

---

# Electronic Transaction Manual for Arkansas Blue Cross Blue Shield

## **HIPAA Transaction Companion Document Guide**

---

### **Refers to the X12N Implementation Guides:**

**004010X092A1: (270/271) Health Care Eligibility  
Benefit Inquiry and Response**

**004010X093A1: (276/277) Health Care Claim  
Status Request and Response**

**004010X094A1: (278) Health Care Services Review  
– Request for Review and  
Response**

## **INTRODUCTION**

The ASC X12N Implementation Guides were adopted under HIPAA as the official guides to use for the exchange of electronic transactions. This Electronic Transaction Manual contains the Companion Documents for the 270/271, 276/277 and 278 transactions. The Companion Documents provide further clarification and specifies the data content when exchanging electronic transactions with Arkansas Blue Cross Blue Shield. Transmissions based on this companion document, used in tandem with the X12N Implementation Guides, are compliant with both the X12 syntax and those guides. These Companion Guides are intended to convey information that is within the framework of the ASC X12N Implementation Guides adopted for use under HIPAA. The Companion Guides are not intended to convey information that in any way exceeds the requirements or usages of data expressed in the Implementation Guides. The Companion Guides on the next few pages describe the requirements and recommendations of implementing 270/271, 276/277 and 278 transactions.

The hours of operation for submitting ANSI 27X transactions are 6:00 a.m. to 12:00 a.m. CST, Monday through Saturday.

As of May 23, 2008, per HIPAA regulations, NPI will be required on all transactions instead of the Blue Cross provider id assigned by Arkansas Blue Cross Blue Shield.

## **27X Connections**

ANSI 27X transactions will be sent to Arkansas Blue Cross Blue Shield via secure internet connections in secure HTTP wrappers. The test and production URLs will be provided by EDI Services upon completion of enrollment. Arkansas Blue Cross Blue Shield will strip the wrappers and then pass the transactions to the submitter authentication. Arkansas Blue Cross Blue Shield will support either HTTP 1.0 or HTTP 1.1. The wrapper formats are as follows:

### **Request (Request Interchange)**

GET /ELIG HTTP/1.0

Accept: \*/\*

Connection: Close

Content-Length: **xxx** (**xxx** = content length)

Content-type: text/ansix12

### **Response (Reply Interchange)**

HTTP/1.0 200 OK

Date: **ddd** (**ddd** = date, example = Sat Jul 12 23:50:04 2003)

Content-type: text/ansix12

Content-Length: **xxx** (**xxx** = content length)

Password-expire: **ppp** (**ppp** = expiration, example = 3 days)

## **Passwords**

A clearinghouse submitter ID will be assigned to submitters by EDI Services at Arkansas Blue Cross Blue Shield. Submitters will be able to change passwords prior to expiration by using a maintenance transaction (PWC). A TA1 or a 997 response transaction with the error status will be returned if the transaction does not pass authentication.

Submitters must have a valid password. Standard password rules are:

- When using the password change (PWC) transaction, the old password specified in the transaction must match the current password.
- The password must be a minimum of 8 characters and a maximum of 10 characters.
- The password must be different from the initial password assigned by EDI Services.
- The password cannot be the same as the current password.
- The password cannot contain the clearinghouse submitter ID.
- Adjacent characters or symbols cannot be the same. e.g., Aef119F2 is invalid because of the two ones that are adjacent
- The password is case sensitive.
- The password must be changed at least every 30 days.

EDI Services will also create a clearinghouse organization in AHIN so that one or more users can be added for the clearinghouse. At least one user will need to be added and this user (or users) will be responsible for the initial setting and maintenance of the clearinghouse password which is required by the transaction (/ELIG) interface. It is strongly recommended that each vendor set up two users who can manage the account.

Submitters will be able to change passwords before they expire without logging on to AHIN by using the following maintenance transaction:

### **Request**

POST /PWC HTTP/1.0

Accept: \*/\*

Connection: close

Content-Length: 0

Content-type: text/plain

Userid=**xxx**&oldpass=**yyy**&newpass=**zzz** (where **xxx** = user ID, **yyy** = old password and **zzz** = new password)

**NOTE:** The line above is not part of the actual HTTP header. It should be separated from the HTTP header by a carriage return / line feed (CRLF). This transaction should be sent without an X12 transaction.

### **Good Response**

HTTP/1.0 202 Accepted

### **Error Response**

HTTP/1.0 406 Not Acceptable

If you supply an incorrect old password without a successful login more than 3 times or if the password expires prior to execution of the maintenance transaction, the account will be locked and must be reset by logging on to AHIN and resetting the clearinghouse password.

Additionally, a text string will be returned indicating the status of the request. Possible values are:

- Password changed successfully.
- Invalid parameters. Usage is: `userid=xxx&oldpass=yyy&newpass=zzz`
- AHIN is currently offline for maintenance. Please try again later.
- System Error. AHIN Administration has been notified.
- Unable to locate userid
- Account is locked. Please logon to AHIN in order to reset your clearinghouse account/password.
- Old password incorrect. Too many failed attempts. Account is locked. Please logon to AHIN in order to reset your clearinghouse account/password.
- Old password incorrect.
- Password must be a minimum of 8 characters and a maximum of 10 characters.
- Password cannot be the same as or contain the user ID.
- New password cannot be same as old password.

### **Documentation and Instructions**

- For 27X and password change transaction samples, see Appendix A.
- For instructions for adding a user to AHIN, see Appendix B.
- For instructions on how to log on to AHIN and reset your password manually, see Appendix C.

**27X ISA/GS Authentication Error Responses**

The 27X ISA/GS authentication error responses will apply to the 270, 276 and 278 transactions if an error has occurred in the ISA or GS segment. The chart below shows the error response that will be returned for a specific data element.

<b>Interchange Control Header (ISA) and Functional Group (GS) authentication error responses. Authentication errors are returned on the TA1 (Interchange Acknowledgment).</b>	
<b>Invalid Data Element</b>	<b>Interchange Acknowledgment Error Response</b>
Password Expired (see NOTE below)	TA104 = R Transaction Rejected TA105 = 011 Invalid Authorization Information Value
ISA03	TA104 = R Transaction Rejected TA105 = 012 Invalid Security Information Qualifier Value
ISA04	TA104 = R Transaction Rejected TA105 = 013 Invalid Security Information Value
ISA05	TA104 = R Transaction Rejected TA105 = 005 Invalid Qualifier for Sender ID
ISA06	TA104 = R Transaction Rejected TA105 = 006 Invalid Sender ID
ISA07	TA104 = R Transaction Rejected TA105 = 007 Invalid Qualifier for Receiver ID
ISA08	TA104 = R Transaction Rejected TA105 = 008 Invalid Receiver ID
GS02	TA104 = R Transaction Rejected TA105 = 006 Invalid Sender ID
GS03	TA104 = R Transaction Rejected TA105 = 008 Invalid Receiver ID

**NOTE:**

- TA105=011 normally would indicate that ISA02 has an invalid value. If it indeed contains invalid characters then that is the reason for the failure.
- AHIN will also return the same error code (TA105=011) when ISA06 / ISA04 (used for security verification) fails the security lookup.
- If you receive a TA105=011 and ISA02 is all blanks, it indicates ISA06 / ISA04 is the problem. These problems could include incorrect values or be the result of account lockout.

## **270 Eligibility Inquiries**

The optimum 270 search criteria should include one or more of the following items listed below. To maximize the search result, include as much information as possible in the 270 Eligibility Request.

- Primary criteria must include: first name, last name, date of birth and member ID number (maximum length of 17).
- Secondary criteria could include: gender or social security number.
- Data is required at either the subscriber or dependent loop.

For members in the Federal Employees Program (FEP) and out-of-state Blue Plans (i.e., non-Arkansas members), ALL of the primary criteria must be provided.

For Arkansas members (i.e., BlueAdvantage, Blue Cross and Health Advantage), the member ID prefix is not required.

As of December 2007, Arkansas Blue Cross Blue Shield accepts service type codes (EQ01) other than '30'. '98' is the recommended default service type code. Arkansas Blue Cross Blue Shield supports only one service type code per 270 transaction.

## **270 Companion Document**

<b>IG Page #</b>	<b>Loop ID</b>	<b>Reference</b>	<b>Name</b>	<b>Notes/Comments</b>
<b>First Level Authentication: All data elements in the Interchange Control Header (ISA) are required. The data elements listed below are Arkansas Blue Cross Blue Shield specific requirements and must contain the information assigned by EDI Services at Arkansas Blue Cross Blue Shield.</b>				
B.4	Header	ISA03	Security Information Qualifier	Must be a value of 01.
B.4	Header	ISA04	Security Information	Must be the password initially assigned by EDI Services at Arkansas Blue Cross Blue Shield or the value to which it has been changed.
B.4	Header	ISA05	Interchange ID Qualifier	Must be a value of ZZ.
B.4	Header	ISA06	Interchange Sender ID	Must be equal to the clearinghouse submitter ID assigned by EDI Services at Arkansas Blue Cross Blue Shield.
B.4	Header	ISA07	Interchange ID Qualifier	Must be a value of ZZ.
B.5	Header	ISA08	Interchange Receiver ID	Must be equal to a value of 020.
<b>Second Level Authentication: All data elements in the Functional Group (GS) are required. The data elements listed below are Arkansas Blue Cross Blue Shield specific requirements and must contain the information assigned by EDI Services at Arkansas Blue Cross Blue Shield.</b>				
B.8	Header	GS02	Application Sender's Code	Must be equal to the clearinghouse submitter ID assigned by EDI Services at Arkansas Blue Cross Blue Shield. This is the same value as the ISA06.
B.8	Header	GS03	Application Receiver's	Must be a value of 020. This is the same value as

			Code	the ISA08.
<b>See page 10 for the Interchange Control Header (ISA) and Functional Group (GS) authentication error responses. Authentication errors are returned on the TA1 (Interchange Acknowledgment).</b>				
52	2100B	NM108	Identification Code Qualifier	Must be a value of XX.
52	2100B	NM109	Identification Code	Must be equal to the pay-to provider's National Provider Identifier (NPI).
55	2100B	REF01	Reference Identification Qualifier	Must be equal to EO.
56	2100B	REF02	Reference Identification	Must be equal to the provider's submitter ID number assigned by EDI Services at Arkansas Blue Cross Blue Shield.

**271 Authentication Error Responses**

<b>Authentication errors for specific loops are returned on the 271. The 271 will always return the AAA segment on the 271 if there are errors.</b>		
<b>Invalid Loop / Data Element</b>	<b>271 Loop Returned</b>	<b>271 Segment &amp; Data Element Error Response Returned</b>
2100B / NM108	2100B	AAA01 = N The Transaction Has Been Rejected AAA03 = 51 Provider Not on File AAA04 = N Resubmission Not Allowed
2100B / NM109	2100B	AAA01 = N The Transaction Has Been Rejected AAA03 = 51 Provider Not on File AAA04 = N Resubmission Not Allowed
2100B / REF01	2100B	AAA01 = N The Transaction Has Been Rejected AAA03 = 51 Provider Not on File AAA04 = N Resubmission Not Allowed
2100B / REF02	2100B	AAA01 = N The Transaction Has Been Rejected AAA03 = 51 Provider Not on File AAA04 = N Resubmission Not Allowed
2100B	2100B	AAA03 = 51 Provider Not on File (ISA06 or 2100B NM109 invalid)
2100C	2100C	AAA03 = 15 Required Application Data Missing AAA03 = 42 Unable to Respond at Current Time AAA03 = 52 Service Dates Not Within Provider Plan Enrollment AAA03 = 64 Invalid/Missing Patient ID AAA03 = 65 Invalid/Missing Patient Name AAA03 = 67 Patient Not Found AAA03 = 71 Patient Birth Date Does Not Match That for the Patient on the Database AAA03 = 72 Invalid/Missing Subscriber/Insured ID AAA03 = 73 Invalid/Missing Subscriber/Insured Name AAA03 = 75 Subscriber/Insured Not Found AAA03 = 76 Duplicate Subscriber/Insured ID Number AAA03 = 77 Subscriber Found, Patient Not Found
2100D	2100D	AAA03 = 15 Required Application Data Missing AAA03 = 42 Unable to Respond at Current Time AAA03 = 52 Service Dates Not Within Provider Plan Enrollment AAA03 = 64 Invalid/Missing Patient ID AAA03 = 65 Invalid/Missing Patient Name AAA03 = 67 Patient Not Found AAA03 = 71 Patient Birth Date Does Not Match That for the Patient on the Database AAA03 = 72 Invalid/Missing Subscriber/Insured ID AAA03 = 73 Invalid/Missing Subscriber/Insured Name AAA03 = 75 Subscriber/Insured Not Found AAA03 = 76 Duplicate Subscriber/Insured ID Number AAA03 = 77 Subscriber Found, Patient Not Found

**276 Companion Document**

IG Page #	Loop ID	Reference	Name	Notes/Comments
<b>First Level Authentication: All data elements in the Interchange Control Header (ISA) are required. The data elements listed below are Arkansas Blue Cross Blue Shield specific requirements and must contain the information assigned by EDI Services at Arkansas Blue Cross Blue Shield.</b>				
B.4	Header	ISA03	Security Information Qualifier	Must be a value of 01.
B.4	Header	ISA04	Security Information	Must be the password initially assigned by EDI Services at Arkansas Blue Cross Blue Shield or the value to which it has been changed.
B.4	Header	ISA05	Interchange ID Qualifier	Must be a value of ZZ.
B.4	Header	ISA06	Interchange Sender ID	Must be equal to the clearinghouse submitter ID assigned by EDI Services at Arkansas Blue Cross Blue Shield.
B.4	Header	ISA07	Interchange ID Qualifier	Must be a value of ZZ.
B.5	Header	ISA08	Interchange Receiver ID	Must be equal to a value of 020.
<b>Second Level Authentication: All data elements in the Functional Group (GS) are required. The data elements listed below are Arkansas Blue Cross Blue Shield specific requirements and must contain the information assigned by EDI Services at Arkansas Blue Cross Blue Shield.</b>				
B.8	Header	GS02	Application Sender's Code	Must be equal to the clearinghouse submitter ID assigned by EDI Services at Arkansas Blue Cross Blue Shield. This is the same value as the ISA06.
B.8	Header	GS03	Application Receiver's Code	Must be a value of 020. This is the same value as the ISA08.
<b>See page 10 for the Interchange Control Header (ISA) and Functional Group (GS) authentication error responses. Authentication errors are returned on the TA1 (Interchange Acknowledgment).</b>				
63	2100B	NM108	Identification Code Qualifier	Must be a value of 46.
63	2100B	NM109	Identification Code	Must be the submitter ID assigned by EDI Services at Arkansas Blue Cross Blue Shield.
68	2100C	NM108	Identification Code Qualifier	Must be a value of XX.
69	2100C	NM109	Identification Code	Must be the pay-to provider's National Provider Identifier (NPI).

**277 Authentication Error Responses**

<b>Authentication errors for specific loops are returned on the 277. The 277 will always return the STC segment on the 277 if there are errors.</b>		
<b>Invalid Loop / Data Element</b>	<b>277 Loop Returned</b>	<b>277 Segment &amp; Data Element Error Response Returned</b>
2100B / NM108	2200E	STC01-1 = E0 Response Not Possible - Error on Submitted Request Data STC01-2 = 25 Entity Not Approved STC01-3 = RC Receiving Location
2100B / NM109	2200E	STC01-1 = E0 Response Not Possible - Error on Submitted Request Data STC01-2 = 25 Entity Not Approved STC01-3 = RC Receiving Location
2100C / NM108	2200E	STC01-1 = E0 Response Not Possible - Error on Submitted Request Data STC01-2 = 25 Entity Not Approved STC01-3 = RC Receiving Location
2100C / NM109	2200E	STC01-1 = E0 Response Not Possible - Error on Submitted Request Data STC01-2 = 25 Entity Not Approved STC01-3 = RC Receiving Location

## **278 Health Care Services Review – Request for Review and Response**

In a 278 transaction, specifying the following fields will facilitate the processing of the request:

- Service Provider Supplemental Identification (2010E Loop, REF01) equal to 'ZH' for Carrier Assigned Reference Number
- Provider Contact information (2010B Loop, PER02, PER03, PER04, PER05, PER06, PER07, PER08)
- Provider Address information (2010B Loop, N301, N302, N401, N402, N403, N404)
- Subscriber Date of Birth and Gender (2010CA Loop, DMG02, DMG03)
- Patient Date of Birth and Gender (2010DA Loop, DMG02, DMG03)

**278 Companion Document**

IG Page #	Loop ID	Reference	Name	Notes/Comments
<b>First Level Authentication: All data elements in the Interchange Control Header (ISA) are required. The data elements listed below are Arkansas Blue Cross Blue Shield specific requirements and must contain the information assigned by EDI Services at Arkansas Blue Cross Blue Shield.</b>				
B.4	Header	ISA03	Security Information Qualifier	Must be a value of 01.
B.4	Header	ISA04	Security Information	Must be the password initially assigned by EDI Services at Arkansas Blue Cross Blue Shield or the value to which it has been changed.
B.4	Header	ISA05	Interchange ID Qualifier	Must be a value of ZZ.
B.4	Header	ISA06	Interchange Sender ID	Must be equal to the clearinghouse submitter ID assigned by EDI Services at Arkansas Blue Cross Blue Shield.
B.4	Header	ISA07	Interchange ID Qualifier	Must be a value of ZZ.
B.5	Header	ISA08	Interchange Receiver ID	Must be equal to a value of 020.
<b>Second Level Authentication: All data elements in the Functional Group (GS) are required. The data elements listed below are Arkansas Blue Cross Blue Shield specific requirements and must contain the information assigned by EDI Services at Arkansas Blue Cross Blue Shield.</b>				
B.8	Header	GS02	Application Sender's Code	Must be equal to the clearinghouse submitter ID assigned by EDI Services at Arkansas Blue Cross Blue Shield. This is the same value as the ISA06.
B.8	Header	GS03	Application Receiver's Code	Must be a value of 020. This is the same value as the ISA08.
<b>See page 10 for the Interchange Control Header (ISA) and Functional Group (GS) authentication error responses. Authentication errors are returned on the TA1 (Interchange Acknowledgment).</b>				
61	2010B	NM108	Identification Code Qualifier	Must be a value of XX.
62	2010B	NM109	Identification Code	Must be the provider's National Provider Identifier (NPI).

**278 Authentication Error Responses**

<b>Authentication errors for specific loops are returned on the 278. The 278 will always return the AAA segment on the 278 if errors are found.</b>		
<b>Invalid Loop / Data Element</b>	<b>278 Loop Returned</b>	<b>278 Segment &amp; Data Element Error Response Returned</b>
2010B / NM108	2010B	AAA01 = N The Transaction Has Been Rejected AAA03 = 50 Provider Ineligible for Inquiries AAA04 = N Resubmission Not Allowed
2010B / NM109	2010B	AAA01 = N The Transaction Has Been Rejected AAA03 = 50 Provider Ineligible for Inquiries AAA04 = N Resubmission Not Allowed

**Appendix A – Coding Samples**

**X12 Transaction Sample**

```
<?php
// (C) Copyright Arkansas Blue Cross Blue Shield 2009-2010 All Rights Reserved.
//
// sample PHP function to send x12buffer to AHIN Gateway
//
// valid $hostnames are: securetest3.ahin-net.com    test system
//                      secure.ahinedi.com         prod system
//
// $x12buf contains the x12 transaction to submit
//     ISA security and provider IDs are contained within the x12 data and
//     are beyond the scope of this sample application.
//
// the next set of variables are all output fields generated from the request and response
//
// $header_out contains any http header data submitted to AHIN
// $header_rsp contains any http header data returned by AHIN
// $x12buf_rsp contains any payload data returned by AHIN
//
//     in normal conditions, ansi x12 payload will be returned and Content-type: text/ansi x12
//     in cases of error , text string will be returned and Content-type: text/plain
//
//     an error will be returned if the gateway is offline for maintenance or does not respond within 60
seconds.
//
//     authentication errors (invalid senderid/password or provider ids) are carried within the response.
//     meaning an ansi x12 payload will be returned as a TA1 or 997 depending on the type of failure.
//
// the response header may contain some data of interest
// Password-expires: nnn days      <- this is returned to indicate how many days until password must be changed
// Total-time: s.ddd               <- this is how long it took server to handle total request
// Content-type: text/ansi x12     <- this is returned to indicate payload area is an x12 response
// Content-type: text/plain        <- this is returned to indicate payload area is text message reporting an
abnormal condition
```

## *Arkansas Blue Cross Blue Shield 27X Companion Document Guide*

---

```
// AHN-warning: request content-length($contentlength) did not match actual length received($actuallength)
causing delayed response
// this warning is present when the server detects the Content-length variable is missing or larger than actual
data sent
// since the server must 'timeout' before it hands the data off to be processes, it causes a delay of at least
10 seconds.
// this adds to the overall transaction turn around time and will not be part of the Total-time: value since the
timing doesnt start
// until the data is handed off for processing.
//
function transactEligServer( $hostname, $x12buf, &$header_out, &$header_rsp, &$x12buf_rsp )
{
    $CrLf = "\r\n"; // dos style line separator

    $header_out =
        'POST /ELIG HTTP/1.0' . $CrLf . // build the buffer we need to send
        'Host: ' . $hostname . $CrLf . // hostname we're sending to
        'Content-type: text/ansi x12' . $CrLf . // not required but simply specifies the payload data
type we're sending
        // if we calc the content length too short, not all data will get picked up by the server even if we send
all the actual data.
        // the response will be TA105=023 error since the x12 decode stream does not see all the data and thinks
this is an envelope error.
        // if content length calculated as longer than actual, the server will be delayed reading for 10 seconds
before it processes the data.
        // this is due to fact the server attempts to read Content-Length # of bytes of data or until timeout of
10 seconds is reached.
        'Content-Length: ' . strlen($x12buf) . $CrLf . // make sure we properly calculate the payload length
payload
        $CrLf; // important blank line here to separate header from

    $bufsend_out = $header_out . $x12buf; // add on the payload data

    $port = 8008; // port 8008 is the eligibility port
    $addr = gethostbyname($hostname); // get the ipv4 address of hostname

    // lets open the connection to the server and write the data
    $socket = @socket_create(AF_INET, SOCK_STREAM, SOL_TCP) or die(socket_strerror(socket_last_error()));
    @socket_connect($socket, $addr, $port) or die(socket_strerror(socket_last_error()));
}
```

## *Arkansas Blue Cross Blue Shield 27X Companion Document Guide*

---

```
@socket_write($socket, $bufsend_out, strlen($bufsend_out)) or die(socket_strerror(socket_last_error()));
// accumulate the response in 2k chunks until we get an empty read
$rsp = '';
do
{
    $out = @socket_read($socket, 2048);
    if (socket_last_error()) die(socket_strerror(socket_last_error()));
    $rsp .= $out;
} while ($out);
@socket_close($socket);

// we got the response. Lets seperate the header from the payload
// split on the double crlf which seperates the header and data
list($header_rsp, $x12buf_rsp) = preg_split("/\r\n\r\n/", $rsp, 2, PREG_SPLIT_NO_EMPTY);
}
?>
```

## **Appendix A – Coding Samples (continued)**

### **Password Change Transaction Sample**

```
<?php
// (C) Copyright Arkansas Blue Cross Blue Shield 2009 All Rights Reserved.
//
// sample PHP function to send password change request to AHIN Gateway
// this can be adapted to other languages since the basics are the same and only the syntax changes.
// valid $hostnames are: securetest3.ahin-net.com    test system
//                      secure.abcbsemi.com        prod system
//
// $buf contains the field and value data for the change request.
//      "Userid=$userid&oldpass=$opassword&newpass=$npassword"
//
// the next set of variables are all output fields generated from the request and response
//
// $header_out contains any http header data submitted to AHIN
// header_rsp  contains any http header data returned by AHIN
// buf_rsp    contains any message text returned by AHIN
//
//      an error will be returned if the gateway is offline for maintenance or there are issues with the values
sent.
//
//      if the change request is good, a server status of 202 is returned.
//      if there are problems, a server status of status 406 is returned.
//
//      There will also be a text message returned indicating acceptance or failure reason.
//
//      Password changed successfully.
//      Invalid parameters. Usage is: userid=xxx&oldpass=yyy&newpass=zzz
//      AHIN is currently offline for maintenance. Please try again later.
//      System Error. AHIN Administration has been notified.
//      Unable to locate userid
```

## *Arkansas Blue Cross Blue Shield 27X Companion Document Guide*

---

```
// Account is locked. Please logon to AHIN in order to reset your gateway account/password.
// Old password incorrect. Too many failed attempts. Account is locked. Please logon to AHIN in order to
reset your gateway account/password.
// Old password incorrect.
// Password must be a minimum of 8 characters and a maximum of 10 characters.
// Password cannot be the same as or contain the user ID.
// New password cannot be same as old password.
//
// $buf = "User id=$user id&old pass=$opassword&newpass=$npassword";
// transactPwcServer('secure.ahinedi.com', $buf, $header_req, $header_rsp, $buf_rsp);
// echo $header_rsp;
// echo $buf_rsp;
//
function transactPwcServer( $hostname, $buf, &$header_out, &$header_rsp, &$buf_rsp )
{
    $crlf = "\r\n"; // dos style line separator

    $header_out =
        'POST /PWC HTTP/1.0' . $crlf . // build the buffer we need to send
        'Host: ' . $hostname . $crlf . // hostname we're sending to
        'Accept: */*' . $crlf . //
        'Connection: Close' . $crlf . // don't hold the connection after we're done
        'Content-type: text/plain' . $crlf . // not required but simply specifies the payload data
type we're sending
        'Content-Length: ' . strlen($x12buf) . $crlf . // make sure we properly calculate the payload length
        $crlf; // important blank line here to separate header from
payload

    $bufsend_out = $header_out . $x12buf; // add on the payload data

    $port = 80; // port 80
    $addr = gethostbyname($hostname); // get the ipv4 address of hostname

    // let's open the connection to the server and write the data
    $socket = @socket_create(AF_INET, SOCK_STREAM, SOL_TCP) or die(socket_strerror(socket_last_error()));
    @socket_connect($socket, $addr, $port) or die(socket_strerror(socket_last_error()));
    @socket_write($socket, $bufsend_out, strlen($bufsend_out)) or die(socket_strerror(socket_last_error()));
}
```

```
// accumulate the response in 2k chunks
$rsp = '';
do
{
    $out = @socket_read($socket, 2048);
    if (socket_last_error()) die(socket_strerror(socket_last_error()));
    $rsp .= $out;
} while ($out);
@socket_close($socket);

// we got the response. lets separate the header from the payload
// split on the first double crlf which separates the header and data
list($header_rsp, $buf_rsp) = preg_split("/\r\n\r\n/", $rsp, 2, PREG_SPLIT_NO_EMPTY);
}
?>
```

**Appendix B – Instructions for Adding a User to AHIN**

1. The following must be included for each user to be granted access to Arkansas Blue Cross Blue Shield 270/271, 276/277 and 278 real-time transactions:
  - ◆ User's Full Name
  - ◆ User's Date of Birth
  - ◆ User's Signature
2. Complete the AHIN Fax Cover Sheet. Be sure to complete the contact name, phone number, and an email address.
3. Fax the completed document and cover sheet to:

**FAX # 501-378-2484**
4. Allow three (3) business days for any user to be added to the system. AHIN personnel will call the contact person listed on the form by phone with the user name, PIN, and password.



**AHIN FAX # 501-378-2484**

Submitter #:

27X Vendor Name: \_\_\_\_\_

Contact Name: \_\_\_\_\_

Contact Phone: \_\_\_\_\_

Contact Email: \_\_\_\_\_

**ADDING USERS:**

NAME	DATE OF BIRTH	SIGNATURE OF USER

## Appendix C – AHIN 27X User Instructions

Arkansas Blue Cross Blue Shield has a new real-time process for 27X transactions. These instructions outline the required steps you must complete before implementing your 27X process. The changes described below give you the ability to reset locked or expired passwords yourself, view providers who are enrolled with you for 27X transactions and set up contact information for notification of system issues or changes.

Each 27X submitter needs to complete the following prior to implementing your 27X process:

Using the test URL, [securetest3.ahin-net.com](https://securetest3.ahin-net.com), you will need to send a password change (PWC) transaction and at least one eligibility, claim status or services review (ELIG) transaction.

**Do not use the results from the test URL. Test data can be different from production data.**

Once you have verified that you can successfully send transactions and reset your AHIN user password, email David Bailey at [dkbailey@arkbluecross.com](mailto:dkbailey@arkbluecross.com) to confirm that everything worked or to discuss any issues. After you have successfully tested, you may begin sending transactions to the production URL.

**Each organization will need to complete and fax in the AHIN User Form (see Appendix B) to have your user(s) set up. AHIN will issue each user an ID and password then call that user with the information.**

**Each submitter needs to log into AHIN and perform the steps below:**

Once you have received your user name and password you must log into our test system at <https://securealpha.ahin-net.com>. Once logged on then verify you can access your account information and reset your password.

**Step 1 - Logon to AHIN with the user ID and the default password you received from AHIN Customer Support.**



**Note:** First time users are prompted to change their password and agree to the confidentiality agreement before accessing AHIN.

**Password Rules:**

## Arkansas Blue Cross Blue Shield 27X Companion Document Guide

- Cannot contain your userid
- Cannot match the previous two passwords
- Must be between 8 and 20 characters
- Must contain 2 of the following:
  - Upper-case letter
  - Number
  - Special character

**Step 2** - Enter your new password and then again to confirm it. Click on the “Change” button. Passwords are case sensitive.

**Password has expired.**

Please change your password and you will be redirected to the home page.

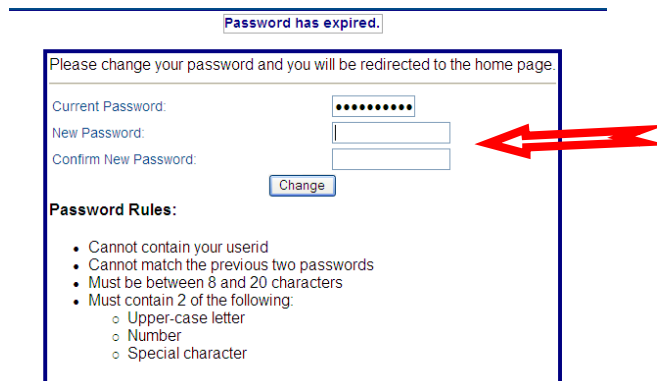
Current Password:

New Password:

Confirm New Password:

**Password Rules:**

- Cannot contain your userid
- Cannot match the previous two passwords
- Must be between 8 and 20 characters
- Must contain 2 of the following:
  - Upper-case letter
  - Number
  - Special character



**Step 3** - Click to mark the “I agree to the terms” statement and then on “I Agree” button to have the option to print the document and then continue to the AHIN homepage. By clicking on the “I Do Not Agree” button you will not be able to log into AHIN.

### AHIN Confidentiality Agreement v1.1

AHIN ACCESS CONFIDENTIALITY AGREEMENT v-1.1 01/10

THIS AHIN ACCESS CONFIDENTIALITY AGREEMENT ("Agreement") is entered into between Advanced Health Information Network, LLC ("AHIN") and the undersigned person ("User").

User is a physician, employee, agent or other representative of a physician, hospital or other health care provider, employer, vendor, or other person having a legitimate need for access to the data management system and health information network ("Network") owned and operated by AHIN. However, AHIN is unwilling to permit or provide access to the Network unless User agrees to maintain the integrity and confidentiality of Network information.

Now, therefore, for and in consideration of the agreements and undertakings of the parties and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and in order to induce AHIN to permit User to access the Network, User agrees, represents and warrants as follows:

1. User has entered into this Agreement because of User's legitimate need to have access to the Network. Without entering into this Agreement, User acknowledges that User would have no legal authority to access the Network.
2. All information contained in the Network including, but not limited to, information pertaining to patient diagnoses, treatments, medical, clinical and financial situation, computer programs, statistical reports, claims, insurance, strategic planning and costs ("Confidential Information") is confidential.
3. Security of Confidential Information is essential to the integrity and operation of the Network. User will not permit unauthorized access to the Network and will not disclose User's name, Personal Identification Number ("PIN") and/or password to any person. User shall be responsible for any damages to AHIN or the Network for the unauthorized use of User's name, PIN and/or password or the unauthorized use of User's access to the Network for which User is responsible.
4. User shall access the Network and use Confidential Information only to the extent to which User has a need to know in the performance of User's duties and responsibilities as an authorized person. User shall not aid or permit any unauthorized person to have access to the Network.
5. User shall not disclose, copy, sell, loan or in any way divulge Confidential Information to any unauthorized person and shall not modify, destroy or otherwise take any action that will alter Confidential Information to which User does not have security privilege or which would be detrimental to the Network.

6. User shall not knowingly or intentionally enter any erroneous, false or fraudulent information into the Network. Misuse of User's access to the Network or disclosure of User's name, PIN and/or password to an unauthorized person will subject User to revocation of User's password and authorization to use the Network.

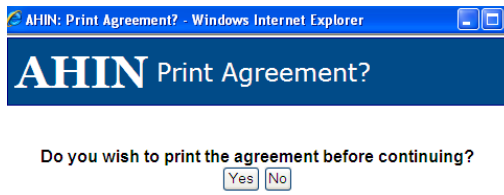
7. User's authorization for the use of Confidential Information and access to the Network shall cease upon the termination of User's need to have access to the Network or termination of this Agreement, whichever shall first occur.

8. All Confidential Information, the Network and any information pertaining thereto are the exclusive property of AHIN. User will not copy or otherwise reproduce any Confidential Information or any other information pertaining to the Network except for a legitimate purpose that will not injure AHIN in any way. All copies or reproductions of Confidential Information or information pertaining to the Network are the exclusive property of AHIN and shall be returned to AHIN upon termination of this Agreement.

9. User understands and agrees that it is prohibited from making any transmission or distributing any content through the Network in violation of any local, state, federal or international laws, regulations or treaties. These laws include, without limitation, those relating to electronic privacy and computer fraud, abuse and trespass laws, copyright and trade secret laws, obscenity laws and U.S. and foreign government regulations relating to the exportation and/or importation of data.

I agree with the Terms and Conditions Above

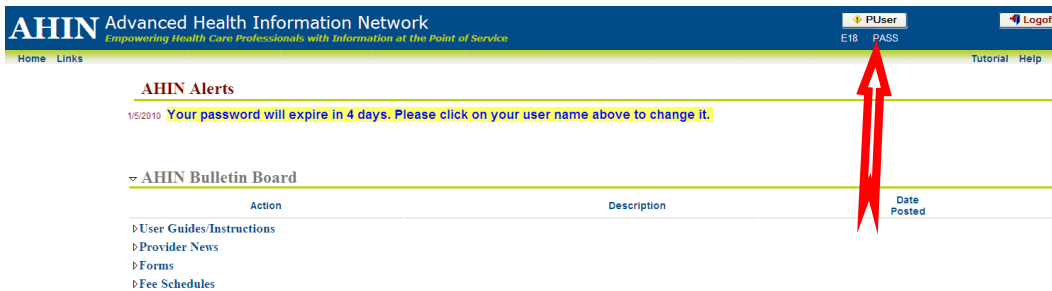
Agreed To By: jdoe @ 01/05/2010 02:55 PM



**Step 4** - Click on your user name in the upper right corner to display your user information and add the following information:

- Email address
- Secret question
- Answer and Answer (again) to the secret question
- Click on the Update button to save the information

By adding this information you will be able to reset your AHIN password using the Reset/Forgot Your Password link on the AHIN Logon page; if this information is not completed, passwords can only be reset during the normal working hours of 8:30 a.m. - 4:30 p.m. Central Standard Time by calling AHIN Customer Support at (501) 378-2336 or sending an email to customersupport@ahin.net.



**AHIN PUser** [Cancel/Close]

User Information [Update]

User Name: PUser  
 User Id: PUser History  
 First Name: Pas  
 Last Name: User  
 Middle Name:  
 Date of Birth: 01/01/1963  
 Password: [Change] Expires: 2010-01-09  
 PIN: 6465  
 Current/Last Role: AHIN Clearinghouse  
 Current/Last Fac: E0000 Clearinghouse Name  
 Email Address: [?]  
 Secret Question: [?]  
 Answer:  
 Answer (again):  
 Audit Records: [View]  
 Agreement Signed Time:  
 Last Logon: 01/05/2010 10:03:26.454

Works At (1)

AUA	NPI	Organization	Start Date	Term Date
-	E0000	Clearinghouse Name	12/10/2009	

Step 5 - To access your organization information click on the green arrow located in the upper right corner (to the right of your user name).

**AHIN** Advanced Health Information Network  
 Empowering Health Care Professionals with Information at the Point of Service

Home Links Clearinghouse E0000 Clearinghouse E0000 Clearinghouse Tutorial [Green Arrow]

**AHIN Alerts**  
 15/02/10 Your password will expire in 4 days. Please click on your user name above to change it.

**AHIN Bulletin Board**

Action	Description	Date Posted
▶ User Guides/Instructions		
▶ Provider News		
▶ Forms		
▶ Fee Schedules		

The User Tab will list all users that have access to this system for your organization

General Information			Address	
Name: Clearinghouse Name	Status: Active	Mailing Address	1234 Lilac Lane	Effective: 11/06/2009 to -
Federal		Address	Somewhere, AR	
AHIN Org Id: 00000	AHIN Fac Id: BBBB		72222	
		Phone:	(501) 123-4567	

AHIN Users (2) | Providers | Password | Contacts

Name	Effective	Terminated	Last Logon
gb	12/18/2009		01/04/2010 16:09:46.693
PUser	12/10/2009		01/05/2010 10:03:26.454

**Arkansas Blue Cross Blue Shield 27X Companion Document Guide**

The Provider Tab will list each provider’s name, Arkansas Blue Cross Blue Shield ID, submitter ID, transaction type each provider is sending under the 27X vendor and the provider’s NPI.

AHIN Users (2)		Providers	Password	Contacts						
Provider	ABCBS Id	Sub Id	CH270	CH276	CH278	CH820	CH834	CH837	835	NPI
A Schools	12345	E0000	Y							12123456789
Arkansas Emergency	55555	E3440	Y							1023456789
Plastic Surgery	65478	E1111	Y							12123456789
Arp, A	64512	E9999	Y							1023456789
Atkinson, Thomas W MD	78945	E2222	Y							12123456789
Baker, OD	85467	E8888	Y							1023456789
Aviation Inc	67898	E3333	Y							12123456789
Memorial Hospital	48956	E7777	Y							1023456789
Columbus MD	11111	E4444	Y							12123456789
Camp Clinic	78945	E0000	Y							1023456789
Cha	22222	E5555	Y							12123456789
William C MD	45612	E0000	Y							1023456789 1478529630
Community Clinic	33333	E6666	Y							12123456789
Conway Inc	64566	E0000	Y							1023456789
Cross			Y							

The Password Tab allows you to reset your Clearinghouse password without calling customer service. It is important that **all of your users** listed on the User Tab know the current password for your submitter number and how to force a change. You can also use the PWC transaction to initiate the password change programmatically. Make sure each user who can change the submitter number’s password for real-time 27X keeps it in sync with the ISA04 location inside the transaction; if not, your transactions will reject. This screen is not for each user’s password.

AHIN Users (2)	Providers	Password	Contacts
New Password: <input type="text"/>			
Confirm Password: <input type="text"/>			
<input type="button" value="Update"/>			
<b>Time</b>	<b>CH Id</b>	<b>Status</b>	<b>User Id</b>
			<b>Function</b>

The Contact Tab allows you to set up contact information. This is needed for AHIN to notify you of planned system outages or other anomalies. Please take a minute and set up one or two contacts. Be sure to click on the Update button once all the contact information has been entered. Please verify that all information entered is accurate and be sure to keep it updated as needed.

AHIN Users (2)	Providers	Password	<b>Contacts</b>
----------------	-----------	----------	-----------------

**Contact 1**  
Contact Name:   
Contact Phone:   
Contact Email:

**Contact 2**  
Contact Name:   
Contact Phone:   
Contact Email:

**Contact 3**  
Contact Name:   
Contact Phone:   
Contact Email:

**Contact 4**  
Contact Name:   
Contact Phone:   
Contact Email:

**Contact 5**  
Contact Name:   
Contact Phone:   
Contact Email: