Bottomline

HIPAA Compliance Policy and Procedures

The purpose of this HIPAA Compliance Policies and Procedures is to establish Bottomline's guidelines regarding the appropriate and compliant use and disclosure of Protected Health Information (PHI) as defined in 45 CFR Parts 160 and 164 (HIPAA).

Bottomline and all of its employees must comply with these procedures.

Last Update:	**12.2019**
Version:	**v3.1**
Approver:	**BT Security Office**

FIRST CLASS C1 CUSTOMER CARE

Document History

Date	Versio	Updates
October 2009	1.0	Original Version
February 2010	2.0	HITECH Updates, expand to company-wide document, requires finalization of HIPAA Drive & VM Process
September 2015	3.0	BT resource updates, Grammatical corrections
August 2017	3.1	Annual review and update to formal appointment of privacy officer
December 2017	3.1	Annual review and approval
December 2018	3.1	Annual review and approval
December 2019	3.1	Annual review and approval
December 2020	3.1	Annual review and approval

Table of Contents

1 Introduction 5
1.1 What is HIPAA? 5
1.2 What Does it Mean for Bottomline? 5
1.3 What Does it Mean for Bottomline Workforce Members?.. 6
1.4 Formal Appointment of Privacy Officer (Data Protection Officer)…………………………6
2 Day-to-Day Bottomline Workforce REQUIRED Process & Procedures 6
2.1 General Rules 6
2.2 Identifying a HIPAA Customer 7
2.3 REQUIRED Secure Data Transmission Process for HIPAA Customer Data 7
2.3.1 PHI Received via Email.. 8
2.3.2 PHI Received via Secure Email, sFTP, or HTTPS 8
2.3.3 PHI Received via Fax.. 8
2.4 REQUIRED Secure Data Storage Process for HIPAA Customer Data 8
2.4.1 HIPAA Drive.. 9
2.4.2 Data Defense 9
2.5 REQUIRED Bottomline Virtual Machine (VM) Process 10
2.6 Salesforce.com 10
2.7 CRM System..10
2.8 Visual Source Safe (VSS) 10
2.9 Mercury Quality Center 10
3 Security Rule and Breaches of Security..10
3.1 Security Rule Requirement..10
3.2 Mitigation and Breach Notification 10
3.3 Safe Harbor 11
3.3.1 Data in Motion Requirements 12
3.3.2 Data at Rest Requirements 12
4 Privacy Rule..12
5 Training..13
6 Ongoing Compliance..13
7 Accounting of Disclosures 13
8 Relationship to Other Policies and Procedures 14
9 Sanctions and “Whistleblower” 14

APPENDIX A: Audit Assessment Tool 15

APPENDIX B: Using sFTP and HTTPS for Data Transmission 18

APPENDIX C: Installation & Configuration of Data Defense 24

APPENDIX D: Email Response for Customer Non-Compliance 26

GLOSSARY 27

1 Introduction

The policies & procedures outlined in this document apply to the entire Bottomline Workforce. Due to their role as a HIPAA Clearinghouse, the Paymode team has some additional process and procedures which are outlined in the Paymode HIPAA POLICIES AND PROCEDURES documents. Further IT procedures related to HIPAA are outlined in the Master IT Procedures document.

1.1 What is HIPAA?

HIPAA is an acronym for the United States Health Insurance Portability and Accountability Act of 1996. It is a federal law that, among other things, imposes privacy and security requirements on healthcare patient data. Additionally, the American Recovery and Reinvestment Act of 2009 (ARRA) included the Health Information Technology for Economic and Clinical Health (HITECH) Act which drastically tightens the HIPAA law by making expansive changes to the privacy and security provisions impacting Covered Entities and Business Associates. The HIPAA law is directly applicable to Covered Entities and, with the enactment of HITECH, to Business Associates as well.

The Glossary to this Policy describes Covered Entities, Business Associates, and defines other capitalized terms used throughout this policy.

1.2 What Does it Mean for Bottomline?

Bottomline is required to operate under the HIPAA and HITECH laws and comply with all privacy and security provisions to protect confidential Protected Health Information (PHI) as both as a HIPAA Covered Entity through its Paymode operations and Business Associate to several of Bottomline’s customers which are HIPAA Covered Entities.

Complying with HIPAA and HITECH generally means complying with the Privacy Rule and the Security Rule defined by the Department of Health and Human Services. Additionally, Paymode is concerned with the Transactions Rule.

The Security Rule relates to protection of PHI from unauthorized Use or Disclosure. Bottomline is required to implement administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic PHI.

The Privacy Rule relates to when and how Protected Health Information (PHI) may be Used and Disclosed. For Bottomline’s non-Paymode business, there should generally be no external Disclosures and internal Use and Disclosure should be minimal and on an as needed basis to perform our obligations to customers.

The Transactions Rule defines standard formats which must be used for the electronic exchange of certain healthcare documents. As a Clearinghouse for healthcare claims payments, Paymode translates payment and remittance information into and out of the standard formats on behalf of the clients and their providers. For further detail and information on the Transactions Rule, please reference the Paymode HIPAA POLICIES AND PROCEDURES documents.

1.3 What Does it Mean for Bottomline Workforce Members?

All members of Bottomline's Workforce are required to understand the implications and execute against the required processes of working with PHI, including the following specific actions:

- Annual training and sign off on Bottomline HIPAA policies as required by your department or role
    - Adhering to the policy and processes described within this document
- Discussing any questions or concerns regarding your Use and/or Disclosure of PHI and compliance with these Policies and Procedures with one of the following HIPAA resources within Bottomline:

○ Privacy Officer, or its Backup

○ Corporate LOB HIPAA Resource

○ Banking LOB HIPAA Resource

- ○ Product Development/QA HIPAA Resource
- ○ Product Management/Marketing HIPAA Resource
- ○ Sales/Sales Operations/Finance/Accounting HIPAA Resource
- ○ TSNA LOB HIPAA Resource

- Reporting any violations of these policies and procedures to the Privacy Officer or Human Resources

1.4 Formal Appointment of Privacy Officer (Data Protection Officer)

Bottomline will formally appoint a global privacy officer \ data protection officer responsible for providing guidance to managers, users and service providers on their individual responsibilities and the specific procedures that must be followed.

2 <u>Day-to-Day Bottomline Workforce REQUIRED Process & Procedures</u>

2.1 General Rules:

- All data files provided by a HIPAA customer should be assumed to include PHI until it is determined that the data file does not contain PHI. You may ask a HIPAA customer in writing if a data file contains PHI. We can only conclude that a data file does not contain PHI if the customer confirms in writing that it does not.
- Faxing of PHI should not be used unless necessary. If faxing PHI, you must ensure that an approved person is on the receiving end and knows that you are sending them PHI and has agreed to intercept it.
- Only use sFTP, HTTPS or other encryption protocols defined in Appendix B or the Paymode HIPAA POLICIES AND PROCEDURES documents to transmit HIPAA data.
- Store all HIPAA data on the designated HIPAA drive (NOTE: *Paymode has its own secure locations for the storage of HIPAA data, please reference* the Paymode HIPAA

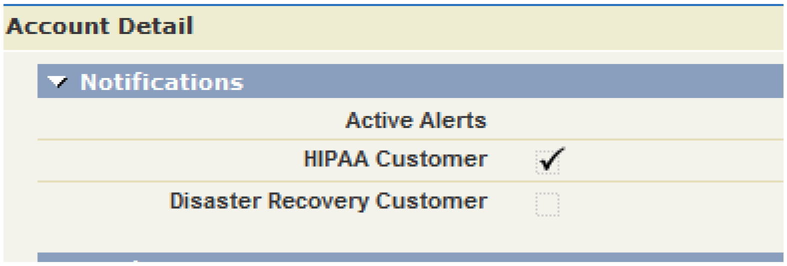
POLICIES AND PROCEDURES documents *for Paymode HIPAA procedures.)*

- Delete all HIPAA data from your laptop/workstation hard drive
- Ensure that Data Defense is installed and properly configured on your laptop or workstation (see Appendix C)
- Always lock/log off your laptop or workstation when not working on it
- Never leave your laptop in an unsecured location

- Do not attach or include PHI in Salesforce.com
- Do not attach or include PHI in Mercury Quality Center
- Do not attach or store data in SourceSafe
- All printed PHI must be shredded after Use or it may be discarded in a confidential data destruction receptacle. Never throw PHI in a trash can.

2.2 Identifying a HIPAA Customer

In Salesforce.com in the *"Account"* entry there is a HIPAA Customer checkbox in the *"Notifications"* section of the account detail record.

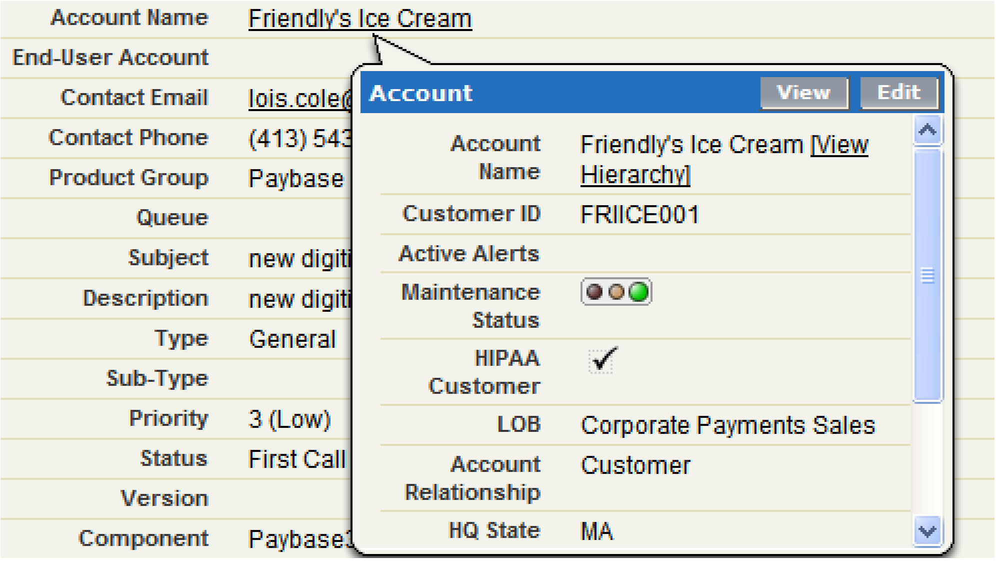


Account Detail

Notifications

Active Alerts	
HIPAA Customer	✓
Disaster Recovery Customer	□

Also in the „hover" view of the account, the HIPAA designation is also included:



Account Name	Friendly's Ice Cream
End-User Account	
Contact Email	lois.cole@
Contact Phone	(413) 543
Product Group	Paybase
Queue	
Subject	new digit
Description	new digit
Type	General
Sub-Type	
Priority	3 (Low)
Status	First Call
Version	
Component	Paybase1

Account

Account Name	Friendly's Ice Cream [View Hierarchy]
Customer ID	FRIICE001
Active Alerts	
Maintenance Status	●●●
HIPAA Customer	✓
LOB	Corporate Payments Sales
Account Relationship	Customer
HQ State	MA

2.3 REQUIRED Secure Data Transmission Process for HIPAA Customer Data

In order to appropriately secure "data in motion" PHI to comply with Safe Harbor, Bottomline's required method of encrypting HIPAA data transmissions to customers is sFTP or HTTPS (see Appendix B and/or the Paymode HIPAA POLICIES AND PROCEDURES documents for instructions on how to use these tools).

Likewise, our HIPAA customers are obligated to send PHI to Bottomline using similar methods.

Note: WinZip and Microsoft Word or Excel password protection methods are commonly used and do NOT provide acceptable levels of encryption.

2.3.1 PHI Received via Email

1. Open the email
2. Select *"Save As"*, and save the email as a file to the customer folder on the HIPAA drive only
3. Save the attachment(s), if applicable, out to the secure HIPAA drive as outlined above
4. Permanently delete the email; confirm email is also deleted from the *"Deleted Items"* folder. Be sure the email is not just *"moved"* to the *"Deleted Items"* folder
5. Reply to the sender of the email using the canned email text found in Appendix D reminding them of their HIPAA obligation of using secure, encrypted means to transmit HIPAA data.

NOTE: This process applies to Banking and Corporate Payments LOB's only; other processes are defined in the Paymode HIPAA POLICIES AND PROCEDURES documents*.*

2.3.1.1 Email PHI Procedures for Black Berry Users

In order to permanently delete items from your BlackBerry, received emails must first be moved to the „Deleted Items" folder. Once the BlackBerry synchronizes with the Outlook server and removes the item from the BlackBerry, you must then permanently delete, from Outlook, the item from the Deleted Items folder.

2.3.2 PHI Received via Secure Email, sFTP, or HTTPS

1. Move the file(s) to the secure HIPAA drive
2. If customer has used the Bottomline sFTP or HTTPS site delete the file(s) from the site.

NOTE: This process applies to Banking and Corporate Payments LOB's only, other processes are defined in the Paymode HIPAA POLICIES AND PROCEDURES documents.

2.3.3 PHI Received via Fax

If you receive a faxed mockup of a check image or other healthcare document that could contain PHI:

1. Print the sample
2. Delete the fax
3. All printed PHI must be shredded after Use or it may be discarded in a confidential data destruction receptacle. Never throw PHI in a trash can.

2.4 REQUIRED Secure Data Storage Process for HIPAA Customer Data

In order to appropriately secure "data at rest" PHI to comply with Safe Harbor, Bottomline requires use of the HIPAA Drive and Data Defense.

NOTE: This process applies to Banking and Corporate Payments LOB's only; other processes are defined in the Paymode HIPAA POLICIES AND PROCEDURES documents.

2.4.1 HIPAA Drive

Note: Further updates to this document will be published in the coming weeks outlining a new process for the HIPAA Drive.

IT has created a secure drive on the Bottomline network for containment of all HIPAA data. HIPAA data includes data files, form samples, PayView images, electronic copies of faxes and any and all other files that contain PHI. Requests for access to the HIPAA drive shall be submitted to the HIPAA contact for your LOB or the Privacy Officer.

1. Each employee requiring access to the HIPAA drive will be assigned authentication credentials including a certificate. Each employee is responsible for maintaining the security of his or her authentication credentials. No employee is permitted to: i) access the HIPAA drive using another employee's authentication credentials; ii) disclose authentication credentials to any other person, including other Bottomline employees.
2. At the start of a HIPAA customer engagement (new Services or Support call) you should first confirm if a customer folder is in existence by reviewing the HIPAA Drive directory. If a folder does not exist for the customer, create one.
3. Off of the main customer folder create the necessary subfolder/s for your current engagement. <u>Be sure to use the following naming convention of your subfolder so that it can be distinguished what project/incident the folder is for and who may be using it</u>.

   <Customer Name>_<Project/Incident Name>_<Project/Incident Owner First Initial and Last Name>

   Example: CHW_Wires Implemenation_KGervasio

   Example: Friendlys_Support Case 2345_MSchepis

   Example: Cigna_Wires QC 3209_EZic
4. ***You must delete all data files used in support of a project or support case once the project/case is completed.***

Note: Due to the length of the path to the files, you may encounter a Bottomline application error when trying to test your implementation with data located on the HIPAA drive. If you encounter such an error, temporarily move the data file to the root of the HIPAA drive and test from there. After you have completed the testing move the data file and any resulting system output files back to their appropriate sub directory on the HIPAA Drive.

2.4.2 Data Defense

All Workforce members who encounter or are required to work with PHI are required to have the Data Defense application installed on their laptops and/or workstations. PHI must only be moved and Used on a laptop or workstation equipped with Data Defense. Data Defense is a tool to encrypt data on the hard drive as well as mitigate risk of unauthorized individuals accessing PHI on that laptop or workstation. Installation and configuration instructions are outlined in Appendix C.

If you use more than one laptop or workstation, Data Defense must be installed on your primary system and that system must be the one used if and when you are dealing with PHI.

2.4.2.1 REQUIRED PHI Storage Process for Local Machine

Data Defense is configured to encrypt all files located in the C:\Documents and Settings\<user id>\My Documents folder on the device on which it is installed.

Any PHI stored on a laptop or workstation MUST be stored in the *"My Documents"* folder (or a subfolder off of My Documents) as this will ensure the data is encrypted. If Data Defense encryption of PHI is preventative of use with Bottomline software applications, the PHI may be temporarily moved to another unencrypted folder on the laptop/workstation for the purpose of providing specific services or support to the customer. It is the employee's responsibility to clean out and permanently delete PHI from any location on their workstation and/or laptop on a regular basis, not less than daily.

2.5 REQUIRED Bottomline Virtual Machine (VM) Process

This section is to be completed in a subsequent release of this document. Until that time, please continue to use VM's in normal business practice and in accordance with Bottomline IT standards.

2.6 Salesforce

Storage of PHI on Salesforce.com is prohibited; this includes all Salesforce.com objects, including but not limited to: opportunities/triggers, support cases, and professional services projects. Any PHI shall be stored as directed on the specified HIPAA drive.

2.7 CRM System

A warning label has been placed on the customer facing screens of Salesforce.com indicating to Covered Entity customers that they should not place PHI on the CRM.

If PHI is found on the CRM system it should be removed by the individual discovering the PHI and secured on the HIPAA drive and the individual should notify the LOB HIPAA resource of the finding.

2.8 Visual Source Safe (VSS)

Storage of PHI on VSS is prohibited. Any PHI must be stored as directed on the specified HIPAA drive.

2.9 Mercury Quality Center

Storage of PHI on Quality Center is prohibited. Any HIPAA data must be stored as directed on the specified HIPAA drive.

3 <u>Security Rule and Breaches of Security</u>

3.1 Security Rule Requirement

Bottomline is required to implement appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic PHI.

3.2 Mitigation and Breach Notification

HIPAA requires Bottomline to mitigate, to the extent practicable, any harmful effect that is known to Bottomline as a result of any unauthorized Use or Disclosure of PHI (a breach).

HITECH imposes a breach notification obligation on Bottomline. Generally, if there is an unauthorized Disclosure, Bottomline's customer and the affected individuals must be notified. If the breach affects a more significant number of individuals, more drastic measures including notification of government officials and imposition of fines may occur.

All Workforce members are required to report any known breach to the Privacy Officer or Human Resources.

Investigation of any report of any breach and determination of the need for mitigation and/or breach notification when PHI has been disclosed without authorization shall be determined on a case-by-case basis by the Privacy Officer in consultation with the LOB HIPAA Resource and Bottomline's executive management and/or legal counsel.

Depending on the circumstances of the breach, an investigation may include the following steps, as necessary based on the findings.

1. Documentation of the initiation of an investigation
2. Notification of internal parties as appropriate
3. Determination of the validity of the breach
4. If breach is substantiated:
   a. Notification of appropriate parties
   b. Identification of the cause
   c. Implementation of measures to prevent reoccurrence
   d. Determination of potential impact of known occurrences
   e. Implementation of measures to mitigate impact
   f. Follow-up on Workforce sanctions
5. If breach is unsubstantiated:
   a. Determination of intent of report
   b. Notification of appropriate parties
   c. Follow-up on Workforce sanctions (if report had malicious intent)
6. Completion/filing of case documentation

If the investigation confirms a breach of Privacy Policy and procedures, steps shall be taken to contain any potential harm to the subject of the PHI and to assure no future unauthorized Uses or Disclosures. If the breach of the policy and procedures is the direct result of an employee's action or inaction, it will be referred to the individual's manager and/or Human Resources for review and appropriate disciplinary action.

3.3 Safe Harbor

Breach notifications are not applicable when PHI has been encrypted and security of the decryption key has not been breached.

Bottomline intends to utilize encryption for purposes of taking advantage of Safe Harbor when practical. This section describes requirements for taking advantage of Safe Harbor:

3.3.1 Data in Motion Requirements

When electronically transmitting files containing PHI, the PHI is considered “data in motion” and securing the PHI to comply with Safe Harbor requires that the PHI be protected by encryption meeting minimum requirements.

Note: The following commonly used password protection methods are NOT acceptable encryption:

- WinZip
- Microsoft Word or Excel password protection

3.3.2 Data at Rest Requirements

Files stored on any media, including a hard drive on a laptop, workstation or network drive are considered “data at rest” and securing the PHI to comply with Safe Harbor requires that the PHI be protected by encryption meeting minimum requirements.

Bottomline LOBs may implement more detailed protocols for implementing safe harbor principals for securing PHI as appropriate.

4 Privacy Rule

Bottomline Workforce members are responsible for assuring that confidential customer information (including PHI) is protected from unauthorized Use or Disclosure and is used only for the purpose for which it was disclosed to Bottomline.

Bottomline and its Workforce members take reasonable steps to limit the Use and Disclosure of PHI - in amount and number of individuals - needed to accomplish the intended purpose for which the PHI is required.

A Workforce member’s Use and Disclosure of PHI must be only as is reasonably necessary to perform the services and support on behalf of its customers. No Workforce member is permitted to:

a) Access or Use any PHI other than the minimum necessary to perform his or her responsibilities for the customer;

b) Disclose any PHI (or any file containing PHI) to any person other than another Workforce Member;

c) Disclose PHI to any other Workforce member who does not require access to the information.

All Workforce members are required to:

a) Only request PHI when absolutely needed.

b) Not keep PHI on their desk, on laptop/desktop hard drive, or anywhere where it could be inadvertently disclosed to any other person.

c) All printed PHI must be shredded after Use or it may be discarded in a confidential data destruction receptacle. Never throw PHI in a trash can.

d) Take reasonable steps to verify the identity and authority of any person or entity requesting access to proprietary customer data and PHI.

5 Training

All Bottomline Workforce members will receive policy and procedures documentation upon joining the Bottomline team. All Workforce members that require access to PHI must also attend an annual training and sign off on Bottomline HIPAA policies

In addition, Bottomline may provide additional privacy awareness and/or security training to Workforce members as Bottomline deems appropriate for their job responsibilities.

6 Ongoing Compliance

In order to protect proprietary customer information, ensure confidentiality and privacy compliance with HIPAA, and to maintain accurate and relevant privacy policies and procedures, Bottomline will undergo periodic compliance and self-assessment activities. Bottomline will allocate appropriate personnel and resources as necessary and reasonable to maintain compliance.

The Privacy Officer is responsible for all ongoing activities related to the development, implementation, communication, training, maintenance of, and adherence to Bottomline's policies and procedures covering the privacy of, and access to, PHI in compliance with HIPAA and HITECH, including a regular assessment of Bottomline's physical environment and staff practices to identify potential risks to improper Disclosure of PHI. Such assessment is expected to include:

1. A regular review of Bottomline's policies and procedures for compliance with the latest versions of applicable statutes.
2. A regular assessment of the effectiveness of Bottomline's policies and procedures including the effectiveness of safeguards.
3. A regular assessment of the degree to which Workforce members are adhering to privacy policies and procedures.
4. A regular assessment of physical and electronic threats and safeguards to ensure that PHI is Used, Disclosed, and stored safely and confidentially.
5. Documentation and reporting to Bottomline Management the results of this analysis for review by Bottomline's management team.
6. Remediation of any deficiencies identified by Bottomline's management team, including any update to these Policies and Procedures that are appropriate.

The assessment spreadsheet attached as Appendix A will be used to facilitate assessments.

7 Accounting of Disclosures

Bottomline must document certain Disclosures of PHI to enable the Covered Entity customer to respond to requests from an individual for an accounting of Disclosures of that individual's PHI.

This documentation requirement pertains to certain non-routine Disclosures outside of normal business practices, generally:

1. As Required By Law (i.e. Bottomline receives a subpoena)
2. Judicial and Administrative Proceedings

In the event any Workforce member is asked to Disclose PHI outside of normal business practice, that person must notify the Privacy Officer and/or the HIPAA LOB Resource prior to such Disclosure. The Privacy Officer will work with the appropriate legal resources to determine whether the Disclosure should be made. In the event the Disclosure is granted the Privacy Officer will document the appropriate Disclosure information.

Bottomline will also account for any unauthorized Disclosures as they become known.

For purposes of monitoring internal compliance of these protocols, an LOB may establish policies and procedures for tracking/logging workforce member access to PHI.

8 Relationship to Other Policies and Procedures

The HIPAA Compliance Policy and Procedures are supplemental to all existing Bottomline policies and procedures.

Each LOB may have specific protocols related to privacy and/or Use and Disclosure of confidential information (including PHI). Workforce members subject to those specific policies are expected to comply with these Policies and Procedures as well as those specific protocols.

9 Sanctions and "Whistleblower"

Bottomline is required to have sanctions for failure to comply with these policies and procedures. Disciplinary actions may be taken in the event an employee fails to adhere to policies and procedures regarding PHI whether the failure is either: unintentional; intentional; or for malicious intent or personal gain. The severity of disciplinary action taken as a result of failure to adhere to these policies and procedures will be based on the complete discretion of Bottomline management and includes, but is not limited to, required retraining on HIPPA policies, verbal and written warnings, re-assignment of responsibilities, and/or termination.

Employees are permitted to file complaints regarding these policies and procedures ***or noted instances of*** failure to comply. Bottomline's "Whistleblower" policy applies. Bottomline will not retaliate or permit reprisals against an employee who reports a breach to the integrity and confidentiality of PHI as long as such report is made on a good faith basis. Any employee involved in retaliatory behavior or reprisals against another for reporting such infractions may be subject to disciplinary action up to and including termination.

In the event that violation of Bottomline's policies constitutes a criminal offense under State or Federal statutes, the violator should expect that Bottomline will provide information concerning the violation to appropriate law enforcement personnel and that Bottomline will cooperate with any law enforcement investigation or prosecution.

APPENDIX A: Audit Assessment Tool

Purpose: Periodic review of Bottomline's administrative, technical, and physical safeguards to protect the privacy of PHI.

The Privacy Officer will schedule periodic reviews with the HIPAA LOB Resources and other appropriate individuals to review Bottomline's administrative, technical, and physical safeguards to protect the privacy of PHI and compliance therewith – including these HIPAA Compliance Policies and Procedures and the technology, architecture, policies, and procedures related to security of PHI described in Bottomline's Information Security Plan.

1. **Physical Safeguards:**

    a. Is access to the work areas containing PHI restricted to Bottomline Workforce members and other authorized individuals using suitable access devices (proximity card system, key lock, combination lock, etc.)?

    b. Are all keys/access cards accounted for (documented evidence), and are they collected from Workforce members upon termination or when access to the area is no longer required?

    c. Are authorized personnel identified in such a way, such that others can easily recognize them as being authorized to access a controlled area?

    d. Are any external doors in the area regularly propped open and/or left unmonitored during temporary use (e.g., smoker access, deliveries, trash/recycling collection, vending machine maintenance, etc.)?

    e. Are all windows in the room (if any open) locked and/or secured?

    f. Are workstations where PHI is used being locked when unattended?

    g. Are server rooms secure (may be evaluated in conjunction with overall security review):

        i. Is access to the server areas restricted to authorized Bottomline workforce members only using suitable access devices (proximity card system, key lock, combination lock, etc.)?

        ii. Is the server room where PHI is stored continually monitored during the hours of operation?

2. **PHI in hard copy form:**

    a. Identify instances where PHI in hard copy form exists or is used.

    b. Is hardcopy PHI secured in locking filing cabinets, file racks, drawers, or other secure means?

    c. Is hardcopy PHI being secured when unattended?

    d. Is hardcopy PHI being shredded when no long needed (shredded on site, not the confidential bins)?

    e. Can processes and procedures be altered to reduce use of PHI in hard copy?

3. **PHI on portable media:**

a. Identify instances where PHI is stored on portable media such as thumb drives, floppy discs, microfilm, microfiche, CD, etc.

b. Is media secured in locking file cabinets, file racks, drawers, etc.?

c. Is media secured when unattended?

d. Is media wiped or shredded when no longer needed?

e. Can processes and procedures be altered to eliminate PHI on portable media?

4. Technical Safeguards

a. Is technology used to secure PHI at secure locations sufficient in view of contemporary threats? This may be evaluated in conjunction with overall threat assessment of Bottomline's systems.

b. Are processes for accessing and using PHI from secure locations appropriately restricting access to authorized individuals, do processes need modification?

c. Are passwords being sufficiently protected (sufficient strength, regularly changes, not posted or visible)?

d. Are all machines where PHI is used covered by appropriate encryption technology (i.e. Data Defense)?

e. Have any new locations of unsecured PHI been identified? Has the location been assessed for risk and appropriate steps taken to protect the PHI?

5. Policies and Procedures.

a. Review of Privacy Policy. Does it require updating?

b. Review policy and procedures. Do they represent reasonable efforts to ensure the minimum necessary amount of PHI is used and disclosed by appropriate persons and within the limits of Bottomline's technological capabilities? Is updating required?

c. Review policy/procedure for verifying the identity and authority of persons requesting PHI. Does it require updating?

d. Review policy/procedure for accounting for the disclosure of PHI. Does it require updating?

e. Review resources in roles of Privacy Officer and HIPAA LOB Resources. Is updating required?

f. Review sanctions policy for failure to comply with HIPAA policies and procedures. Does it require updating?

g. Review "Whistleblower Policy". Does it require updating?

h. Review policies and procedures related to investing reported breaches of PHI and notification. Does it require updating?

i. Review policies and procedures for mitigating any harmful effect of the use or disclosure of PHI. Does it require updating?

j. Review Business Associate standards for use with Vendors obtaining PHI from Bottomline. Do they require updating?

k. Review Business Associate policies for Covered Entity Customers. Do the policies require updating?

l. Review HIPAA Training Outline. Does it require updating?

m. Review policies and procedures, if any, related to de-identification. Do policies require updating?

6. Compliance Review

a. Accounting for Disclosures:

  i. Information shall include: date of disclosure; name and address, if known, of the person or organization that received the information; brief description of information disclosed and the purpose for which the information was disclosed information disclosed.

  ii. Records to be kept for 6 years.

b. Is access to PHI at secure locations limited to using PHI as needed to fulfill responsibilities to customers?

c. Identify vendors obtaining PHI from Bottomline. Are Business Associate Agreements in place?

d. Have all new hires been given the PHI overview and sign off sheet as part of new hire procedures?

e. Have all the necessary and appropriate Workforce members been through HIPAA training within the past year?

  i. Have appropriate records been kept?

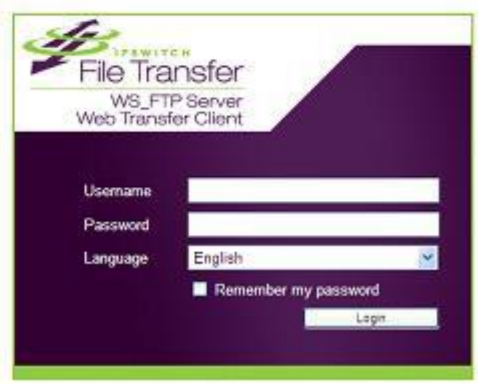
  ii. Have Workforce members signed the training acknowledgement form?

APPENDIX B: Using sFTP and HTTPS for Data Transmission

Secure File Transfer via HTTPS (Secure HTTP)

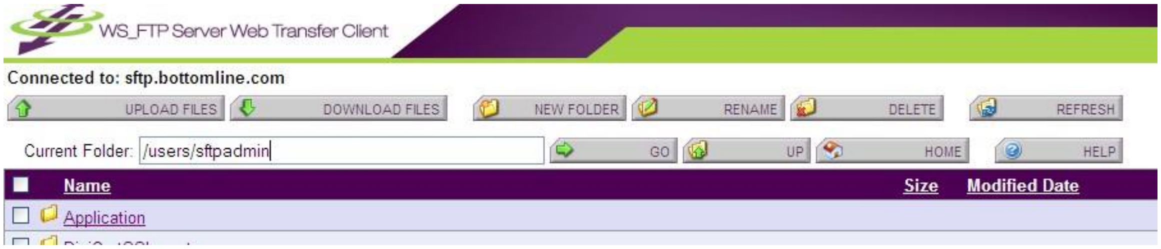
1. If you do not have credentials to the Bottomline SFTP site, you must first submit a ticket to IT. Credentials can be issued to both Bottomline employees as well as to customers for secure sending or receipt of files. A Bottomline employee must request permissions on behalf of a customer.
2. To access the SFTP server, use the following URL with Internet Explorer or Firefox:

   https://sftp.bottomline.com/thinclient/Login.aspx



Language: English

3. Logon to the server using supplied credentials.

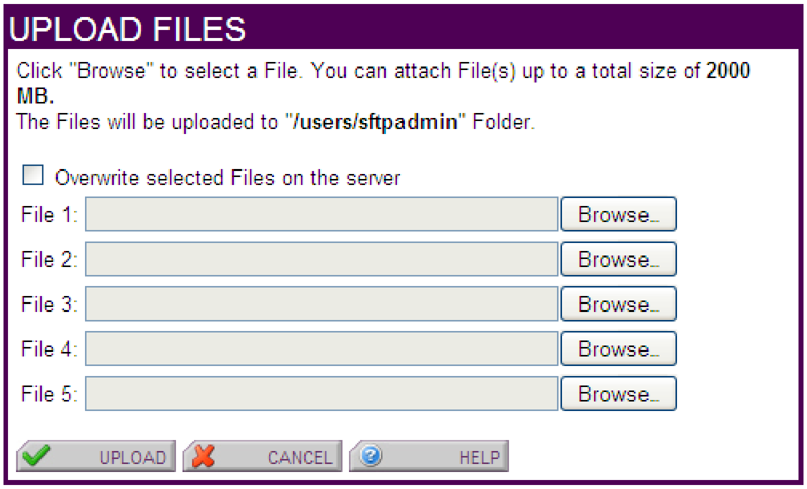


Connected to: sftp.bottomline.com

Current Folder: /users/sftpadmin

□ Application

4. To upload a file click the **Browse** button and select files, click **Upload**.



UPLOAD FILES

Click "Browse" to select a File. You can attach File(s) up to a total size of **2000 MB.**
The Files will be uploaded to "**/users/sftpadmin**" Folder.

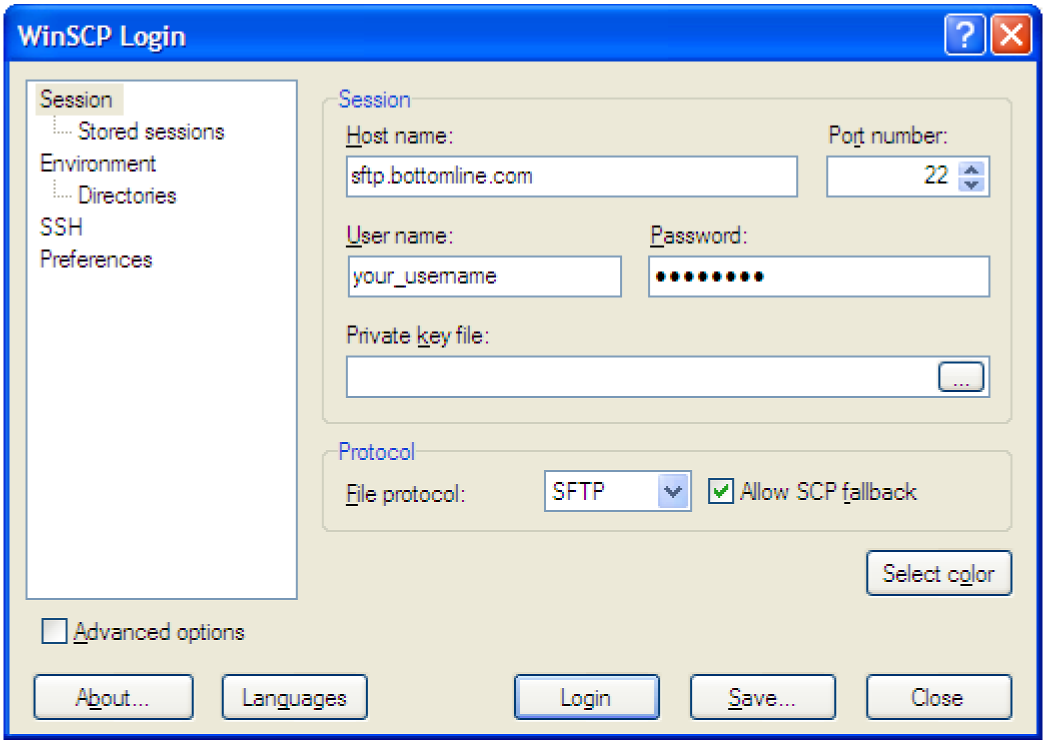
□ Overwrite selected Files on the server

File 1: Browse...
File 2: Browse...
File 3: Browse...
File 4: Browse...
File 5: Browse...

5. To download files, select the check boxes for the files you want to retrieve and click on the **Download File** button.

File Transfer via SFTP

1. Download and install an SFTP client such as WinSCP, which can be downloaded from this URL: http://winscp.net/eng/download.php
2. Once installed, launch WinSCP. Enter the Host name (sftp.bottomline.com) and the user name and password, assigned by IT.



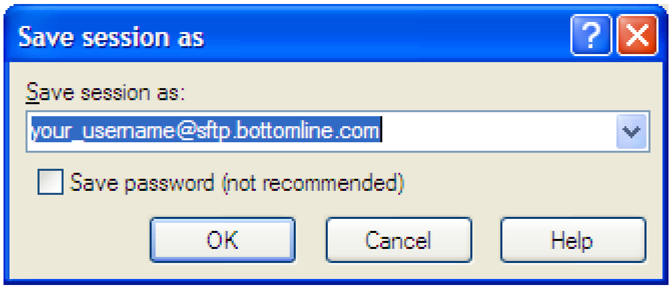
WinSCP Login

Session
Host name: sftp.bottomline.com
Port number: 22
User name: your_username
Password: ●●●●●●●●●
Private key file:

Protocol
File protocol: SFTP
☑ Allow SCP fallback

□ Advanced options

3. Then click on the **Save** button to have the profile saved for future connections.

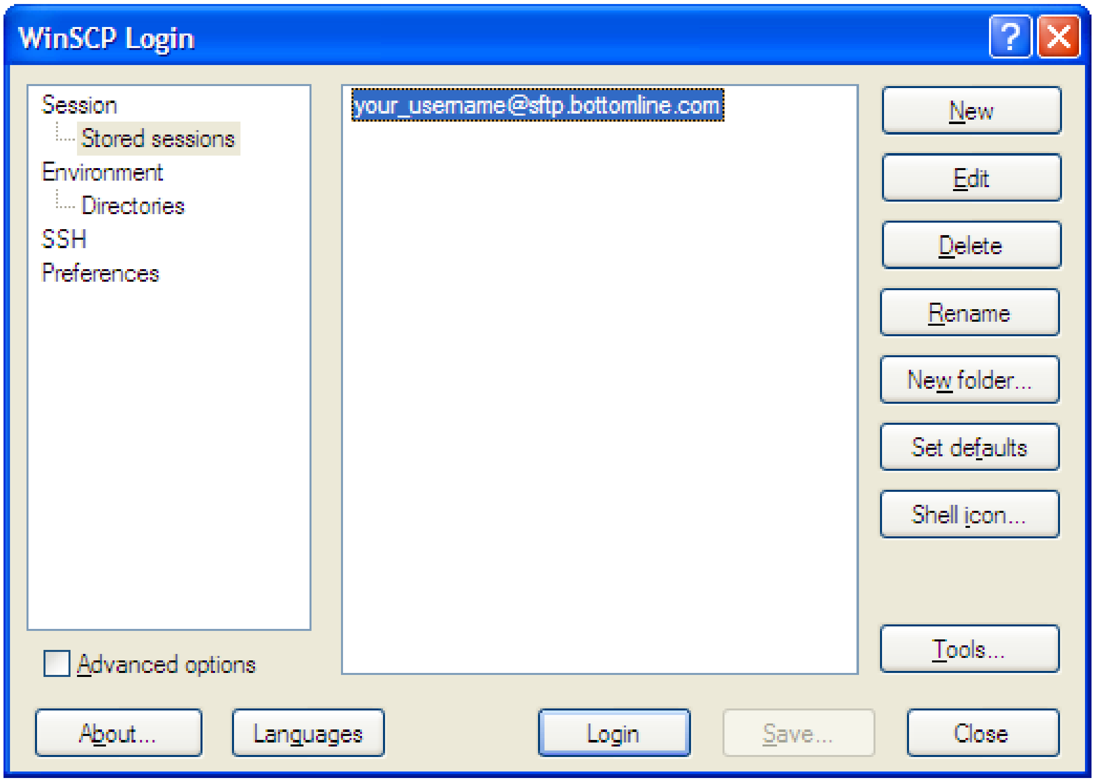


Save session as

Save session as: your_username@sftp.bottomline.com

☐ Save password (not recommended)

4. Accept the default name or enter your preferred name. Click on the **OK** button.

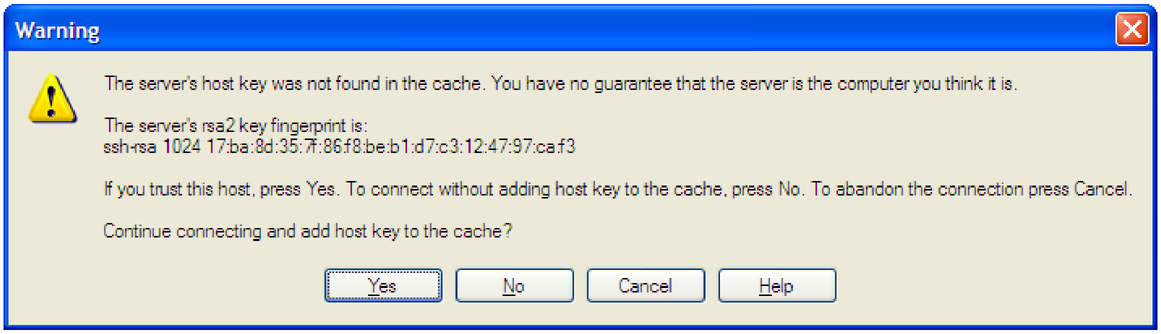


WinSCP Login

your_username@sftp.bottomline.com

☐ Advanced options

5. Click on the **Login** button and enter your password if needed. Upon initial connection, you will be asked to accept the servers SSL keys. Click on the **Yes** button and continue.



Warning

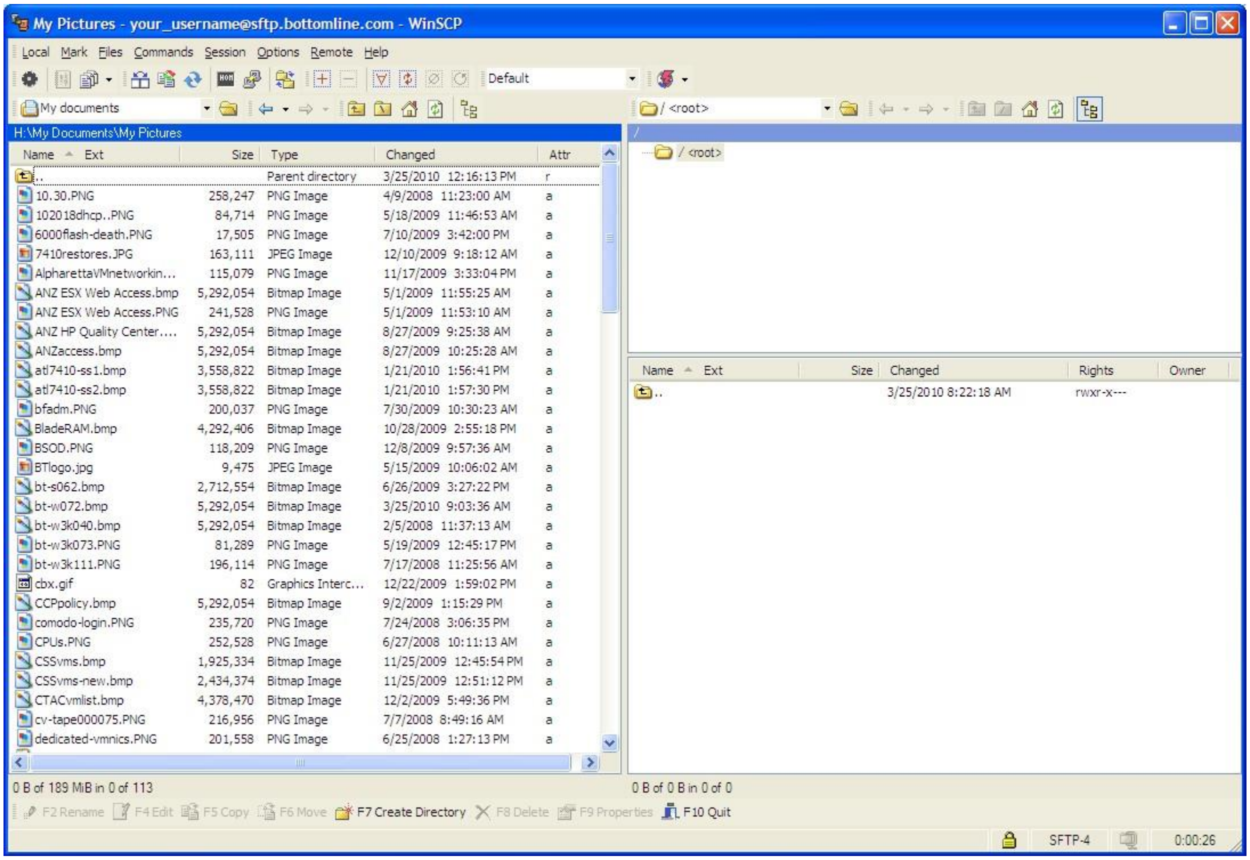
The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:
ssh-rsa 1024 17:ba:8d:35:7f:86:f8:be:b1:d7:c3:12:47:97:ca:f3

If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

Continue connecting and add host key to the cache?

6. You will then be presented with the following screen. The left panel is your local system and the right side is the SFTP server, with the folder tree in the upper panel and its contents in the lower.



My Pictures - your_username@sftp.bottomline.com - WinSCP

H:\My Documents\My Pictures

Name Ext	Size	Type	Changed	Attr
..		Parent directory	3/25/2010 12:16:13 PM	r
10.30.PNG	258,247	PNG Image	4/9/2008 11:23:00 AM	a
102018dhcp..PNG	84,714	PNG Image	5/18/2009 11:46:53 AM	a
6000flash-death.PNG	17,505	PNG Image	7/10/2009 3:42:00 PM	a
7410restores.JPG	163,111	JPEG Image	12/10/2009 9:18:12 AM	a
AlpharettaVMnetworkin...	115,079	PNG Image	11/17/2009 3:33:04 PM	a
ANZ ESX Web Access.bmp	5,292,054	Bitmap Image	5/1/2009 11:55:25 AM	a
ANZ ESX Web Access.PNG	241,528	PNG Image	5/1/2009 11:53:10 AM	a
ANZ HP Quality Center....	5,292,054	Bitmap Image	8/27/2009 9:25:38 AM	a
ANZaccess.bmp	5,292,054	Bitmap Image	8/27/2009 10:25:28 AM	a
atl7410-ss1.bmp	3,558,822	Bitmap Image	1/21/2010 1:56:41 PM	a
atl7410-ss2.bmp	3,558,822	Bitmap Image	1/21/2010 1:57:30 PM	a
bfadm.PNG	200,037	PNG Image	7/30/2009 10:30:23 AM	a
BladeRAM.bmp	4,292,406	Bitmap Image	10/28/2009 2:55:18 PM	a
BSOD.PNG	118,209	PNG Image	12/8/2009 9:57:36 AM	a
BTlogo.jpg	9,475	JPEG Image	5/15/2009 10:06:02 AM	a
bt-s062.bmp	2,712,554	Bitmap Image	6/26/2009 3:27:22 PM	a
bt-w072.bmp	5,292,054	Bitmap Image	3/25/2010 9:03:36 AM	a
bt-w3k040.bmp	5,292,054	Bitmap Image	2/5/2008 11:37:13 AM	a
bt-w3k073.PNG	81,289	PNG Image	5/19/2009 12:45:17 PM	a
bt-w3k111.PNG	196,114	PNG Image	7/17/2008 11:25:56 AM	a
cbx.gif	82	Graphics Interc...	12/22/2009 1:59:02 PM	a
CCPpolicy.bmp	5,292,054	Bitmap Image	9/2/2009 1:15:29 PM	a
comodo-login.PNG	235,720	PNG Image	7/24/2008 3:06:35 PM	a
CPUs.PNG	252,528	PNG Image	6/27/2008 10:11:13 AM	a
CSSvms.bmp	1,925,334	Bitmap Image	11/25/2009 12:45:54 PM	a
CSSvms-new.bmp	2,434,374	Bitmap Image	11/25/2009 12:51:12 PM	a
CTACvmlist.bmp	4,378,470	Bitmap Image	12/2/2009 5:49:36 PM	a
cv-tape000075.PNG	216,956	PNG Image	7/7/2008 8:49:16 AM	a
dedicated-vmnics.PNG	201,558	PNG Image	6/25/2008 1:27:13 PM	a

0 B of 189 MiB in 0 of 113

/

/ <root>

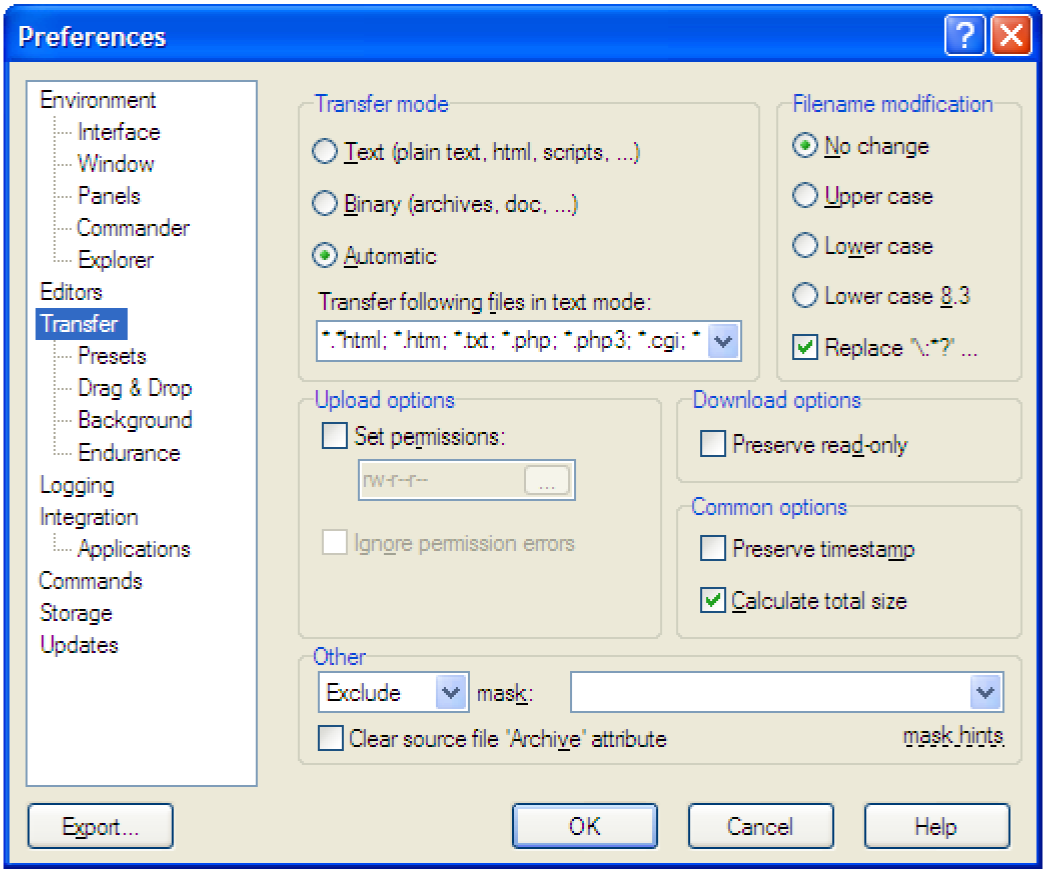
Name Ext	Size	Changed	Rights	Owner
..		3/25/2010 8:22:18 AM	rwxr-x---	

0 B of 0 B in 0 of 0

SFTP-4 0:00:26

7. Before you transfer any data, from the top menus, select **Options -> Preferences** and select **Transfer**.

8. Under **Upload options,** ensure that **Set Permissions** is unchecked. Click **OK**.



Transfer mode

○ Text (plain text, html, scripts, ...)
○ Binary (archives, doc, ...)
● Automatic

Transfer following files in text mode: *.*html; *.htm; *.txt; *.php; *.php3; *.cgi; *

Filename modification

● No change
○ Upper case
○ Lower case
○ Lower case 8.3
☑ Replace '\:*?' ...

Upload options

☐ Set permissions:
rw-r--r--
☐ Ignore permission errors

Download options

☐ Preserve read-only

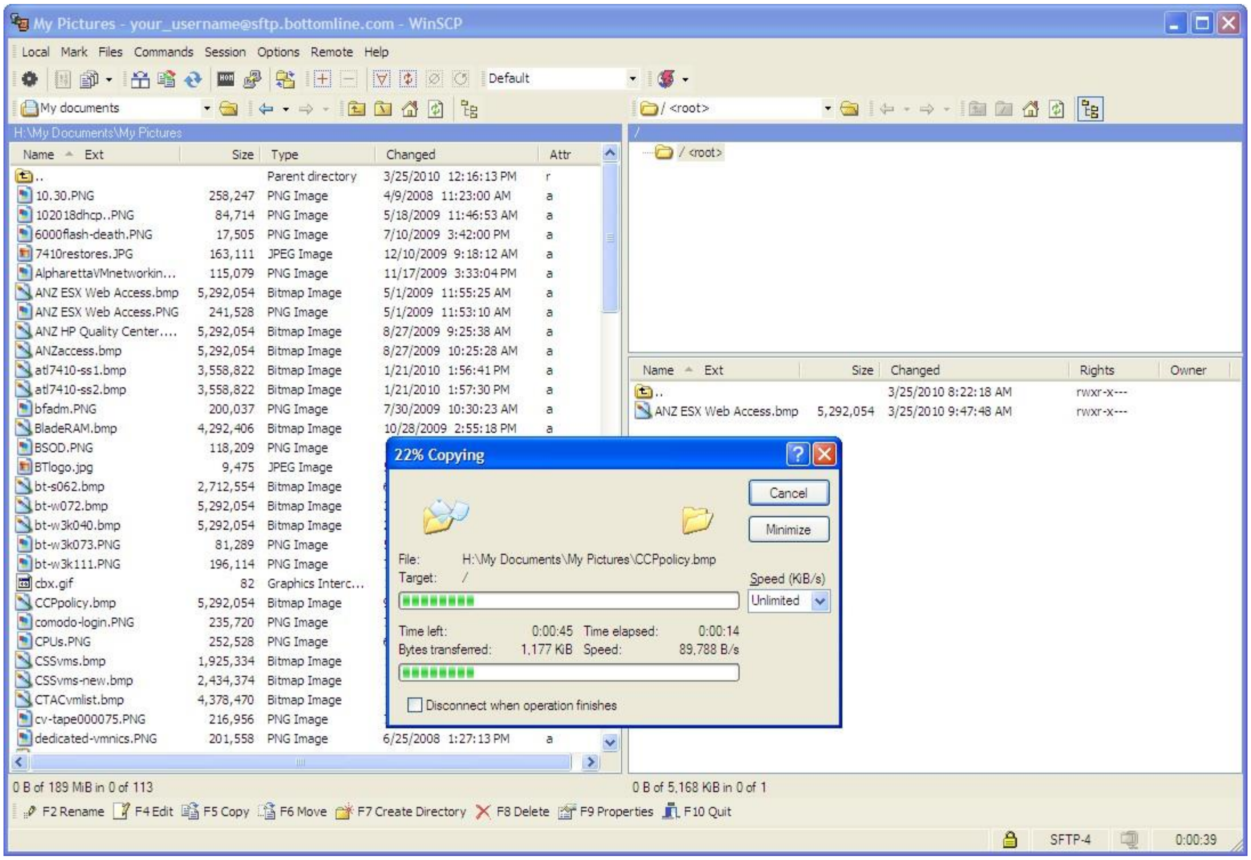
Common options

☐ Preserve timestamp
☑ Calculate total size

Other

Exclude mask:
☐ Clear source file 'Archive' attribute
mask hints

9. To transfer files, simply drag and drop them one direction or the other depending on if you are uploading to or downloading from the SFTP server. To upload, drag a file or folder from your local system on the left over to lower right pane. To download, do vice versa.



H:\My Documents\My Pictures

Name Ext	Size	Type	Changed	Attr
..		Parent directory	3/25/2010 12:16:13 PM	r
10.30.PNG	258,247	PNG Image	4/9/2008 11:23:00 AM	a
102018dhcp..PNG	84,714	PNG Image	5/18/2009 11:46:53 AM	a
6000flash-death.PNG	17,505	PNG Image	7/10/2009 3:42:00 PM	a
7410restores.JPG	163,111	JPEG Image	12/10/2009 9:18:12 AM	a
AlpharettaVMnetworkin...	115,079	PNG Image	11/17/2009 3:33:04 PM	a
ANZ ESX Web Access.bmp	5,292,054	Bitmap Image	5/1/2009 11:55:25 AM	a
ANZ ESX Web Access.PNG	241,528	PNG Image	5/1/2009 11:53:10 AM	a
ANZ HP Quality Center....	5,292,054	Bitmap Image	8/27/2009 9:25:38 AM	a
ANZaccess.bmp	5,292,054	Bitmap Image	8/27/2009 10:25:28 AM	a
atl7410-ss1.bmp	3,558,822	Bitmap Image	1/21/2010 1:56:41 PM	a
atl7410-ss2.bmp	3,558,822	Bitmap Image	1/21/2010 1:57:30 PM	a
bfadm.PNG	200,037	PNG Image	7/30/2009 10:30:23 AM	a
BladeRAM.bmp	4,292,406	Bitmap Image	10/28/2009 2:55:18 PM	a
BSOD.PNG	118,209	PNG Image		
BTlogo.jpg	9,475	JPEG Image		
bt-s062.bmp	2,712,554	Bitmap Image		
bt-w072.bmp	5,292,054	Bitmap Image		
bt-w3k040.bmp	5,292,054	Bitmap Image		
bt-w3k073.PNG	81,289	PNG Image		
bt-w3k111.PNG	196,114	PNG Image		
cbx.gif	82	Graphics Interc...		
CCPpolicy.bmp	5,292,054	Bitmap Image		
comodo-login.PNG	235,720	PNG Image		
CPUs.PNG	252,528	PNG Image		
CSSvms.bmp	1,925,334	Bitmap Image		
CSSvms-new.bmp	2,434,374	Bitmap Image		
CTACvmlist.bmp	4,378,470	Bitmap Image		
cv-tape000075.PNG	216,956	PNG Image		
dedicated-vmnics.PNG	201,558	PNG Image	6/25/2008 1:27:13 PM	a

/

Name Ext	Size	Changed	Rights	Owner
..		3/25/2010 8:22:18 AM	rwxr-x---	
ANZ ESX Web Access.bmp	5,292,054	3/25/2010 9:47:48 AM	rwxr-x---	

22% Copying

File: H:\My Documents\My Pictures\CCPpolicy.bmp
Target: /
Speed (KiB/s): Unlimited
Time left: 0:00:45 Time elapsed: 0:00:14
Bytes transferred: 1,177 KiB Speed: 89,788 B/s
☐ Disconnect when operation finishes

0 B of 189 MiB in 0 of 113

0 B of 5,168 KiB in 0 of 1

10. Once done, either continue to transfer files or simply close the target.

Using FTP from a UNIX system

You may also use the UNIX “scp” command to copy files to and from the SFTP server.

Example:

```
$ scp filename your_username@sftp.bottomline.com:
your_username@sftp.bottomline.com's password: ********
filename                              100%       720    0.7KB/s     00:00
$
```

APPENDIX C: Installation & Configuration of Data Defense

If your position requires that you occasionally and temporarily have PHI on your laptop or desktop, you are required to have Data Defense installed. Data Defense is a security application that encrypts data as well as provides data destruction in the event of loss, theft, or other unauthorized access. To request an installation first acquire your manager's approval, then send an IT ticket via iPortal; specific installation instructions will be provided by IT.

Iron Mountain Data Defense

Iron Mountain Data Defense is an encryption and data destruction software package. The settings are policy based and cannot be modified by individual users. The data on the device is encrypted by file type and data location. Data destruction is triggered by specific rules set for the machine. If you report your laptop as stolen, IT will change the status to stolen.   When the computer comes online the data destruction will begin.

Data Destruction Triggers

- Device is Lost (shut down)
  - Device is lost
  - Persistent shut down
- Failed Logon Attempts (5)
  - On 5 consecutive failed logons
  - Shut down
- Failed Logon Attempts (7)
  - On 7 consecutive failed logons
  - Display message
    - Your device is experiencing a system failure. Please contact the Help Desk for assistance.
- Failed Logon Attempts (8)
  - On 8 consecutive failed logons
  - Secure delete filesoverwrite 1x
    - <EFS_CERTS>\
    - This deletes the encryption keys from your device nullifying your ability to read encrypted files should you regain access to your system; contact the Help Desk for assistance in possible recovery of data.
- Failed Logon Attempts (9)
  - On 9 consecutive failed logons
  - Shut down
- Unrecoverable (shut down)
  - Unrecoverable expires (2 months)
  - Persistent shut down

- Out of Contact
    - Out of contact expires (1 month)
    - Secure delete filesoverwrite 1x
        - <EFS_CERTS>\
- Device is Stolen
    - Device is stolen
    - Secure delete filesoverwrite 3x
- Lock Computer (10 minutes)
    - Idle
    - Lock computer

Data Encryption Policy

The following directories and file types outline what specific files on the device will be encrypted by Data Defense.

- All files located in C:\Documents and Settings\<user id>\My Documents
    - IMPORTANT NOTE: it is the users‟ responsibility to ensure that any and all HIPAA data is stored in the designated My Documents folder (or in a HIPAA subfolder off of My Documents) for proper PHI encryption. Additionally the user must ensure that any residual data due to use of PHI for customer services and/or support is removed from all locations on the laptop/desktop. This includes but is not limited to: .pdf files, *.out files, *.tmp, files, etc.

APPENDIX D: Email Response for Customer Non-Compliance

Dear Customer,

We received <FILE NAME> from you via email on <DATE> which appears to include unsecured PHI. Regulations under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act do not permit the transfer of unsecured PHI by plain email or other unencrypted transmission means. We are taking steps to secure the PHI as expeditiously as possible, as required by your Business Associate Agreement. Please contact me for details on utilizing secure processes and technologies for transmission of PHI.

GLOSSARY

ARRA	The American Recovery and Reinvestment Act of 2009.
Business Associate	As defined by HIPAA, a business associate is a person or entity who on behalf of a Covered Entity performs a function or service involving the Use of PHI.
Clearinghouse	A person or entity operating between a healthcare provider and health plans, for example an entity that takes PHI and formats it using standard coded format.
Covered Entity	HIPAA defines the following as covered entities: (1) healthcare providers who transmit data electronically, (2) health plans, and (3) healthcare clearinghouses.
Disclosure	The release, transfer, provision of, access to, or divulging in any other manner, of PHI outside of Bottomline.
HIPAA	The United States Health Insurance Portability and Accountability Act of 1996.
HITECH	The Health Information Technology for Economic and Clinical Health Act.
PHI	Protected Health Information, PHI comprises any information that i) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.
Privacy Officer	Designated Bottomline associate who is responsible for overseeing the implementation of this policy and related procedures.
Privacy Rule	Regulations promulgated by Department of Health and Human Services defining permissible Uses and Disclosures of PHI.
Production PHI	As used in this policy, production data refers to PHI used to provide Paymode services to customers and to send electronic payment and remittance information.
Non Production PHI	As used in this policy, non-production data refers to PHI used to provide non-production services, for example support services.
Security Rule	Regulations promulgated by Department of Health and Human Services defining required administrative, technical and physical safeguards for protecting electronic PHI.

Transactions Rule

The Transactions Rule defines standard formats which must be used for the electronic exchange of certain healthcare documents.

Use

The sharing, employment, application, utilization, examination, or analysis of PHI.

Workforce

Includes Bottomline employees, associates, temporary employees, consultants, on-location contractors, and agents.