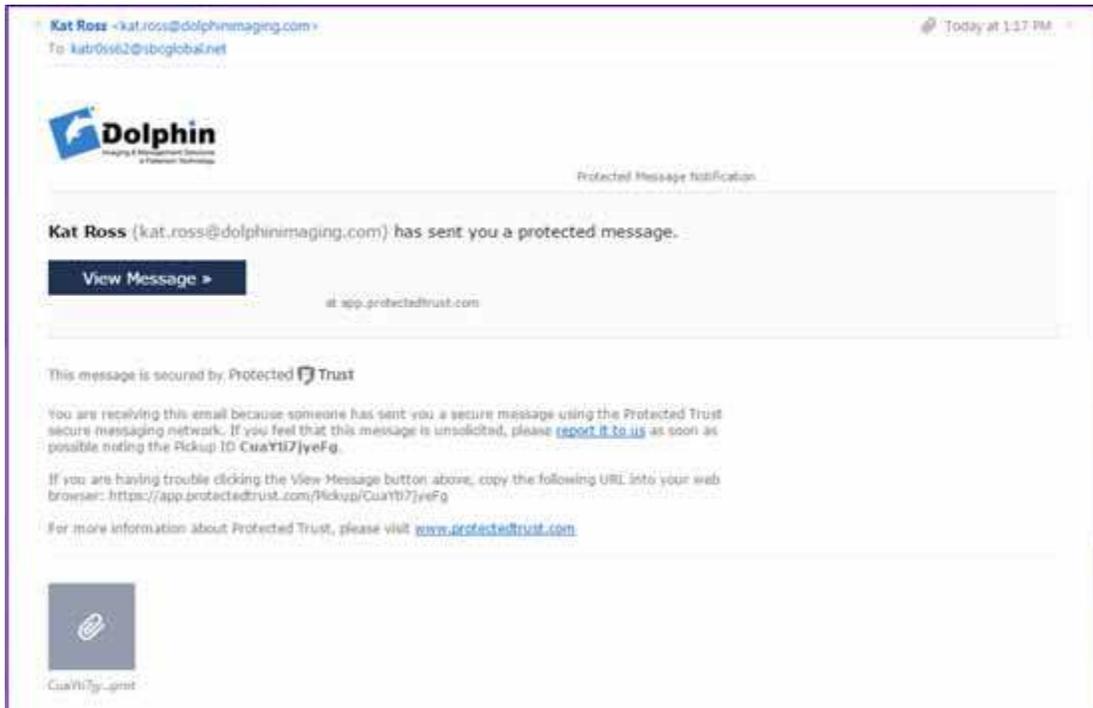
- 2 Click **OK**.

To send secure email to a patient:

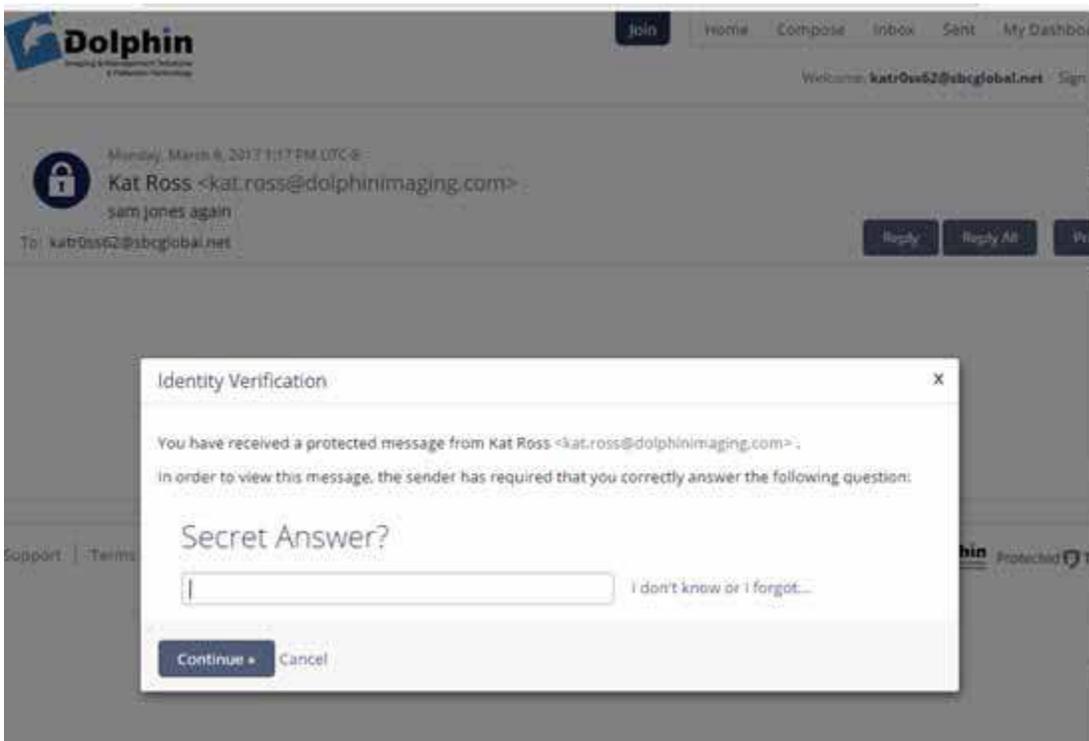
- 1 From the [Edit a Patient](#), [Patient](#) tab, [Email Address](#) field, right-click on the patient’s email address, and select **Send Message**.
- 2 When the [Email Settings](#) dialog box opens, enter the text of the message and include any attachments you want to send.
- 3 Click **OK** to send the message.

What the Recipient Sees

The screens below show an example of what the email recipient sees when opening an email from Protected Trust that requires the recipient to verify his or her identity:



- If the policy requires a secret answer:
 - a The email recipient clicks **View Message** and is prompted:



What the Recipient Sees

- b The email recipient enters the required secret answer, and clicks **Continue**.

The secure email opens, and if there are attachments associated with it, the recipient can download and open them.

- If the policy requires the email recipient to sign-in to Protected Trust, and the recipient already has a Protected Trust account:

- a The email recipient clicks **View Message** and is prompted:

The screenshot shows the Protected Trust sign-in interface. At the top left is the Dolphin logo. The top navigation bar includes 'Home', 'Compose', 'Inbox', 'Sent', and 'My Dashboard'. A user is logged in as 'kat.ross@dolphinimaging.com'. The main content area is split into two columns. The left column contains a welcome message and a sign-in prompt. The right column is titled 'Sign In' and contains a form with fields for 'Your e-mail address' (pre-filled with 'kat.ross@dolphinimaging.com') and 'Password'. There are also buttons for 'Sign In', 'Keep me signed in', and 'Use different account'.

- b The email recipient logs in to his or her Protected Trust account.

The secure email opens, and if there are attachments associated with it, the email recipient can download and open them.

- If the policy requires the email recipient to register with Protected Trust:

- a The email recipient clicks **View Message** and is prompted:

Dolphin
Imaging & Management Solutions
a Pathstream Technology

Home Compose Inbox Sent My Dashboard

Welcome, **katross62@sbcglobal.net** Sign Out

1 Register for email encryption 2 View protected message

Trouble registering?
Please [contact support](#) for assistance.

Fields marked with * are required.

Instructions **Kat Ross** (kat.ross@dolphinimaging.com) has sent you a protected message.
To view the message, please register your free guest account. Next time, you can sign in with your new password.

Name* First Last

Choose a Password* New Password Re-type New Password

- Must be at least 6 characters long
- Must have at least 1 number

Account Recovery* If you forget your password or become locked out of your account, we will use this phone to help you reset your password.

+1 (USA) Country code Phone number Optional area

Verify Phone >

Account Information You are registering for a guest account. How will you be using email encryption?

For Business Personal Use

Company Name Industry

Contact Phone

This software is licensed to you subject to the [Protected Trust Terms and Policies](#).

Register >

Support Terms and Policies

Dolphin Protected Trust

- b The email recipient completes the information and registers with Protected Trust.

The secure email opens, and if there are attachments associated with it, the email recipient can download and open them.

What the Recipient Sees

The screenshot shows the Dolphin email interface. At the top left is the Dolphin logo with the tagline 'Images & Management Systems of Patient Technology'. To the right are navigation links: 'Invite', 'Home', 'Compose', 'Inbox', 'Sent', and 'My Dashboard'. A user greeting 'Welcome, Kat Ross' and a 'Sign Out' link are on the far right.

The main content area shows an email header for 'Monday, March 6, 2017, 11:50 AM UTC-8'. The sender is 'Kat Ross <kat.ross@dolphinimaging.com>' and the recipient is 'from sam jones'. The subject is 'To: Kat Ross <kat.ross@dolphinimaging.com>'. Action buttons for 'Reply', 'Reply All', 'Forward', and 'Print' are visible.

The message content includes an attachment 'Readme First (304 KB)' and the text 'readmefirst'. Below this are tabs for 'Delivery Status' and 'Proof of Delivery Log'. A 'Show: All' dropdown and a search box 'Search by email address...' are present.

Recipient	Status
kat.ross@dolphinimaging.com	Viewed Today 11:51 AM

At the bottom of the message area is a link: 'Revoke All Recipients & Sender'. The footer contains 'Support | Terms and Policies' on the left and the Dolphin logo with 'Protected Trust' on the right.