KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

Privacy and Security

Quick Reference Guide

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

This Quick Reference Guide is designed to help you understand privacy and security requirements for health information, why it is important, and what resources you can access for additional help and information.

Table of Contents

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

1. Privacy and Security

Why it matters – it is the law

Consumer privacy and security is a major priority. Customer information is extremely sensitive and it is important for us to maintain privacy while electronically accessing state government information, as guided by Kentucky's Division of Enterprise Information Technology. The Commonwealth of Kentucky collects only the personal information necessary to provide better services to citizens and customers. Please note that all non-exempt information collected by Kentucky.gov services may be subject to public disclosure under the Kentucky Open Records Act. However, public records containing information of a personal nature are protected from disclosure by the personal privacy exemption of state law. Personal data in our possession is kept and used in ways that respect individual privacy. Only authorized employees have access to this personal information.

There are serious legal and personal consequences to breaching privacy and security laws. As Agents and Assisters helping citizens apply for healthcare and Medicaid coverage, you will be exposed to their private and personal information. You must handle this information carefully and not leave it in public places or areas where others may be able to access it. It is important that you understand the overarching Federal guidelines in addition to internal office policies of the Kentucky Health Benefit Exchange.

Because privacy and security are of the utmost importance, the Kentucky Office of the Health Benefit Exchange (KOHBE), has dedicated personnel – a Privacy Officer and a Security Compliance Team - who ensure the privacy and security of citizen information.

2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Definition:

Established in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a federal law that primarily aims to:

1. Make it easier for people to keep health insurance
2. Protect the confidentiality and security of healthcare information
3. Help the healthcare industry control administrative costs

HIPAA is comprised of various rules and regulations, which apply to covered entities and their business associates. Individuals, organizations, and agencies that meet the definition of a covered entity must comply with HIPAA's requirements to protect individually identifiable health information and provide patients with certain rights pertaining to that information. If a covered entity works with a business associate, the entity must have a contract or other arrangement with the business associate that establishes specifically what the business associate will do and requires the business associate to comply with the rules' requirements to protect the privacy and security of protected health information. If covered entities and their business associates do not follow the HIPAA rules and regulations, they are directly liable and face severe penalties for the release of that information.

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

A covered entity is one of the following:

Healthcare Provider

This includes:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

Health Plan

This includes:

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for healthcare

Healthcare Clearinghouse

This includes entities that process nonstandard health information that they receive from another entity into a standard electronic format or data content, or vice versa.

Please note that healthcare providers must transmit information in an electronic form in connection with a transaction that falls under the HIPAA standards. Also, government programs that pay for healthcare include Medicare, Medicaid, and the military and veterans' healthcare programs.

HIPAA's various rules and regulations include the following:

Regulation	Description
Privacy Rule	• Establishes national standards to protect individuals' medical records and other personal health information
Security Rule	• Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity • Requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information
Enforcement Rule	• Contains provisions relating to compliance and investigations, the imposition of civil money penalties for violation of the HIPAA Administrative Simplification Rules, and procedures for hearings

Breach Notification Rule	• Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information • Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers
Transactions and Code Sets Standards	Creates a uniform way to perform electronic data interchange (EDI) transactions for submitting, processing, and paying claims.
Employer Identifier Standard	• Requires employers have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN) is the identifier for employers and is issued by the Internal Revenue Service (IRS).
National Provider Identifier (NPI) Standard	• The NPI is a unique identification, 10-digit number for covered healthcare providers. Covered healthcare providers and all health plans and healthcare clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA.

1. Protected Health Information (PHI) and Personally Identifiable Information (PII)

Protected Health Information

It is of the utmost importance and a legal requirement to always be aware of the privacy and security of handling individuals' personal information. While performing Agent and Assister duties, there is a high likelihood of being exposed to sensitive client information, or Personally Identifiable Information (PII).

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

Agent and Assisters must handle PII carefully and should not leave it in public places or areas where others may be able to access it. When discarding PII, Agents and Assisters should use a shredder, not a trash can or recycling bin.

The HIPAA Privacy Rule aims to protect individually identifiable health information (IHII). This information is also known as protected health information or (PHI) and is a subset of Personally Identifiable Information (PII) which is discussed below. For information to be considered PHI, it must meet all of the following conditions:

1. The information is created, received, or maintained by a health provider or healthplan
2. The information is related to past, present or future healthcare or payment for that healthcare
3. The information identifies a member or patient, or there is enough information to be able to identify the individual

Individually identifiable health information includes many common identifiers, such as name, address, birth date, and Social Security Number.

Please note that the HIPAA regulations do not provide a list of information that is defined as individually identifiable health information. The following are direct identifiers of a limited data set. These identifiers are accepted in the healthcare field as being protected health information. The information must be collected by a covered entity. This includes:

(i) Names;
(ii) Postal address information, other than town or city, state, and zipcode;
(iii) Telephone numbers;
(iv) Fax numbers;
(v) Electronic mail addresses:
(vi) Social security numbers;
(vii) Medical record numbers;
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers, including license plate numbers;
(xii) Device identifiers and serial numbers;
(xiii) Web Universal Resource Locators (URLs);
(xiv) Internet Protocol (IP) address numbers;
(xv) Biometric identifiers, including finger and voice prints;
(xvi) Full face photographic images and any comparable images.

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

Personally Identifiable Information (PII)

As previously mentioned, PHI is a subset of Personally Identifiable Information (PII). PII is defined as information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

The generally accepted set of individually unique data elements in PII include the following list:

Data Element	Description
Name	First name, last name, maiden name combinations. It could be possible to identify an individual using a combination of data e.g. first name, zip code, street address etc.
Geographic locators	Street address, city, precinct, zip code, latitude and longitude coordinates, etc.
Dates	Significant events in an individual's life - birth, death, marriage, admission, discharge, etc. The year is generally considered fine for use except in the case of the very elderly (>89 years of age; in which case they would be represented by an aggregate category e.g. =>90
Phone numbers	Personal, work, other mobile or land line numbers linked to an individual
Fax numbers	Same as above
Electronic mail addresses (email)	Same as above
Social Security Number	9-digit number that continuously links an individual to his/her Social Security
Medical record numbers	Medical record numbers can be used to identify individuals if one also knew the institution that assigned it
Health plan beneficiary numbers	Insurance card/member ID
Account numbers	Bank numbers, etc
Certificate/license numbers	Driver's license, birth certificate, etc
Vehicle identifiers and serial numbers, including license plate	Any vehicle characteristic that can help track down an individual
Device identifiers and serial numbers	Medical devices with unique serial numbers, personal electronics, etc
Web Universal Resource Locators (URLs)	Technology can now track individuals' locations and identities based on browser history and web site visits
Internet Protocol (IP) address numbers	Similar to above
Biometric identifiers, including finger and voice prints	Retinal images also fall into this category
Full face photographic images and any comparable images	Visual aids that identify who you are

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

Personal Information

The Kentucky Revised Statutes of the Kentucky Legislature, 61.931, further clarifies Personal Information to be:

One of the following:	In combination with one or more of the following data elements:

• First name and last name
• First initial and last name
• Personal mark
• Unique biometric
• Genetic print or image
	• An account number or
	• Credit card number or
	• Debit card number with
	  ○ Required security code or
	  ○ Access code or
	  ○ Password, that grants access to the account
	• Social Security number
	• Taxpayer identification number that incorporates a Social Security number
	• Driver's license number or
	• State identification card or
	• Other individual identification number issued by any agency or
	• Passport number or
	• Other identification number issued by the US government or
	• Individually identifiable health information as defined in 45 CFR 160.103 except for education records covered by the Family Educational Rights and Privacy Act.

As you can see, the internal office policies and procedures of Kentucky are based on the overarching guidelines set forth by the Federal government. As Agents and Assisters, you will have access to this type of information when helping individuals and businesses apply for health coverage.

It is critical for you to know that personal information must be shredded.

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

4. Security Breaches and Steps to Remediation

Defining a security breach

A security breach is the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that has resulted in or is likely to result in the misuse of personal information.

If the agency has reason to believe that the records or data subject to the unauthorized access may compromise the security, confidentiality, or integrity of the personal information and has resulted in or is likely to result in the misuse of the personal information or likelihood of harm to one or more individuals, then the occurrence will be considered a security breach.

Third party business partners of the Kentucky Office of the Health Benefit Exchange (KOHBE) are responsible for ensuring the security of emails sent to KOHBE if the email contains confidential or personal information.

KOHBE business partners must use secure email if sending confidential information to KOHBE staff. Sending both a case number and name via email is a violation of PII.

Please note the importance of clearing your desk of confidential data files and papers at the end of the day.

The following steps are those that KOHBE takes if an employee receives personal information via email. These are recommended best practices for Agents and Assisters. The procedure is based on the Kentucky Revised Statutes Chapter 61 Sections 931 through 934, under “Personal Information Security and Breach Investigations.” To learn more, Agents and Assisters can visit the Kentucky Legislature website at www.lrc.ky.gov/statutes/index.aspx.

KOHBE treats matters around personal information very seriously. Therefore, Agents and Assisters should not send a consumer’s personal information by unsecured email. KOHBE staff will follow the steps below if they receive personal information from Agents and Assisters by unsecured email. Agents and Assisters can also use the following steps for their own procedures should they receive Personal Information (defined above in Section 3) by unsecured email. Unsecured email is defined as unencrypted email.

Please note that an individual does not violate the law just by receiving information illegally disclosed by another person.

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

Steps to take if a KOHBE employee or contractor receives a citizen's Personal Information

When KOHBE receives unsecure personal information via email, the KOHBE employee or contractor will Reply-All to the email that contains the personal information and add or modify the message as follows before sending it:

a) Add the text "IMMEDIATE ACTION REQUIRED" to the subject line
b) Copy the KOHBE Privacy Officer to the email
c) Manually delete the personal information from the message that was received
d) Reply to the sender to notify them that unsecured personal information was delivered to KOHBE and that the remedy process has been initiated
e) In the message of the email, include the instructions you just followed, outlined above, with the explanation, "Please follow these directions to remove personal information from all unsecured email."
f) Be sure to delete the email containing the personal information from your inbox,sent box, drafts, deleted items folders, and any and all email folders

Steps **a** through **f** are what KOHBE personnel follow for unsecured personal information. Agents and Assisters can modify these steps for your own internal processes.

5. Identity Proofing

Verifying individual information

Because IHII and PII are extremely sensitive and important, it is critical for you as Agents and Assisters to verify the identity of whom you are assisting.

Identity proofing is a federal requirement and a necessary step included in facilitating enrollment. The information provided to benefind is sensitive Personally Identifiable Information, requiring a rigorous online verification process. Determining eligibility involves sensitive federal and state data, and benefind must verify individuals' identities before granting them full access to the system.

There are three methods of verifying an individual's identity:

1. Provide the correct answers to a series of personal questions
   It is important to note that Agent or Assisters will only have one attempt to correctly enter the individuals' answers to the Experian questions.
2. Upload various forms of identification throughout the application process.
   a) These forms of identification can include:
   Adoption Record, Affidavit from non-US citizen, Affidavit from US citizen, Award Letter, Birth Record, Certificate of Tribal Affiliation, Certificate of US Citizenship (N-560 or N-561), Incarceration Discharge Record, Divorce Decree, Driver's License, Employee ID, Federal Government issued ID, GED, Health Insurance Card, High School or College Diploma, Immigration Document (Government Issued), Income Tax Return, Law Enforcement Records, Local Government Issued ID, Marriage License, Military Dependent's ID, Naturalization Certificate, Passport, Personal Records Showing Deductions, Property Deed or Title, School Photo ID, School

Record, State Government Issued ID, US Coast Guard Merchant Mariner card, US Military ID Card or Draft Record, and Wage Stubs

3. If the individual fails to correctly answer the Experian questions, they will be provided with a reference number and will need to call the Experian Help Desk at 1 (866) 578-5409. They will have to provide their last name, date of birth, and the reference number.

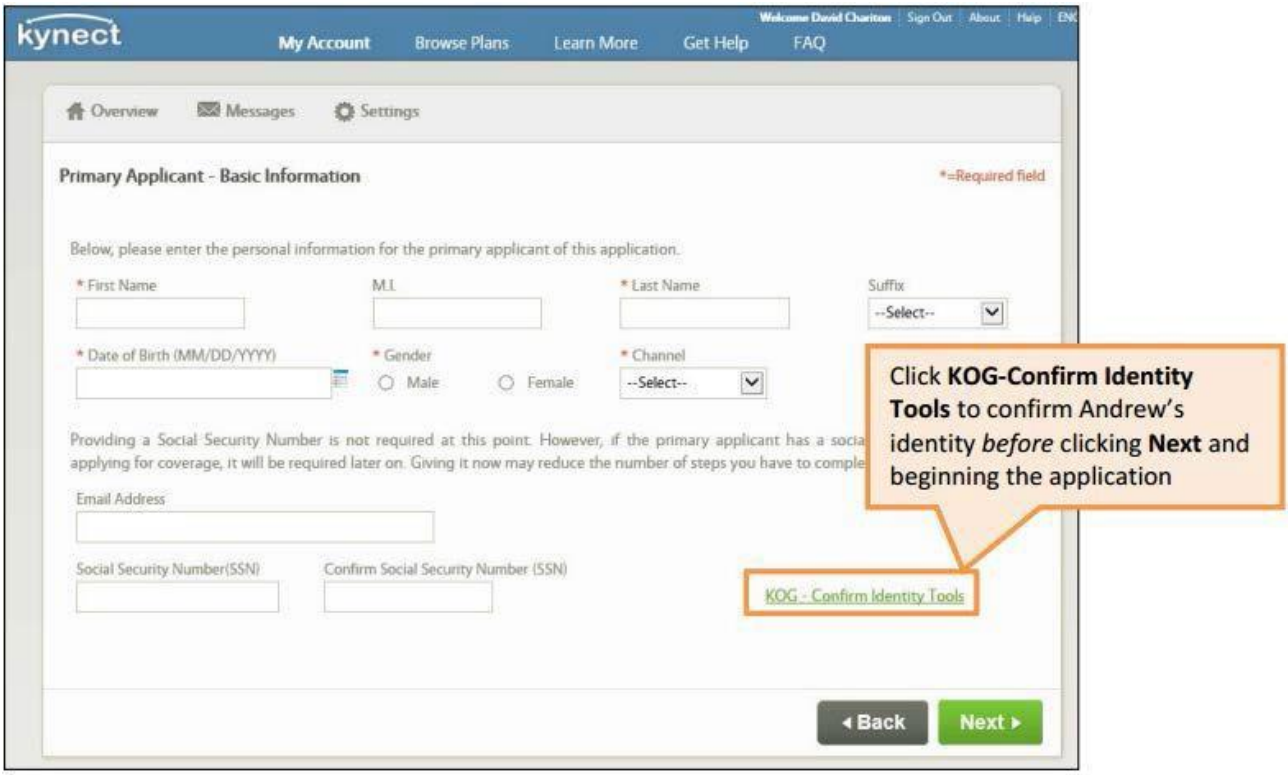
Using the KOG-Confirm Identity Tools Link

As an Agent or Assister assisting individuals with an application, it is a mandatory requirement to use the KOG-Confirm Identity Tools link to verify an individual's identity.

Once you initiate an individual application from your Agent or Assister dashboard, you can begin the identify confirmation process for the individual. You will ask the individual a series of unique personal questions. These questions are generated using public records and consumer credit information.

After you have begun an application, the Primary Applicant-Basic Information page displays.

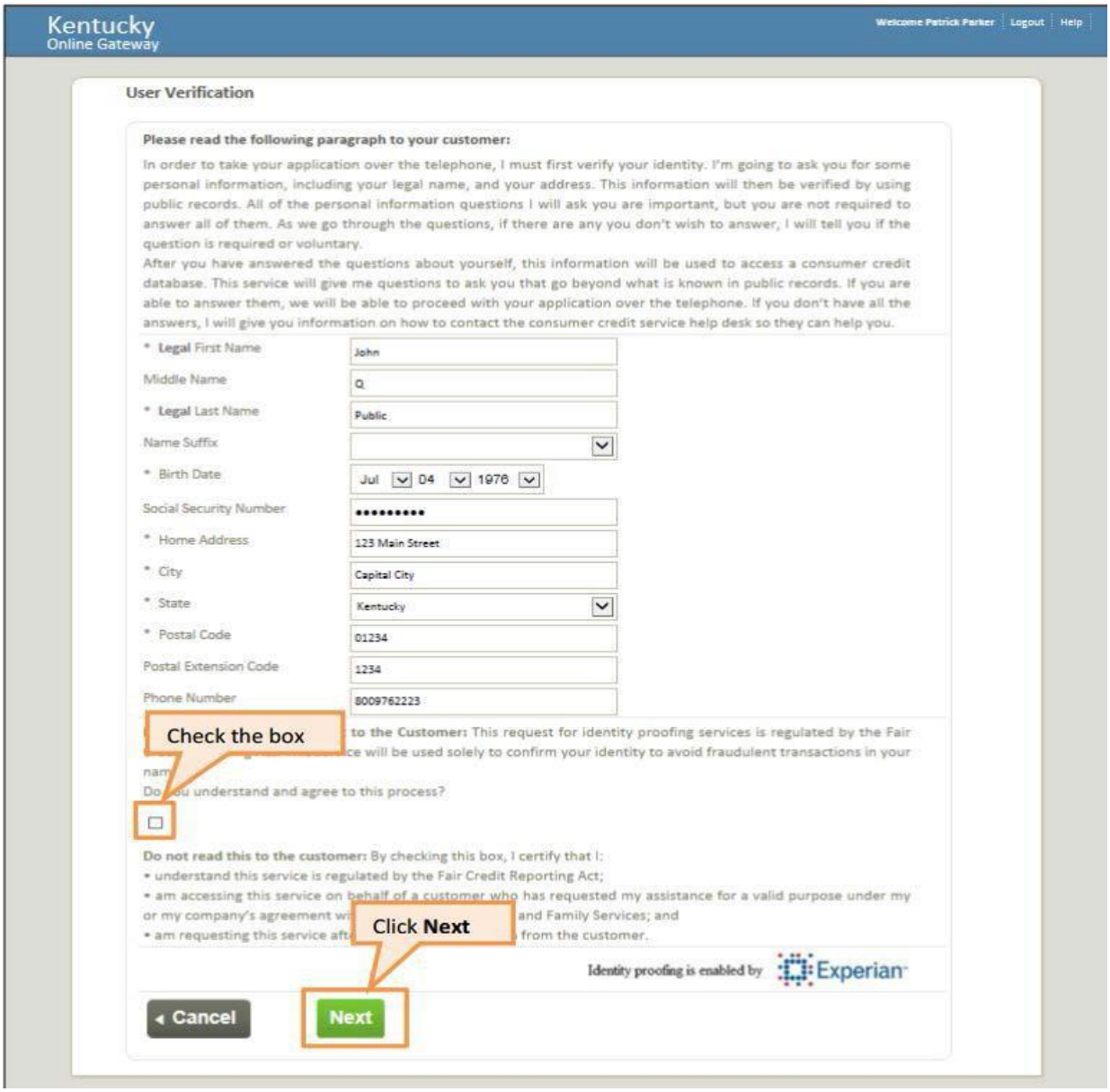
1. Enter the individual's first name, last name, date of birth, gender, and application channel.
2. Click the **KOG-Confirm Identity Tools** link at the bottom of the page to verify the individual's identity. You can confirm an individual's identify through this process or upload identification documents later.



KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

On the following screen, the Kentucky Online Gateway (KOG) website displays. KOG uses public records and consumer credit information to verify an individual's identity before issuing health insurance.

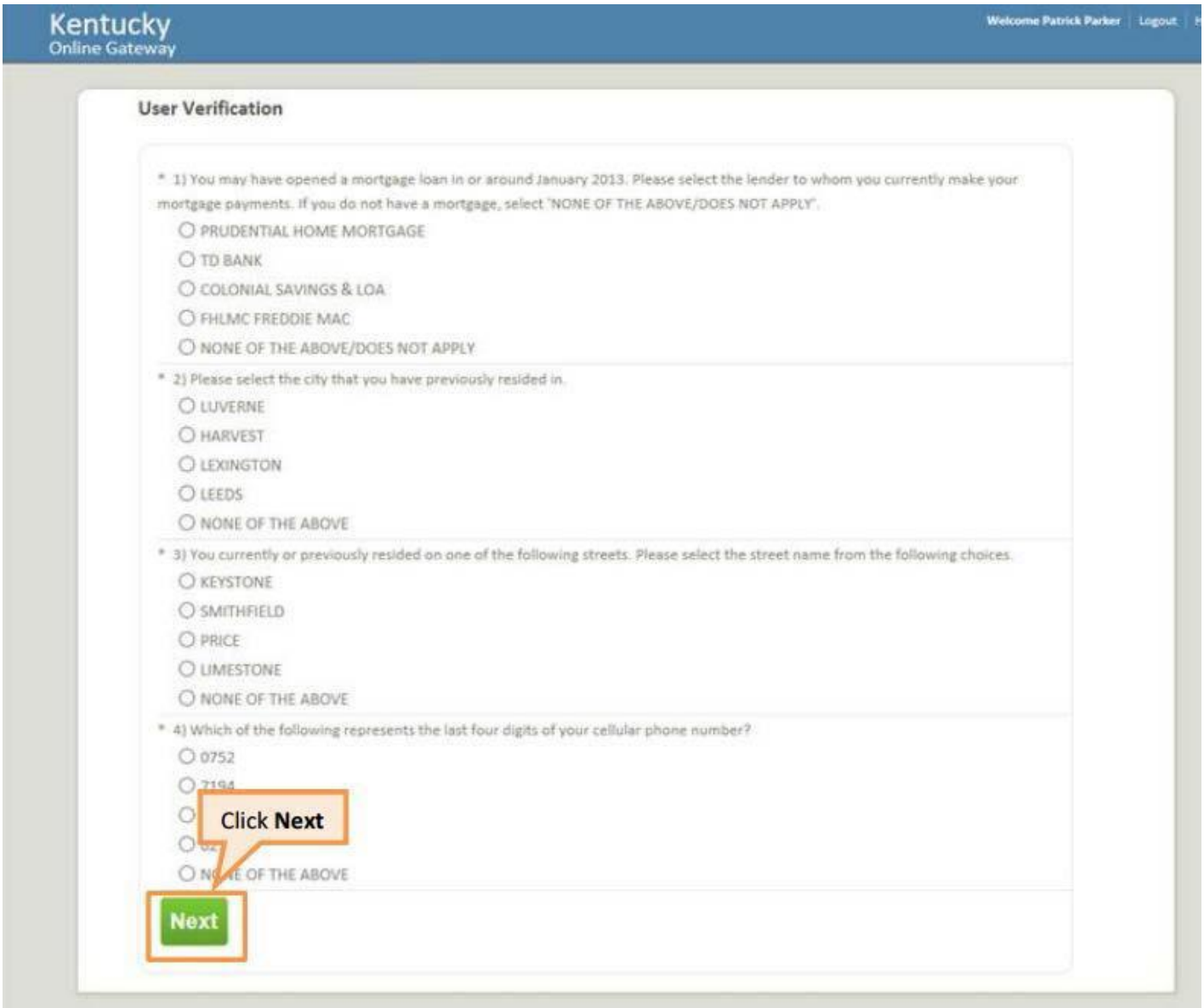
3. Read the statement at the top of the page to the individual to inform them of this verification process. The individual must say yes before you can continue.
4. Enter the individual's name, DOB, SSN, and home address.
5. Check the box to indicate that the individual agrees to the identity proofing terms and conditions and click **Next**.



KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

Examples of questions an individual might be asked are: *please select the county you have previously resided in, or which of the following represents the last four digits of your cellular phone number*? Note that these questions are unique to each individual based on their credit history. If the individual does not have a credit history, use the third manual ID proofing option mentioned on page 9.

6. Provide answers to each question.
7. Click **Next**.



If the individual provides the correct answers to all of his or her verification questions you can continue with his or her application on benefind. Should the individual you are assisting fail the online ID proofing, he or she will receive a reference number.
Instruct him or her to call the Experian Helpdesk at 1 (866) 578-5409 for assistance and troubleshooting.
If the individual you are assisting answers the identity proofing questions incorrectly, you **will not be able to proceed with his or her application** until this issue is resolved.

Manual ID Proofing

There is also a manual identification proofing option for those without credit history or those unable to pass the Experian identity proofing.
These individuals may be manually identity proofed.
Email a copy of a photo ID, contact information, and a signed written statement by a supervisor to DMS.eligibility@ky.gov<mailto:DMS.eligibility@ky.gov with "Request manual identity proofing" in the subject line.

Assisters may also call 1-502-564-6890 and ask for RIPD assistance.

DMS office staff who receive these requests may contact the individual and or supervisor for additional information before approval. Please note that this process is for contracted agencies only.

6. Penalties and Violations

Consequences to violating privacy rules and procedures

Civil Penalties	Criminal Penalties
Single violation of a provision, or multiple violations of different provisions could amount to a $25,000 fine.	
Violations due to reasonable cause and not willful neglect of an identical requirement or prohibition during a calendar year, will provoke a $1,000 fine for each violation, not exceeding $100,000.	Wrongful disclosure of Individually Identifiable Health Information can incur a maximum fine of $50,000 with up to 1 year of imprisonment.
Multiple violations due to willful neglect, not corrected, of an identical requirement or prohibition made during the same calendar year can lead up to a $1.5 million fine.	Wrongful disclosure of Individually Identifiable Health Information committed under false pretenses could be up to a $100,000 fine with up to 5 years of imprisonment.
Multiple violations due to willful neglect, not corrected, of an identical requirement or prohibition made during the same calendar year can lead up to a $1.5 million fine.	Wrongful disclosure of Individually Identifiable Health Information (IIHI) committed under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm could be up to a $250,000 fine with up to 10 years of imprisonment.

KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.

7. Additional Information and Resources

You may call Customer Service at 1 (855) 459-6328 for any and all matters related to KHBE.
You can also reach the Experian Helpdesk at 1 (866) 578-5409 for additional help and troubleshooting.
Specifically, if you'd like to submit a complaint, call 1 (887) 807-4027.

Office of Civil Rights (OCR)

The Office of Civil Rights (OCR) is a part of the U.S. Department of Health and Human Services (HHS). OCR enforces civil rights of healthcare providers receiving federal financial assistance from HHS. You can visit the OCR website at https://www.hhs.gov/ocr/index.html

U.S. Department of Health and Human Services (HHS)

The U.S. Department of HHS aims to improve the health, safety, and well-being of America.
You can find more information on health information privacy at https://www.hhs.gov/hipaa/index.html