

MEDCURITY

User Guide

This in-depth guide is intended to assist Users in navigating the various features of Medcurity from registering as a new customer through completion of the Security Risk Analysis, updating the Worklist, customization of Policies & Procedures, and management of Business Associate Agreements.

Contents

- Navigation and Setup..... 3**
 - Dashboard..... 3
 - User Profile 8
 - Company Profile 9
 - Manage Locations 11
 - Manage Users..... 13
 - Purchase 16
 - Make Payment..... 17
- Utilizing the Tools18**
 - Complete the Security Risk Analysis..... 18
 - Dashboard..... 19
 - Assessment 22
 - Review the Worklist..... 27
 - Download or Print Documentation 29
 - Walkthrough..... 29
 - Policies and Procedures 31
 - Customize a Policy 32
 - Create a Policy 37
 - Appendices..... 39
 - Customizing an Appendix..... 39
 - Editing an Appendix 42
 - Business Associate Agreements..... 43
 - Types of BAAs 44
 - Upload a BAA 48
 - Managing BAAs..... 49
- Contact Us52**

Navigation and Setup

Dashboard

From the Medcurity dashboard you can access your Security Risk Analysis (SRA), Policies and Procedures (P+P), and Business Associate Agreements (BAA).

To access the Dashboard:

1. Login to your Medcurity account
2. Click the menu icon in the upper right-hand corner
3. Select Dashboard



Welcome to the Dashboard

Navigate between tabs to access any of the three tools. From each tab, you can edit, view, or print the documents.

On the **Security Risk Analysis** tab, you will see the status of your current SRA. If you have past SRAs they will appear on the Security Risk Analysis tab listed by year, under your most current SRA.

Security Risk Analysis | Policies and Procedures | BAAs

2019 HIPAA Security Risk Assessment

Demo Clinic

[Finalize Assessment](#)

Questions OPEN	104	Questions ANSWERED	24	Percentage ANSWERED	19%
----------------	-----	--------------------	----	---------------------	-----

To access questions in a specific section of your assessment, please select from the links below.

Assessment Sections

[▶ Administrative](#) (6/68 answered) | [▶ Physical](#) (10/10 answered) | [▶ Technical](#) (4/26 answered)

[▶ Access Full Survey](#)

Walkthroughs

Select a Location: 1 of 10 locations used | [Add a Location](#)

Last Updates: Oct 31, 2019 | Updated by: April Needham

On the **Policies and Procedures** tab, you will see the status of each policy and procedure. To preview, edit, print, or approve, click on the appropriate policy and procedure to expand the list of options.

Once policies and procedures have been approved, they will appear on a website where your workforce members can view them. To see this view, click the Public View button in the upper right-hand corner.

The screenshot shows a web interface with three tabs: "Security Risk Analysis", "Policies and Procedures", and "BAAs". The "Policies and Procedures" tab is active. In the top right corner, there are two buttons: "Public View" and "Expand All". Below the tabs, there is a list of five policy entries, each with a title, a status indicator (a colored circle), and a "Next Renewal Date".

Policy Title	Status	Next Renewal Date
00-Information Security Policy	Not Started	N/A
01-Introduction to the Information Security Policy	Not Started	N/A
02-Security Management Process	Not Started	N/A
03-Workforce Security	In Progress	N/A
04-Sanctions	Approved	10/30/2020

The "03-Workforce Security" entry is expanded, showing a detailed view with the title "03-Workforce Security", the text "Last Updated: 10/30/2019 3:23pm", and four action buttons: "Approve" (with a checkmark icon), "Preview", "Print", and "Edit".

At the bottom of the Policies and Procedures screen, you'll find the option to Add a Custom Policy. Selecting this option enables you to upload your own policy or customize a Medcurity policy.

Below the Custom Policy option, you can see the library of Appendices that accompany the Policies and Procedures. Click on any Appendix to view, edit, or save the file.

The screenshot displays a user interface for managing policies and procedures. At the top, there is a card for a policy titled "12-Breach Notification" with a status of "Not Started" and a "Next Renewal Date: N/A". Below this is a dashed green box containing a "+ Add Custom Policy" button. Underneath is a section titled "Appendices" which contains four items, each with a file icon and a title: "Appendix A - Risk Management Team Meeting Attendance Log" (Excel icon), "Appendix B - Audit Log" (Excel icon), "Appendix C - Confidentiality Statement" (Word icon), and "Appendix D - Network Access Request" (Word icon).

On the **BAAs** tab, you will see the status of each Business Associate Agreement (BAA). To preview, edit, print, or approve, click on the appropriate BAA to expand the list of options.

At the bottom of the BAAs screen, you'll find the option to Add Business Associate. Selecting this option enables you to upload your own BAA or customize a Medcurity BAA.

The screenshot displays the 'BAAs' tab interface. At the top, there are three tabs: 'Security Risk Analysis', 'Policies and Procedures', and 'BAAs'. Below the tabs is a list of Business Associate Agreements. The first entry is 'Business Associate Agreement' with a status of 'In Progress' and a 'Next Renewal Date: N/A'. The second entry is 'Business Associate Agreement' with a status of 'Approved' and a 'Next Renewal Date: 10/30/2020'. Below the second entry, a detailed view of a BAA is shown, including the title 'Business Associate Agreement', the last updated date '10/30/2019 3:28pm', and four action buttons: 'Preview', 'Print', 'Email 0 Associates', and 'Edit'. At the bottom of the screen, there is a dashed green box containing a green plus sign and the text '+ Add Business Associate'.

User Profile

When you click on User Profile you can update your name, job title, email, phone number, and password.

USER PROFILE

Welcome  ▼ April Needham ▼

USER INFORMATION

First Name	Last Name
<input type="text" value="April"/>	<input type="text" value="Needham"/>
Title	Phone Number
<input type="text" value="Program Director"/>	<input type="text" value="509-368-9301"/>

LOGIN CREDENTIALS

Your email address will be assigned as your Medcurity username. To update your password, please enter and verify your new password and click Submit.

Email

Password

Verify Password

Company Profile

When you access the Dashboard for the first time, you will be prompted for additional information about the Company, a color to associate with your documents, and the company's logo. These will be incorporated in final SRA documents, Policies and Procedures, and BAAs.

COMPANY PROFILE

Welcome
Demo Clinic A ▼

A company logo and brand color is required

COMPANY INFORMATION

Name	Company Abbreviation	
<input type="text" value="Demo Clinic A"/>	<input type="text"/>	
Legal Name	<input type="text"/>	
Address	Address Ext.	
<input type="text" value="905 W Riverside Avenue"/>	<input type="text"/>	
City	State	Zip
<input type="text" value="Spokane"/>	<input type="text" value="WA"/>	<input type="text" value="99201"/>

EXTRA DETAILS

Brand Color

Logo

Images should be 500px wide and in a .jpg, .png, or .gif format

No file chosen

Company Size

Once completed, the Company Profile page will also show Order History.

COMPANY PROFILE

Welcome
Demo Clinic A ▼

Company profile updated.

ACCOUNT INFORMATION

Demo Clinic A

Address
905 W Riverside Avenue
Spokane WA, 99201

Company Size:
251-500

Logo:



[Edit](#)

ORDER HISTORY

November 25th, 2019 - \$0.00 Invoice	
Security Risk Assessment	\$3,600.00
Policies and Procedures	\$3,000.00

Manage Locations

Use the **Manage Locations** option when your company has more than one location requiring a walkthrough. Adding a location creates a separate set of walkthrough questions for each location.

Select **Manage Locations** from the menu in the upper right-hand corner. Add or remove locations as appropriate. To add, type the name of the location. To remove, click the X next to the location name. Once location information is complete, click **Save Changes**.

2019 HIPAA Security Risk Assessment - MANAGE LOCATIONS

DIRECTIONS: To activate one of your purchased location credits please assign it a name below. Once a department has been named, click Save Changes and it will be available to use in the Walkthrough section of the assessment. Location names may be edited by following the same process.

Locations will remain inactive until named. Named Locations can be deactivated by clicking the "X" next to them.

Location 1	<input type="text" value="default"/> X	Location 2	<input type="text"/> X
Location 3	<input type="text"/> X	Location 4	<input type="text"/> X
Location 5	<input type="text"/> X	Location 6	<input type="text"/> X
Location 7	<input type="text"/> X	Location 8	<input type="text"/> X
Location 9	<input type="text"/> X	Location 10	<input type="text"/> X

▼

[Save Changes](#)

If you have more than ten locations, scroll down to the **Add Additional Locations** section and follow the instructions found there.

Add Additional Locations

To add additional locations for your organization please enter the quantity you would like to add below. You will be given the option to activate them immediately by assigning a name right away, or you can activate them at a later time by using the location manager above.

Please enter the number of additional locations you would like to add:

Quantity

Manage Users

Once registration is completed, individual users will need to be set up and granted the appropriate level of access to the assessment.

Two levels of permission are available - Admin or General User.

To add a user, select **Manage Users** from the menu in the upper right-hand corner. Enter the person's name and email and select Admin or General User.

Permission Levels

Admin

Admin User will have full read/write permissions on all purchased products with the following additional permissions:

- Finalize Risk Analysis
- Approve Policies or BAAs
- Manage Company Profile
- Manage Users
- Purchase Additional Products
- Manage Payment Information

General User

General User will have limited read/write permissions on all purchased products with permission to:

- Answer questions
- Update Risk Analysis Recommendations
- Leave Comments

Add User Manage

First Name

Last Name

Email

Admin General User

When setting up permissions for a **General User**, you'll also need to select which assessment you are assigning them to as well as which sections of that assessment they should have access to. If granted access to a Walkthrough, you'll need to designate the proper locations.

Permission Levels

Admin

Admin User will have full read/write permissions on all purchased products with the following additional permissions:

- Finalize Risk Analysis
- Approve Policies or BAAs
- Manage Company Profile
- Manage Users
- Purchase Additional Products
- Manage Payment Information

General User

General User will have limited read/write permissions on all purchased products with permission to:

- Answer questions
- Update Risk Analysis Recommendations
- Leave Comments

Add User Manage

First Name	Last Name	Email	Admin	General User
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>

Available Assessment:

Demo HIPAA Security Risk Assessment	2019 HIPAA Security Risk Assessment
<input type="radio"/>	<input checked="" type="radio"/>

Choose the section(s) you would like to assign to this user:

All	Administrative	Physical	Technical	Walkthrough
<input type="checkbox"/>				

Submit Changes

To make changes to a user's access, select the **Manage** tab. From here, you can edit the employee's name or email or delete them as a user, if necessary.

Permission Levels

Admin
Admin User will have full read/write permissions on all purchased products with the following additional permissions:

- Finalize Risk Analysis
- Approve Policies or BAAs
- Manage Company Profile
- Manage Users
- Purchase Additional Products
- Manage Payment Information

General User
General User will have limited read/write permissions on all purchased products with permission to:

- Answer questions
- Update Risk Analysis Recommendations
- Leave Comments

Add User **Manage**

FIRST NAME	LAST NAME	EMAIL		
April	Needham	apriln@medcurity.com	Delete	Manage

Purchase

Once you have purchased a plan, you can select the **Purchase** option from the Dashboard to add additional products to your account. For example, if you currently use only the SRA product and have decided to add more tools by incorporating Medcurity's Policies and Procedures into your organization, select **Policies and Procedures** and select **Checkout**. This will lead you to our payment options screen. Pricing will vary depending on the size of your Client's organization.

Welcome to Medcurity

Thank you for registering your organization with Medcurity. The next step is to purchase your first assessment. To get started, please select the appropriate plan for your organization from the available options.

For additional assistance please feel free to contact us.

To Get Started

Please select a plan:

Security Risk Assessment

Annual HIPAA Risk Assessment with Medcurity®

\$3600.00/Year

Policies and Procedures

Policies and Procedures Subscription

\$3000.00/Year

BAA

BAA Subscription

\$1500.00/Year

Please select a plan to checkout

Make Payment

Select the **Payment Method**, enter your payment information then click **Submit**.

Payment Method

Credit ACH Check/Invoice

Please enter your card information:

Credit/Debit Card Number

Expiration MM/YY CVC

Auto Renew?

If paying by credit card, your access will be immediate. When paying by invoice, access will be granted after payment is received.

Payment Method

Credit ACH **Check/Invoice**

By selecting this option you are requesting to submit payment via an invoicing process. A representative from Medcurity will provide an invoice for purchase within 1-2 business days. Once payment is received your assessment will be activated by a Medcurity representative.

Utilizing the Tools

Complete the Security Risk Analysis

The Assessment has four parts – Administrative, Physical, Technical, and Walkthroughs.

Administrative Safeguards focus on the organization's policies, procedures, and security measures that protect Protected Health Information (PHI). The goal is to ensure patient data is correct and accessible to authorized parties.

Physical Safeguards focus on the physical access to PHI. They establish how devices store PHI and how they are protected to prevent physical theft and loss of devices.

Technical Safeguards focus on protecting electronic PHI and controlling access to it. These contain technology-related measures to guard your networks and devices from data breaches and unauthorized access.

On-Site Walkthrough is the process designed to watch employees in action. This is accomplished by conducting a walkthrough using a checklist that helps you compare security requirements with actual employee practices. In the current version of Medcurity, we recommend you use the paper checklist provided on the last page of the guide and then transfer the answers to the tool. We recommend performing this once during business hours and once after business hours. Best practice is to not announce when these walkthroughs will be conducted in order to provide the most accurate measure of policy and procedure implementation in the field.

NOTE: "Yes" answers in this category indicate opportunities for improvement.

Dashboard

Access the **Dashboard** from the menu in the upper right-hand corner.

The Security Risk Analysis (SRA) tab is divided into three sections which provide a snapshot of your progress and links to the actual SRA and Walkthroughs.

The first section provides an overview of the current SRA. You will see the total number of questions divided into two categories – Open and Closed. Open questions still need to be answered while Closed questions have been completed. Questions in either category can be edited until the assessment is finalized. The Percentage Answered illustrates how much of the SRA is complete.

The screenshot shows a dashboard for a "2019 HIPAA Security Risk Assessment" for "Demo Clinic A". At the top, there are two tabs: "Security Risk Analysis" (active) and "Policies and Procedures". The main title "2019 HIPAA Security Risk Assessment" is in blue, with "Demo Clinic A" below it. A blue button labeled "Finalize Assessment" is on the right. Below this, three statistics are displayed: "Questions OPEN 215" (with a yellow vertical bar on the left), "Questions ANSWERED 9" (in green), and "Percentage ANSWERED 5%" (in blue). A message states: "To access questions in a specific section of your assessment, please select from the links below." Under "Assessment Sections", there are three options: "Administrative" (5/68 answered), "Physical" (2/10 answered), and "Technical" (2/26 answered). A green link "Access Full Survey" is also present. The "Walkthroughs" section includes a "Select a Location" dropdown (showing "2 of 10 locations used") and an "Add a Location" button. At the bottom, it says "Last Updates: Nov 26, 2019 | Updated by: April Needham".

In the second section, you will see links to the three sections of the SRA - Administrative, Physical, and Technical. If you would like to view your full assessment, click on the Access Full Survey link.

The screenshot displays the '2019 HIPAA Security Risk Assessment' for 'Demo Clinic A'. At the top, there are tabs for 'Security Risk Analysis' and 'Policies and Procedures'. The main header includes the title '2019 HIPAA Security Risk Assessment' and a 'Finalize Assessment' button. Below this, a summary shows 'Questions OPEN 215', 'Questions ANSWERED 9', and 'Percentage ANSWERED 5%'. A message states: 'To access questions in a specific section of your assessment, please select from the links below.' The 'Assessment Sections' section features three cards: 'Administrative' (5/68 answered), 'Physical' (2/10 answered), and 'Technical' (2/26 answered). A yellow 'Access Full Survey' button is visible. The 'Walkthroughs' section includes a 'Select a Location' dropdown (2 of 10 locations used) and an 'Add a Location' button. At the bottom, it notes 'Last Updates: Nov 26, 2019 | Updated by: April Needham'.

The last section the SRA is Walkthroughs. Here you will find the locations associated with your Medcurity account.

The screenshot displays the '2019 HIPAA Security Risk Assessment' for 'Demo Clinic A'. At the top, there are tabs for 'Security Risk Analysis' and 'Policies and Procedures'. The main header includes the assessment title and a 'Finalize Assessment' button. Below this, a summary shows 215 open questions, 9 answered questions, and 5% completion. A message instructs the user to select a section to access questions. The 'Assessment Sections' are listed as Administrative (5/68 answered), Physical (2/10 answered), and Technical (2/26 answered), with an 'Access Full Survey' link. The 'Walkthroughs' section features a 'Select a Location' dropdown (showing '2 of 10 locations used') and an 'Add a Location' button. At the bottom, it notes 'Last Updates: Nov 26, 2019 | Updated by: April Needham'.

On the bottom of this screen, you will see when the SRA was last updated and by whom.

Assessment

Sections of the SRA can be completed in the order you choose. Once you click on **Administrative**, **Physical**, or **Technical**, you will be guided through questions pertaining to that part of your business. When all questions in a section have been completed, the tool will automatically move into the next section.

Sections of the SRA can be assigned to specific users. See instructions under Managing Users.

Decide which section of the SRA you'd like to begin and select it from the **Assessment Sections** on the Dashboard.

The screenshot displays the '2019 HIPAA Security Risk Assessment' dashboard for 'Demo Clinic A'. At the top, there are tabs for 'Security Risk Analysis' and 'Policies and Procedures'. The main header includes the title '2019 HIPAA Security Risk Assessment' and a 'Finalize Assessment' button. Below this, a summary row shows 'Questions OPEN 215', 'Questions ANSWERED 9', and 'Percentage ANSWERED 5%'. A message states: 'To access questions in a specific section of your assessment, please select from the links below.' The 'Assessment Sections' section is highlighted in yellow and includes three options: 'Administrative' (5/68 answered), 'Physical' (2/10 answered), and 'Technical' (2/26 answered). There is also a link for 'Access Full Survey'. The 'Walkthroughs' section includes a 'Select a Location' dropdown (showing '2 of 10 locations used') and an 'Add a Location' button. At the bottom, it notes 'Last Updates: Nov 26, 2019 | Updated by: April Needham'.

Questions will be listed on the **Open** tab or the **Answered** tab, depending on status. To navigate to the next question, select the question from the list on the left-hand side of the screen or select **Next Question** in the bottom right-hand corner.

You can also navigate between questions using hot keys:

- MAC
 - Command + P for Previous Question
 - Command + N for Next Question
- Windows
 - Shift + P for Previous Question
 - Shift + N for Previous Question

You can access definitions and explanations for each question by clicking on the blue circle at the end of the question or the white circle following **Impact of Risk** and **Likelihood**.

There is a link to the Code of Federal Regulations (CFR) in the upper right-hand corner underneath **HIPAA Citation**.

The screenshot shows the Medcurity assessment interface for Demo Clinic A. The interface is divided into two main sections: a list of questions on the left and a detailed view of the selected question on the right. The left section has tabs for 'OPEN' and 'ANSWERED' questions, and a sub-tab for 'ADMINISTRATIVE' questions. The right section displays 'Question 4' with the text: 'Do you have policies and procedures to periodically monitor and evaluate security of your organization's PHI? This may be in your Security Plan.' Below the question text are several input fields: 'ANSWERS' with radio buttons for Yes, No, Partial, and N/A; 'IMPACT OF RISK' with radio buttons for Low, Medium, and High; and 'LIKELIHOOD' with radio buttons for Low, Medium, and High. There is a 'DETAILS' field for entering comments. At the bottom of the question view, there is an 'ASSOCIATED POLICIES' section with checkboxes for '01-Introduction to the Information Security Policy', '02-Security Management Process', and '05-Security Awareness and Training'. Navigation buttons for 'Previous Question' and 'Next Question' are located at the bottom of the interface, along with a progress indicator '4 of 224'. A 'HIPAA Citation' link is visible in the top right corner of the question view.

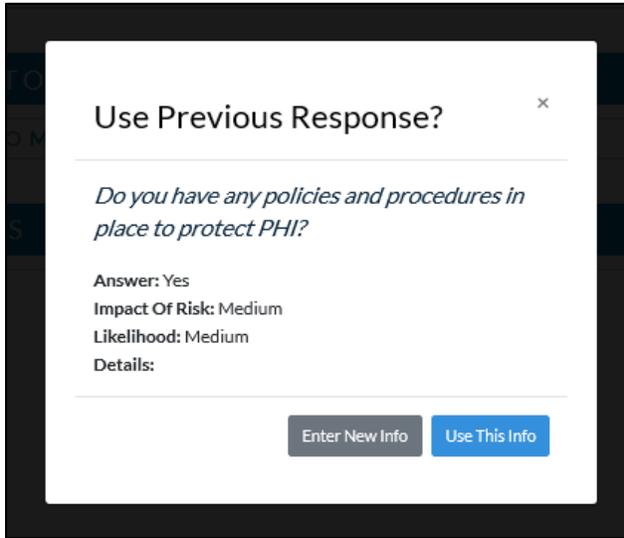
When completing questions, select the answer (Yes, No, Partial, or N/A) that best fits your company's current practices. Select the appropriate **Impact of Risk** and **Likelihood** then enter any comments or notes in the **Details** field.

If you have purchased Medcurity's Policies and Procedures, you can choose which Policy(s) you would like to link to each question by selecting the box next to the appropriate Policy(s). Policies that your organization has uploaded will also appear in the list, once approved. Only policies that have been approved will appear in this list.

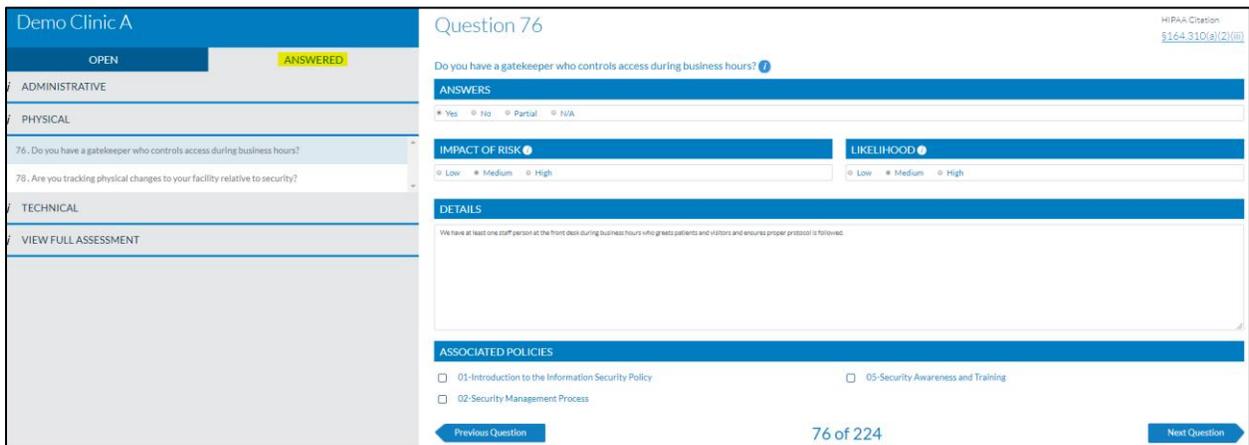
An important feature to note is that once you click **Next Question**, your answers are automatically saved. These answers can be edited until the assessment is finalized.

If you have completed an SRA with Medcurity in the past, you will have the option to populate the current assessment with answers from your most recent SRA. In your new

assessment, you will be prompted to maintain the response from the previous year's assessment or update the response. If you choose "Use This Info," you may still edit the answers.



To go back and view questions that have been answered, click on the Answered tab.



If you have not purchased Medcurity's Policies and Procedures, there will be a link you can follow at the bottom of each question that will enable you to upgrade your subscription by purchasing Policies and Procedures.

ASSOCIATED POLICIES (NOT ENABLED)

You do not have an active policy subscription. Purchasing one will allow you to link your policies to your assessment questions to better clarify your answers.
Purchase a subscription to enable.

[Previous Question](#) 1 of 152 [Next Question](#)

When all questions in all sections have been answered, complete the assessment by clicking **Finalize Assessment**. Once finalized, you cannot reopen the assessment. It is also important to note that the Security Risk Assessment Completion date reflects the date that the **Finalize Assessment** button is selected.

Security Risk Analysis | Policies and Procedures

2019 HIPAA Security Risk Assessment

Demo Clinic A [Finalize Assessment](#)

Questions OPEN	215	Questions ANSWERED	9	Percentage ANSWERED	5%
----------------	-----	--------------------	---	---------------------	----

To access questions in a specific section of your assessment, please select from the links below.

Assessment Sections [Access Full Survey](#)

Administrative 5/68 answered	Physical 2/10 answered	Technical 2/26 answered
---	---	--

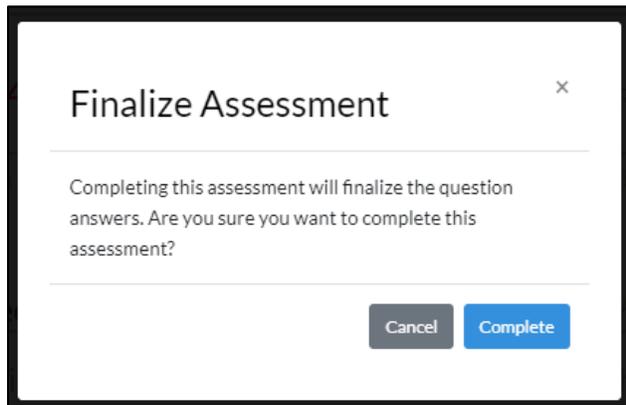
Walkthroughs

Select a Location [Add a Location](#)

2 of 10 locations used

Last Updates: Nov 26, 2019 | Updated by: April Needham

You will be asked to confirm that you want to finalize the assessment.



Review the Worklist

After the assessment is finalized, any answers that represent improvement opportunities are moved to the Worklist with recommended actions. To view your action items, click **Access Full Worklist**.

Much like the SRA, the Worklist shows the number of Open items, Closed items, and the percentage of Closed items.

The screenshot displays the '2019 HIPAA SRA Worklist' for 'Demo Clinic A'. At the top, there are tabs for 'Security Risk Analysis' and 'Policies and Procedures'. The main header shows the title '2019 HIPAA SRA Worklist' and 'Demo Clinic A', along with an 'Avg Risk Level: Medium' indicator (a progress bar with 5 yellow segments) and a 'Re-Open Assessment' button. Below this, a summary section shows 'Items OPEN 5', 'Items CLOSED 0', and 'Percentage CLOSED 0%'. A message states: 'To access questions in a specific section of your worklist, please select from the links below. Worklist item numbers will correspond to the related assessment question.' The 'Worklist Sections' section includes a yellow 'Access Full Worklist' button and three categories: 'Administrative' (0/3 closed, Avg Risk Level: High), 'Physical' (0/1 closed, Avg Risk Level: High), and 'Technical' (0/1 closed, Avg Risk Level: Medium). The 'Walkthroughs' section includes a note about allowing popups and two buttons: 'Print Assessment' and 'Print Worklist'. At the bottom left, it says '2 of 10 locations used'.

In the Worklist, click on a section to see which questions need attention. For each recommendation, you'll have the option to **Assign** action items to specific users, set a **Due Date** and **Status**, add or edit **Comments**. The Priority Level is automatically determined by the answer in the SRA and carries over to the associated recommendation.

Recommendation 72

Update your procedures to specify a frequency (such as quarterly) to periodically review your organizations workstation layout. Ensure physical access to workstations is restricted as much as possible to guard against unauthorized access or theft.

Assign to: **Due date:**

Status:

Priority: Low

COMMENTS

Oct 31, 2019 > April Needham [delete](#) | [edit](#)
test

Oct 31, 2019 > April Needham [delete](#) | [edit](#)
testing

1 of 9

Download or Print Documentation

The Assessment and the Worklist can be downloaded and/or printed from the Dashboard.

The screenshot displays the '2019 HIPAA SRA Worklist' for 'Demo Clinic A'. At the top, there are tabs for 'Security Risk Analysis' and 'Policies and Procedures'. The main header shows the title '2019 HIPAA SRA Worklist' and 'Demo Clinic A', along with an 'Avg Risk Level: Medium' indicator (a progress bar with 3 yellow segments) and a 'Re-Open Assessment' button. Below this, three summary cards show: 'Items OPEN 5', 'Items CLOSED 0', and 'Percentage CLOSED 0%'. A text block explains that worklist item numbers correspond to assessment questions. The 'Worklist Sections' section features three cards: 'Administrative' (0/3 closed, Avg Risk Level: High), 'Physical' (0/1 closed, Avg Risk Level: High), and 'Technical' (0/1 closed, Avg Risk Level: Medium). Each card has a play button icon and a risk level progress bar. A link 'Access Full Worklist' is also present. The 'Walkthroughs' section includes a note about print links and two buttons: 'Print Assessment' and 'Print Worklist'. At the bottom, it states '2 of 10 locations used' and 'Last Updates: Nov 26, 2019 | Updated by: April Needham'.

Walkthrough

On the following page is a checklist that can be used to assist with the Walkthrough portion of the Assessment. If using the paper form, transfer all answers to the Walkthrough section in Medcurity using the appropriate location.

Walkthrough Location: _____

#	Y/N	Question
1		Is the Notice of Privacy Practices (NPP) missing or not easily viewable by patients?
2		Do sign-in sheets contain more than the minimum information needed?
3		Are appointment schedules containing PHI posted in department?
4		Are visitors (other than patients or employees) able to access areas with PHI, without ID Badges, visitor badges, sign-in sheets, and/or escorts?
5		Are paper documents containing PHI visible to unauthorized persons?
6		Are fax machines within arm's reach of a patient traffic area?
7		Is the department/unit faxing without an appropriate fax cover sheet contain a confidentiality statement?
8		Are pictures of patients or Thank You notes posted on bulletin boards?
9		Do white boards (if used) only contain minimal info?
10		Are any aspects of shred bin usage compromising PHI or sensitive information?
11		Are additional controls/mechanisms needed to prevent overhearing conversations with patients?
12		Do employees need further training on where to find system HIPAA policies and forms?
13		Do employees need further training on the name of the local privacy/security officer or where to find the contact information?
14		Does the department/unit share passwords?
15		Are any passwords posted or otherwise visible in the area?
16		Do employees leave computers unlocked or logged in when no one is in attendance?
17		Are computers and PHI applications not automatically logging out or locking after a period of inactivity?
18		Are computer screens visible to unauthorized individuals?
19		Are locks and appropriate key access to department door(s) and files established where needed?
20		Do restricted areas need additional controls such as signs, cameras, or alarms installed?
21		Are any devices missing appropriate identification as the organization's property, with labels, tags, engraving on equipment, etc.?
22		Are laptops unencrypted?
23		If any of the facilities are shared with other organizations, are additional controls needed for managing access?
24		Are any server or telecom areas unsecured?

Policies and Procedures

To access the policies and procedures tool, navigate to your Medcurity dashboard and click on the **Policies and Procedures** tab. This will display a list of policy and procedure templates that are available for customization to your organization.

Dashboard

Welcome
Demo Clinic A

Security Risk Analysis | Policies and Procedures

Sort By: None

Public View | Expand All

00-Information Security Policy Next Renewal Date: N/A	● Not Started	▲
01-Introduction to the Information Security Policy Next Renewal Date: 11/26/2020	● Approved	▲
02-Security Management Process Next Renewal Date: 11/26/2020	● Approved	▲
03-Workforce Security Next Renewal Date: N/A	● In Progress	▼

03-Workforce Security
Last Updated: 11/26/2019 8:30am

✓ Approve | Preview | Print | Edit

Customize a Policy

To customize a policy with parameters that match your organization, choose a policy and click **Edit**. From the dashboard, you can also Preview, Print, Approve or Renew policies.

The screenshot shows the 'Demo Clinic A' dashboard with three tabs: 'Demo Security Risk Analysis', 'Security Risk Analysis', and 'Policies and Procedures'. The 'Policies and Procedures' tab is active. At the top right, there is a 'Sort By: None' dropdown menu and two buttons: 'Public View' and 'Expand All'. The main content area displays a list of policies with their titles, next renewal dates, and status indicators:

Policy Title	Next Renewal Date	Status	Action
00-Information Security Policy	N/A	Not Started	Up Arrow
01-Introduction to the Information Security Policy	11/26/2020	Approved	Up Arrow
02-Security Management Process	11/26/2020	Approved	Up Arrow
03-Workforce Security	N/A	In Progress	Up Arrow
Two Year Renewal	11/20/2019	Expired	Down Arrow

Below the 'Two Year Renewal' policy, there is a detailed view showing the policy title, last updated date (12/03/2019 3:14pm), and four action buttons: 'Renew', 'Preview', 'Print', and 'Edit'.

At the top of the policy, you'll see **Policy Details**. This section provides an overview of the administration of the policy such as date the policy was initially implemented (Adopted), last revision date (Revised), and who approved the policy.

In this section, you will set the **Review** frequency for this policy. To do so, click into this field to display three options to choose from – Annual, Every two years, or Every three years.

03-Workforce Security

POLICY DETAILS:

Approved by:	Adopted:
Review: Annual	Revised: 11/26/2019
	Reviewed:

Workforce Security

Policy Statement

It is the policy of Demo Clinic A to ensure that all members of the workforce who should have access to ePHI have the appropriate level of access required to operate at a privilege level no high prevent those who should not have access to ePHI from obtaining it, and to ensure that access to ePHI is terminated when employment is terminated.

Procedure

- Authorization & Supervision §164.308(a)(3)(ii)(A)

When you edit a policy, you can answer the questions from the menu on the left or answer directly within the policy. Whichever you choose, your answers will automatically populate in the template.

Demo Clinic A

03-Workforce Security

POLICY DETAILS:

Approved by:	Adopted:
Review: Annual	Revised: 11/26/2019
	Reviewed:

Workforce Security

Policy Statement

It is the policy of Demo Clinic A to ensure that all members of the workforce who should have access to ePHI have the appropriate level of access required to operate at a privilege level prevent those who should not have access to ePHI from obtaining it, and to ensure that access to ePHI is terminated when employment is terminated.

Procedure

- Authorization & Supervision §164.308(a)(3)(ii)(A)
The Security Officer shall have the authorization and/or supervisory permission to approve access to information systems and/or locations where ePHI may be accessed. Since the Office Manager® Workforce member's supervisor® Other I is the person who most closely recognizes a workforce member's need to access data, requests for access to information systems shall be submitted by the Office Manager® Workforce member's supervisor® Other I using the Network Access Request form ([Appendix D](#)) and the Hiring and Term Checklist ([Appendix F](#)). The workforce member's access to data shall be granted only as specifically re

At the bottom of each policy, you'll find the **Comments** section as well as **Policy Revisions**. Medcurity maintains a record of comments (user, date stamp) and policy

revisions (who, when, and what was revised). Comments can be edited or deleted; however, policy revisions cannot be changed.

Temporary workers and third-party workforce members not already covered by a confidentiality agreement shall sign such a document prior to accessing Demo Clinic A information resources. Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or workforce members are leaving Demo Clinic A.

Cancel Save

Comments

Leave a Comment:

Submit

April Needham - 11/26/2019 9:17am - [Edit](#) | [Delete](#)
Commenting

Policy Revisions

DATE	CHANGE AUTHOR	CHANGE SUMMARY
11/26/19 8:30AM	April Needham	Company Policy content was changed.

Once you have completed the required fields, click **Save**. This will store your policy with an updated status of **In Progress** on the Policies and Procedures dashboard.

The screenshot shows a dashboard for 'Demo Clinic A' with two tabs: 'Security Risk Analysis' and 'Policies and Procedures'. The 'Policies and Procedures' tab is active, displaying a list of four policies. At the top right of the list, there is a 'Sort By' dropdown menu set to 'None', and two buttons: 'Public View' and 'Expand All'. Each policy entry includes a title, a 'Next Renewal Date', a status indicator (a colored circle followed by text), and an upward-pointing arrow.

Policy Title	Next Renewal Date	Status
00-Information Security Policy	N/A	Not Started
01-Introduction to the Information Security Policy	11/26/2020	Approved
02-Security Management Process	11/26/2020	Approved
03-Workforce Security	N/A	In Progress

When the policy is ready for review, click **Edit** next to the policy on the dashboard. In the upper right-hand corner, click **Send for Review**. This sends email notification to all users that the policy is available for review.

POLICY DETAILS:	
Adopted:	
Revised:	11/26/2019
Review:	Annual

Workforce Security
Policy Statement
It is the policy of Demo Clinic A to ensure that all members of the workforce who should have access to ePHI have the appropriate level of access required to operate at a privilege level no higher than necessary to accomplish required job duties, to prevent those who should not have access to ePHI from obtaining it, and to ensure that access to ePHI is terminated when employment is terminated.
Procedure

Once the policy is ready for approval, the approver will navigate to the Dashboard and click **Approve**. A pop-up box will appear requesting the name of the approver and confirmation.

Approve Policy [X]

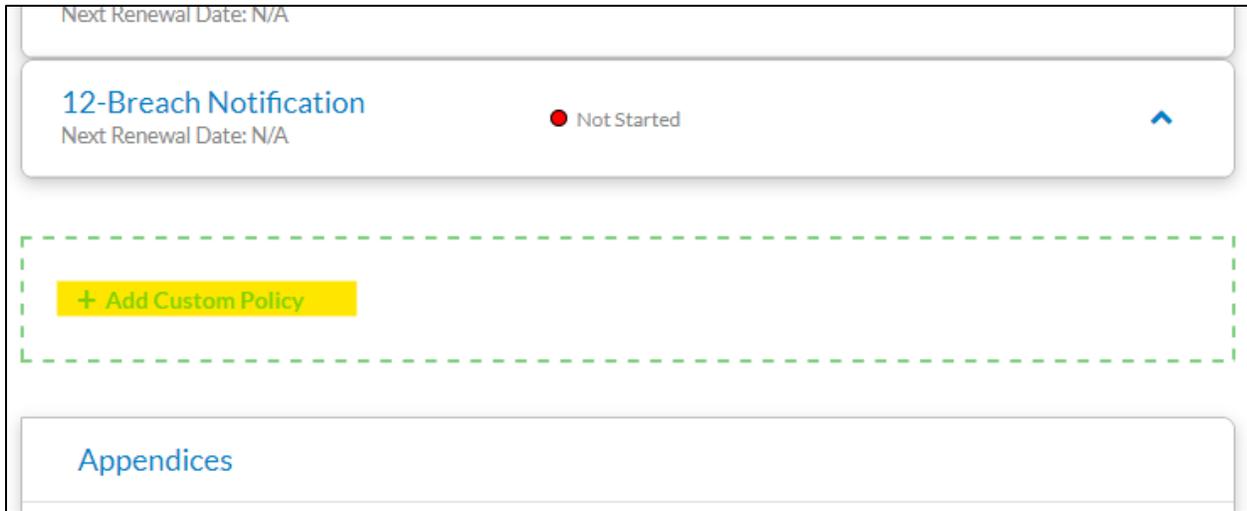
Approved By: Jane Doe

Cancel Approve

Once approved, the status will show **Approved** on the dashboard.

Create a Policy

If your organization has a policy you would like to use in lieu of or in addition to a Medcurity policy, click on **Add Custom Policy** located under the Medcurity templates.



The screenshot shows a user interface for managing policies. At the top, there is a header with the text "Next Renewal Date: N/A". Below this is a list of policies. The first policy is "12-Breach Notification" with a status of "Not Started" (indicated by a red dot) and a "Next Renewal Date: N/A". To the right of the policy name is a blue upward-pointing arrow. Below the list is a dashed green box containing a yellow button with a plus sign and the text "+ Add Custom Policy". At the bottom of the interface is a section titled "Appendices".

From the drop-down menu, choose **Custom Policy** or **Upload a Policy**.



The screenshot shows a dialog box titled "GENERATE A CUSTOM POLICY". At the top right, there are two buttons: "Send for Review" and "Back". Below the title bar is a section labeled "Choose type of Policy". This section contains a dropdown menu with the text "Choose Type" and a downward arrow. The dropdown menu is open, showing two options: "Custom Policy" and "Upload a Policy". At the bottom right of the dialog box, there are two buttons: "Cancel" and "Save".

If you choose Custom Policy, you can select a Medcurity template to edit or create an entirely new policy using the text editor. Set your **Review** period and select the Medcurity template to edit. If you want to create an entirely new policy, select No Template and type or copy/paste your policy into the text editor. Edit or add a **Title** to your policy then click **Save** at the bottom of the screen.

GENERATE A CUSTOM POLICY

Choose type of Policy

POLICY DETAILS:

Approved by:	Adopted:
Review: <input type="text" value="Annual"/>	Revised:
	Reviewed:

Medcurity Policy Template

Title

Policy

Format | Size | ?

If you choose to upload your own document, select the **Review** period, add a **Title**, and enter the **Policy Adopted Date**. Click **Choose File** to upload your document. Once the file has successfully uploaded, click **Save**.

GENERATE A CUSTOM POLICY

Choose type of Policy

POLICY DETAILS:

Approved by:	Adopted:
Review: <input type="text" value="Annual"/>	Revised:
	Reviewed:

Title

Policy Adopted Date

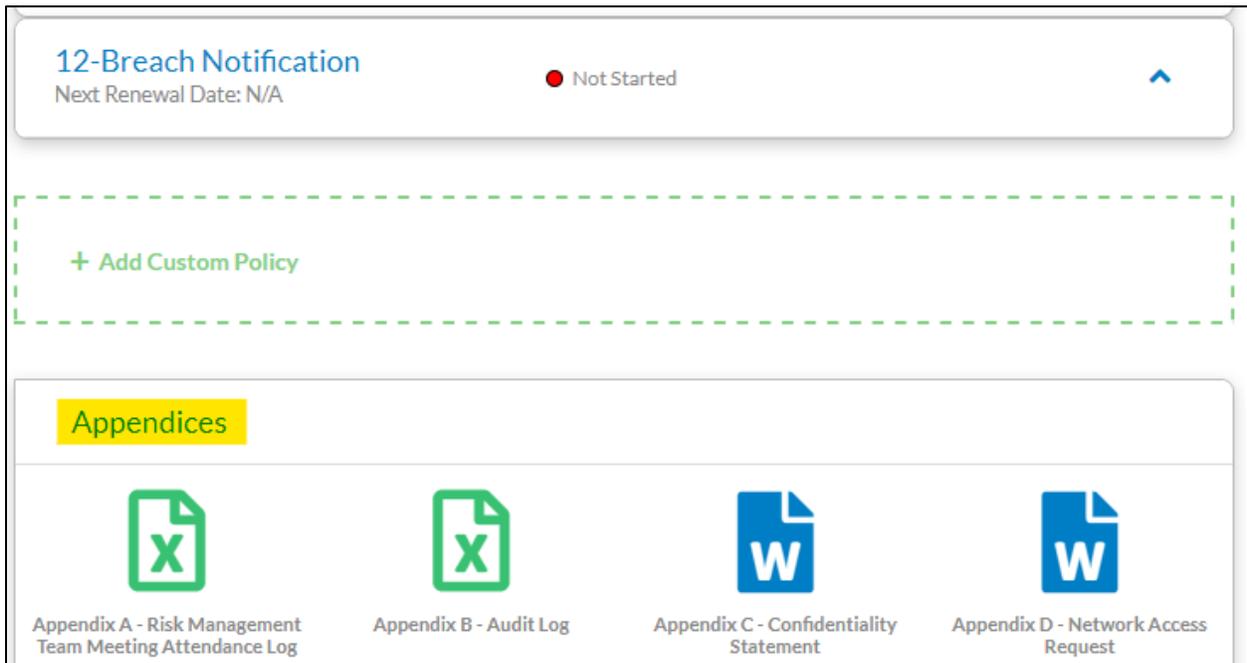
[Upload an existing Policy](#) No file chosen

Appendices

Customizing an Appendix

Medcurity appendices are embedded in the corresponding Policy and Procedures. You will see links to appendices within the body of the policies. Appendices can be edited to meet the needs of your organization and there is also an option to upload a custom appendix.

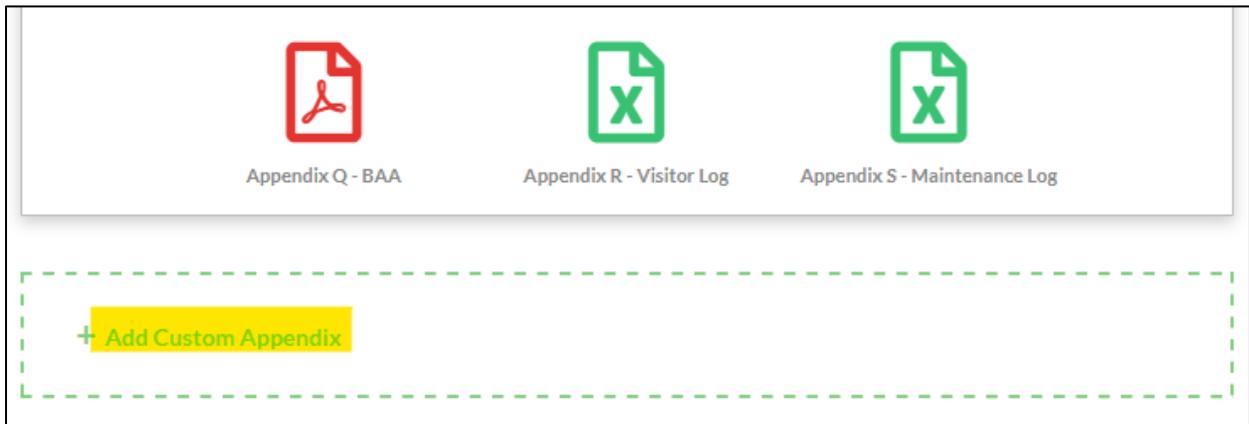
On the dashboard, located under the list of policies, is the list of appendices.



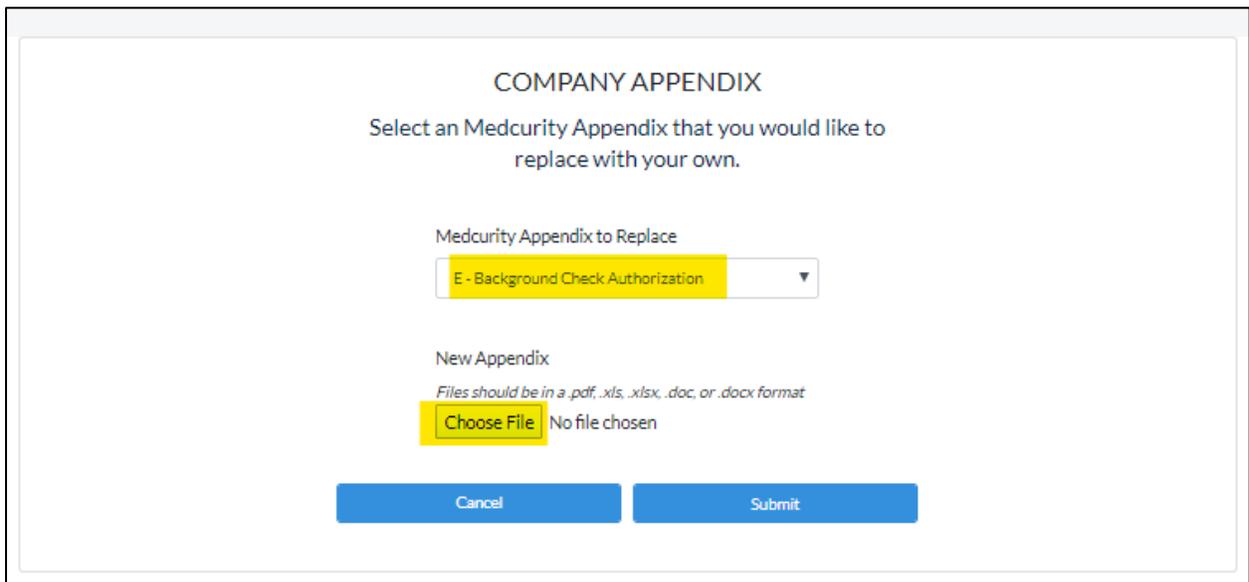
These appendices can be saved locally, edited to satisfy your organization's requirements, and re-uploaded to your Medcurity account.

To customize an appendix, select it from the list. The file will download to your computer as a Word, Excel, or Adobe file. Open the file, make your edits, save, and upload it to your Medcurity account.

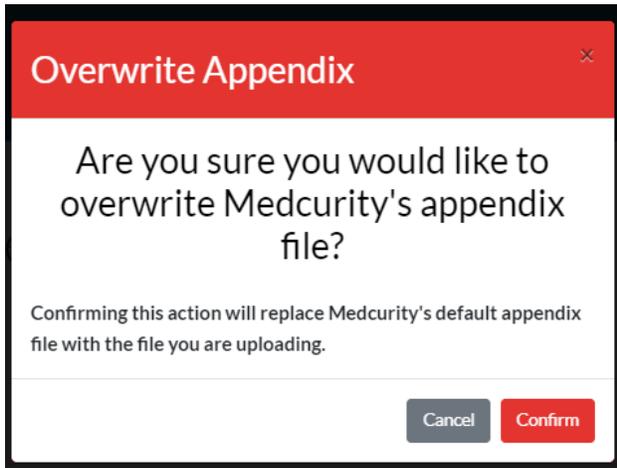
If you have an appendix that you would like to use in lieu of a Medcurity appendix, click **Add Custom Appendix** underneath the appendices.



From the drop-down menu, select the Medcurity appendix you would like to replace then choose the replacement appendix. Click **Submit**.

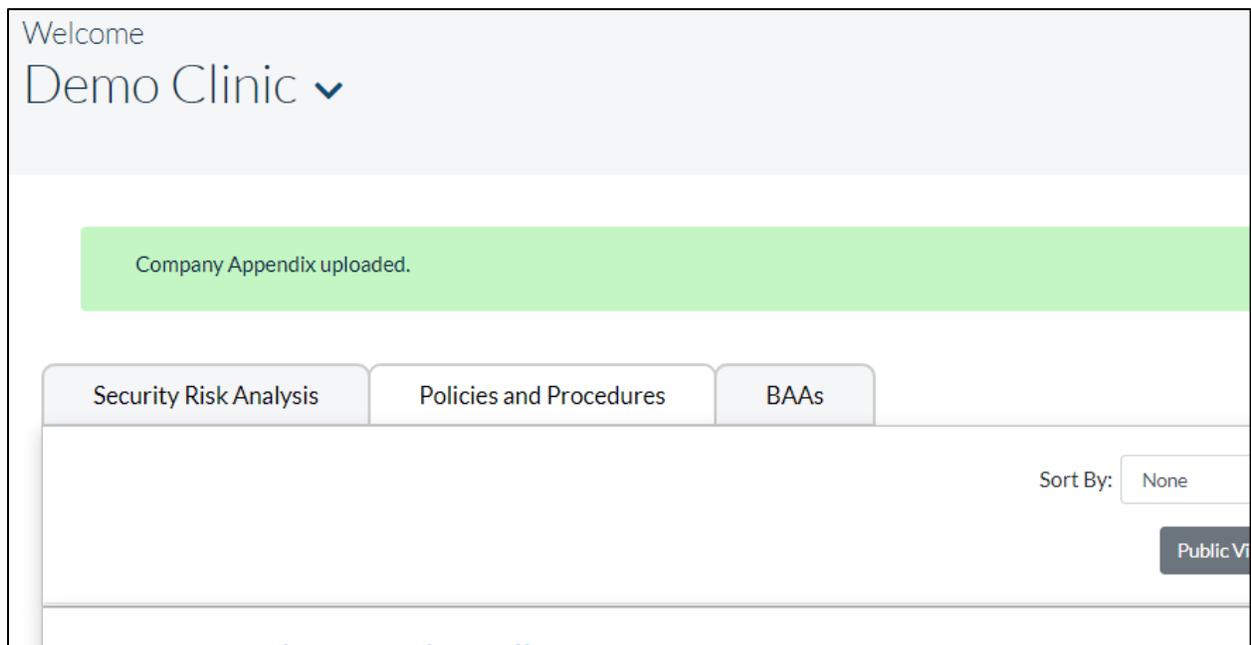


Your uploaded appendix will override the Medcurity appendix so you will be asked to confirm this upload.



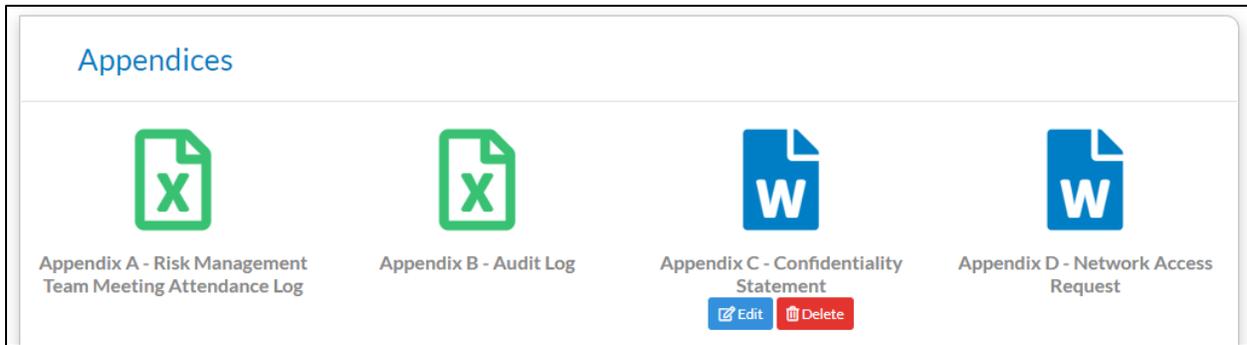
If you later decide to use the Medcurity appendix, simply delete the uploaded appendix and the file will revert to Medcurity's appendix.

You will receive a confirmation once your appendix has been successfully uploaded.

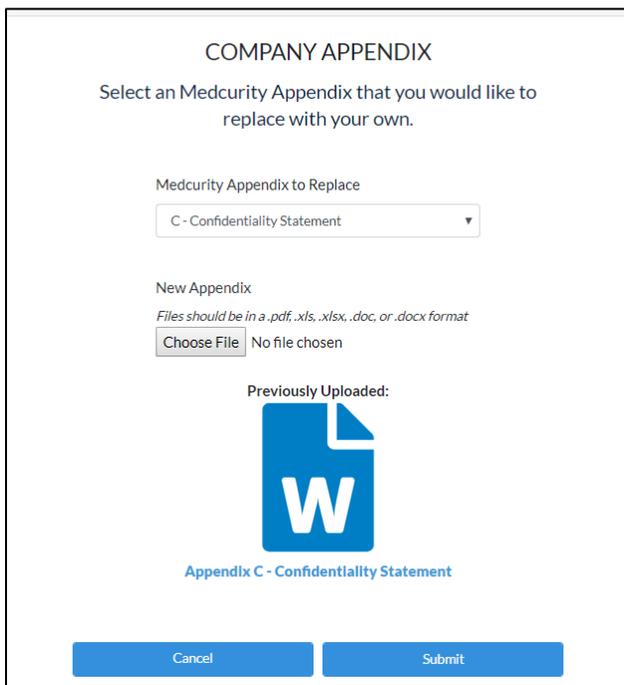


Editing an Appendix

If you need to make changes to an appendix you previously uploaded, return to the list of appendices and click either **Edit** or **Delete**.



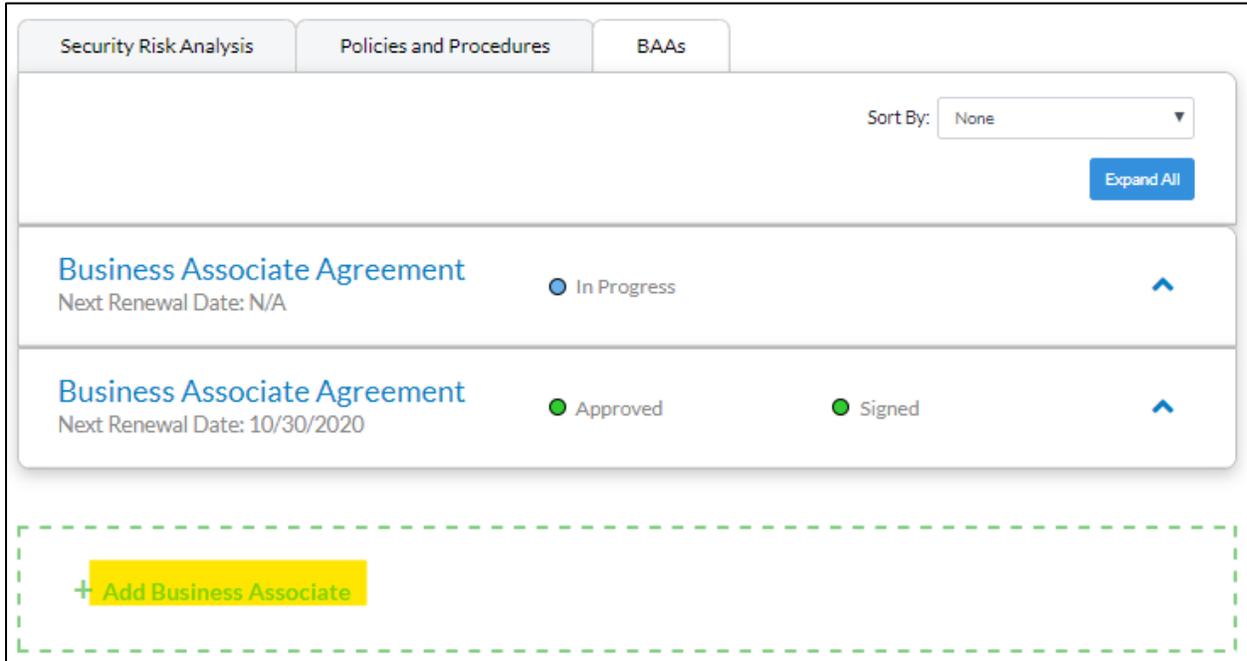
Edit allows you to download and edit the existing appendix or upload a new file. Once you have made your desired changes, click **Submit**.



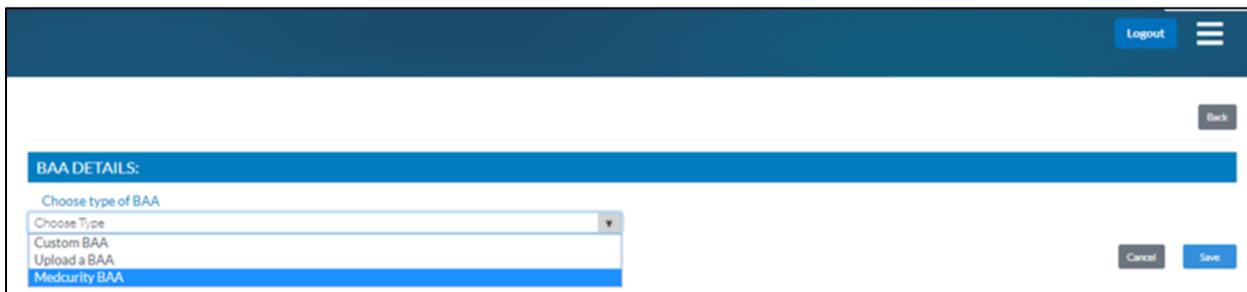
Delete will delete the appendix previously uploaded to the portal and revert to the Medcurity appendix.

Business Associate Agreements

To access the Business Associate Agreement (BAA) tool, navigate to your Medcurity dashboard and click on the **BAAs** tab. Next, click **Add Business Associate**.



From the drop-down menu, choose which type of BAA you want to use. Then, click **Save**.



Types of BAAs

Medcurity BAA

In the BAA details, verify the **Title** and set the **Review Frequency**.

Business Associate Agreement

BAA DETAILS:

Choose type of BAA
Medcurity BAA

Title
Business Associate Agreement

Renew Frequency
Annual

Next, complete the Business Associate Details. The **Master Password** will be provided to the Associate (BAA point of contact) on this agreement enabling them to sign in, access the agreement, and e-sign. We suggest creating a strong password unique to the client, not one that you have used for other accounts.

Enter the email address of the person responsible for signing the BAA. Once the BAA is approved, it can be sent to the Associate in just one click.

BUSINESS ASSOCIATE DETAILS

Master Password

Associate Email #1

Add Email

When you edit the Medcurity BAA, you can answer the questions from the menu on the left or directly within the BAA. Whichever you choose, your answers will automatically populate in the template. Once you have completed the BAA, click **Save**.

If you need to leave the BAA and return to it later, click **Save** before exiting.

The screenshot shows the Medcurity user interface for creating a Business Associate Agreement (BAA). On the left, a sidebar titled "Demo Clinic" contains a "BUSINESS ASSOCIATE AGREEMENT" section with a "+ CREATE A BAA" button. Below this, a scrollable list of questions allows users to configure the agreement, such as "BAA is made as of this date", "Business Associate", and "Do you want to specify a stricter timeframe for the business associate to report a potential breach to the covered entity?".

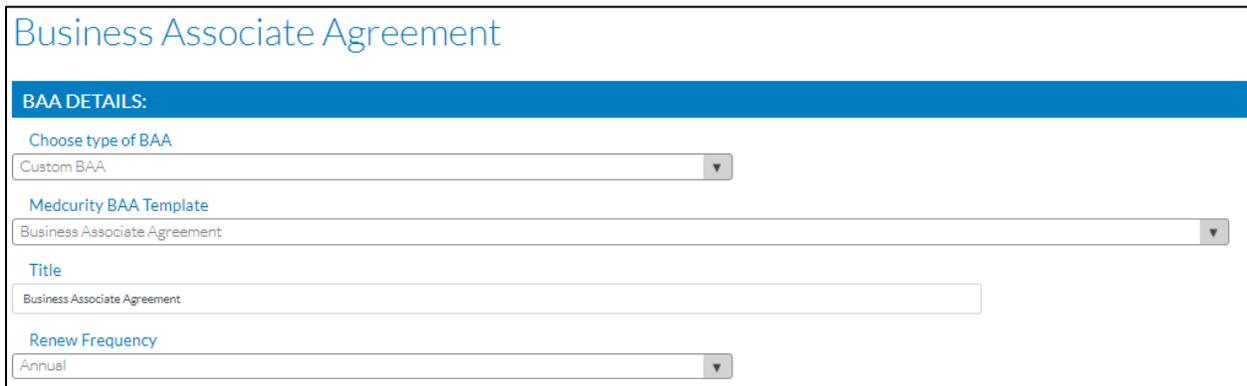
The main area on the right displays the "Business Associate Agreement" template. It includes a header with the title and a "Project 1 Password" field. Below the header, there is an "Associate Email #1" field with an "Add Email" button. The agreement text begins with "This Business Associate Agreement ('Agreement') is made as of [Date] a [Business Associate Name] ('Business Associate' or 'BA'). Covered Entity and Business Associate Insurance Portability and Accountability Act of 1996 and its related regulations ('HIPAA')."

The agreement text continues with "Recitals" and "WHEREAS" clauses, detailing the purpose of the agreement and the regulatory requirements. It concludes with "NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein, the receipt and sufficiency of Definitions".

Custom BAA

From the template drop-down menu, you have the option to choose Medcurity's **Business Associate Agreement** or **No Template**. Starting with Medcurity's BAA template allows you to edit the agreement to meet the requirements of your organization. The No Template option will leave the form completely blank enabling you to create a BAA using the text editor.

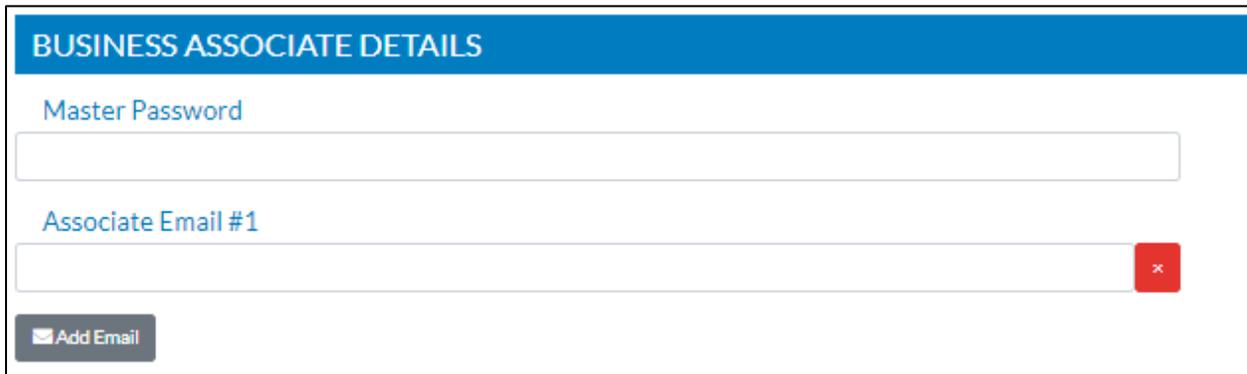
After you've selected your template, choose a **Title** for your document and set the **Renewal Frequency**.



The screenshot shows a form titled "Business Associate Agreement" with a blue header. Below the header is a section labeled "BAA DETAILS:" containing four fields: "Choose type of BAA" (a dropdown menu with "Custom BAA" selected), "Medcurity BAA Template" (a dropdown menu with "Business Associate Agreement" selected), "Title" (a text input field with "Business Associate Agreement" entered), and "Renew Frequency" (a dropdown menu with "Annual" selected).

Next, complete the Business Associate Details. The **Master Password** will be provided to the Associate (BAA point of contact) on this agreement enabling them to sign in, access the agreement, and e-sign. We suggest creating a strong password unique to the client, not one that you have used for other accounts.

Enter the email address of the person responsible for signing the BAA. Once the BAA is approved, it can be sent to the Associate in just one click.



The screenshot shows a form titled "BUSINESS ASSOCIATE DETAILS" with a blue header. Below the header are two text input fields: "Master Password" and "Associate Email #1". The "Associate Email #1" field has a red "x" icon on the right side. At the bottom left of the form is a button labeled "Add Email" with an envelope icon.

Edit the text of the Medcurity BAA template to comply with your organizational needs or enter text for the entirely custom BAA.

BAA

Business Associate Agreement

This Business Associate Agreement ("Agreement") is made as of %date% and is entered into by and between (company common_name), ("Covered Entity" or "CE"), and %business_associate% ("Business Associate" or "BA"). Covered Entity and Business Associate may be referred to individually as a "Party" and collectively as the "Parties." in order to comply with the Health Insurance Portability and Accountability Act of 1996 and its related regulations ("HIPAA").

Recitals

WHEREAS, CE and BA have entered into an agreement pursuant to which BA will provide certain services to or on behalf of CE, and BA may create, receive, maintain, transmit, or have access to Protected Health Information in order to provide those services ("Services Agreement");

Whereas, the Department of Health and Human Services ("HHS") has promulgated regulations at 45 Code of Federal Regulations ("CFR") Parts 160 and 164 implementing the privacy requirements ("Privacy Rule") and regulations at 45 CFR Parts 160, 162, and 164 implementing the security requirements ("Security Rule") set forth in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, ("HIPAA") as amended by regulations implementing Subtitle D of the Health Information Technology for Economic and Clinical Health Act which is Title XIII of the America Recovery and Reinvestment Act of 2009 (Public Law 111-5);

WHEREAS, the Privacy Rule and Security Rule require CE to enter into a written contract with BA in order to assure certain protections for the privacy and security of Protected Health Information, and the Privacy Rule and Security Rule prohibit the disclosure or use of Protected Health Information to or by BA if such a contract is not in place;

WHEREAS, both Parties mutually agree to satisfy the foregoing regulatory requirements and all federal, state, and local confidentiality, privacy, and security laws through this Agreement;

NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein, the receipt and sufficiency of which are hereby acknowledged, CE and BA agree as follows:

Definitions

Catch-all

Terms used, but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR Part 160, Part 162, and Part 164, then in effect or as amended, which are collectively referred to as the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific

"Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

"Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

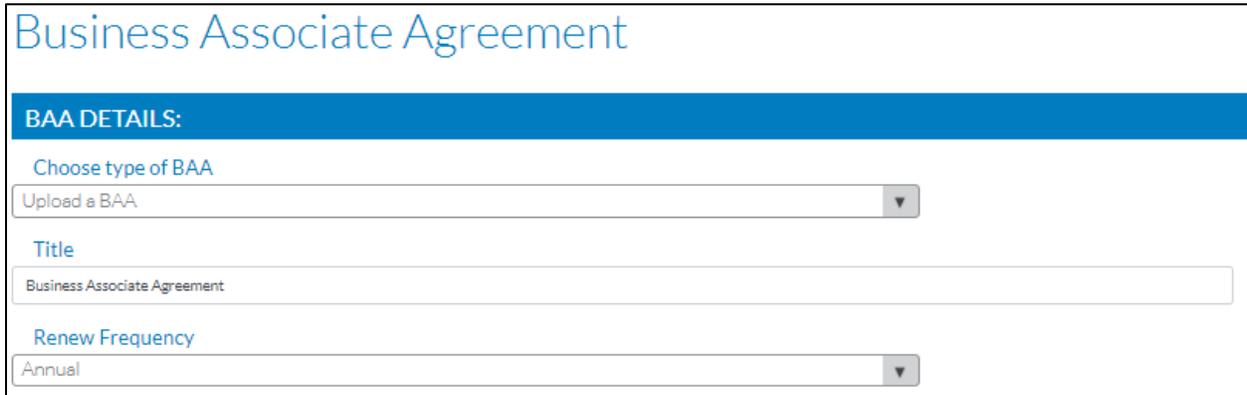
"Electronic Health Record" shall have the same meaning as the term "electronic protected health information" in 45 CFR 160.103, limited to the information that Business Associate creates, receives, maintains, or transmits from or on behalf of Covered Entity.

Once you have completed the BAA, click **Save**.

If you need to leave the BAA and return to it later, click **Save** before exiting.

Upload a BAA

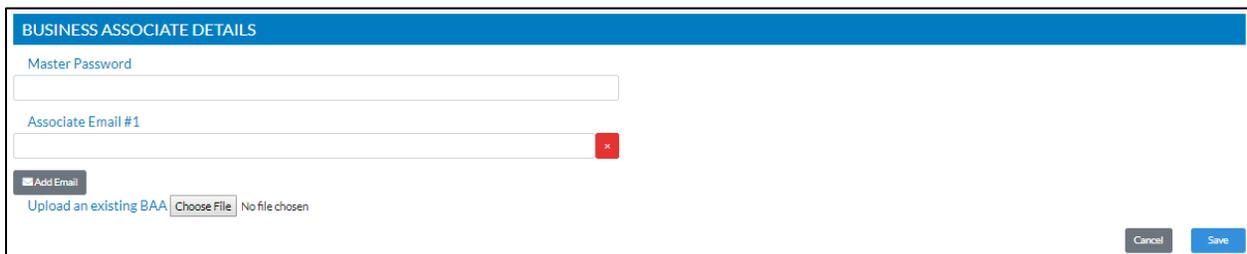
In the BAA details, choose a **Title** for your document and set the **Renewal Frequency**.



The screenshot shows a form titled "Business Associate Agreement". Below the title is a blue header labeled "BAA DETAILS:". The form contains three main sections: "Choose type of BAA" with a dropdown menu set to "Upload a BAA"; "Title" with a text input field containing "Business Associate Agreement"; and "Renew Frequency" with a dropdown menu set to "Annual".

Next, complete the Business Associate Details. The **Master Password** will be provided to the Associate (BAA point of contact) on this agreement enabling them to sign in, access the agreement, and e-sign. We suggest creating a strong password unique to the client, not one that you have used for other accounts.

Enter the email address of the person responsible for signing the BAA. Once the BAA is approved, it can be sent to the Associate in just one click.



The screenshot shows a form titled "BUSINESS ASSOCIATE DETAILS". It contains three input fields: "Master Password", "Associate Email #1", and "Add Email". Below the "Add Email" field is a file upload section with the text "Upload an existing BAA" and a "Choose File" button. The status below the button reads "No file chosen". At the bottom right of the form are "Cancel" and "Save" buttons.

After you've completed the requested information, click **Browse** and select the file to upload. Once the file has successfully uploaded, click **Save**.

Managing BAAs

Status

In Progress

Once you have created and saved BAAs, you will see the status of each on the dashboard. In Progress means that a BAA has been created and is being edited or needs to be reviewed and has not yet been approved.

The screenshot shows a card for a Business Associate Agreement. At the top, the title "Business Associate Agreement" is displayed in blue, followed by "Next Renewal Date: N/A". To the right, there is a blue circle icon and the text "In Progress", and a blue downward arrow. Below this, a white box contains the same title "Business Associate Agreement" and "Last Updated: 10/09/2019 8:47am". To the right of this box are four buttons: a green "Approve" button with a checkmark, and three white buttons with blue borders labeled "Preview", "Print", and "Edit".

Approved / Not Sent

Once a BAA is approved, it then needs to be emailed to the Business Associate for signature. Not Sent means that the BAA has been approved but it has not yet been sent for signature.

To send the BAA, click **E-mail 1 Associates**. You will receive a confirmation that an email has been sent to the email address entered in the BAA details.

The screenshot shows a card for a Business Associate Agreement. At the top, the title "New Test BAA" is displayed in blue, followed by "Next Renewal Date: 11/14/2021". To the right, there is a green circle icon and the text "Approved", a red circle icon and the text "Not Sent", and a blue downward arrow. Below this, a white box contains the same title "New Test BAA" and "Last Updated: 11/14/2019 2:58pm". To the right of this box are four buttons: "Preview", "Print", "Email 1 Associates", and "Edit".

Approved / Sent

A status of Sent means that the BAA has been sent to the Associate but the Associate has not signed the and returned the agreement.

Business Associate Agreement- Custom Test ● Approved ● Sent ▼

Next Renewal Date: 10/31/2021

Business Associate Agreement- Custom Test Preview Print Email 1 Associates Edit

Last Updated: 10/31/2019 9:07am

Once sent, the Business Associate will receive an email with a link to the document where they can electronically sign the BAA and return it via email to the Covered Entity.

Electronic copies of this fully executed Agreement shall be deemed to be originals.

Business Associate	Covered Entity
<p>Signature</p> 	<p>Signature</p> 
<p>Name: Amanda Hepper</p> <p>Title: President</p>	<p>Name Clear</p> <input type="text" value="April Needham"/> <p>Title</p> <input type="text" value="Program Director"/>
	<input type="button" value="submit"/>

Signed

A status of Signed means that the Associate has electronically signed and returned the agreement.

**Business Associate Agreement-
testing** ● Approved ● Signed ▼

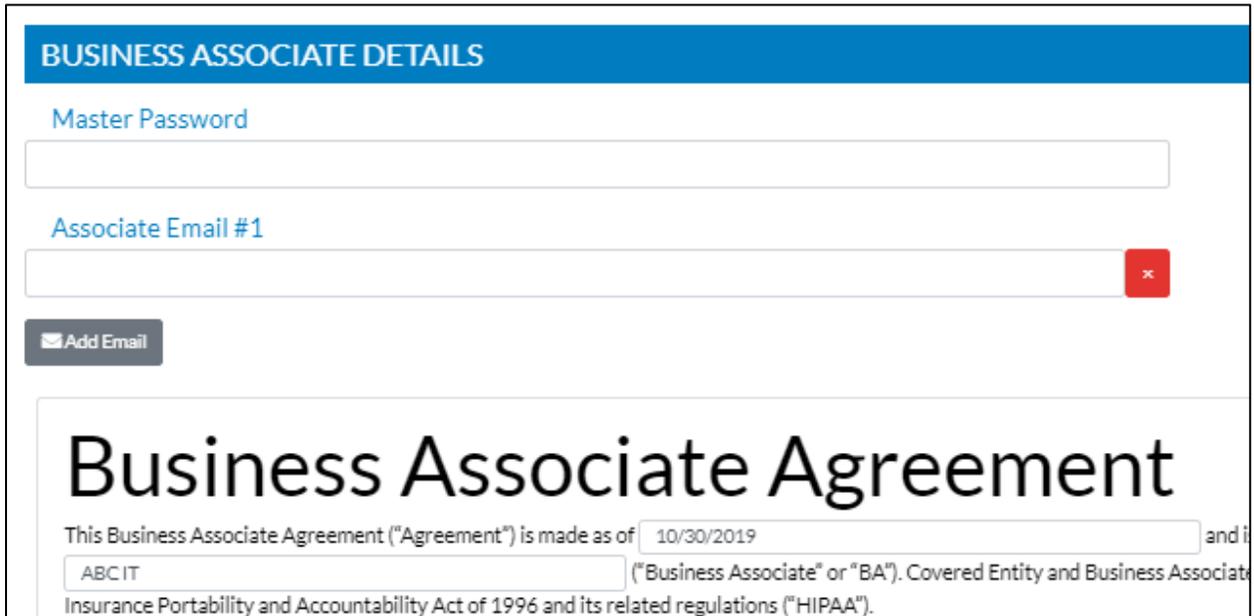
Next Renewal Date: 11/12/2020

Business Associate Agreement- testing Preview Print Email 1 Associates Edit

Last Updated: 11/12/2019 11:11am

Deleting Email Addresses

To remove an email address after the BAA has been saved but not sent for Approval. Click Edit next to the BAA on the Dashboard. Click the **x** in the red box next to the email address you want to delete then enter a new email or leave the window blank.



BUSINESS ASSOCIATE DETAILS

Master Password

Associate Email #1

Add Email

Business Associate Agreement

This Business Associate Agreement ("Agreement") is made as of 10/30/2019 and it is between ABCIT ("Business Associate" or "BA"), Covered Entity and Business Associate Insurance Portability and Accountability Act of 1996 and its related regulations ("HIPAA").

Click **Save** at the bottom of the screen.

Contact Us

Support is available Monday through Friday, 8:00 am to 5:00 pm Pacific time and can be reached via telephone at (509) 867-3645 or via e-mail at support@medcurity.com.