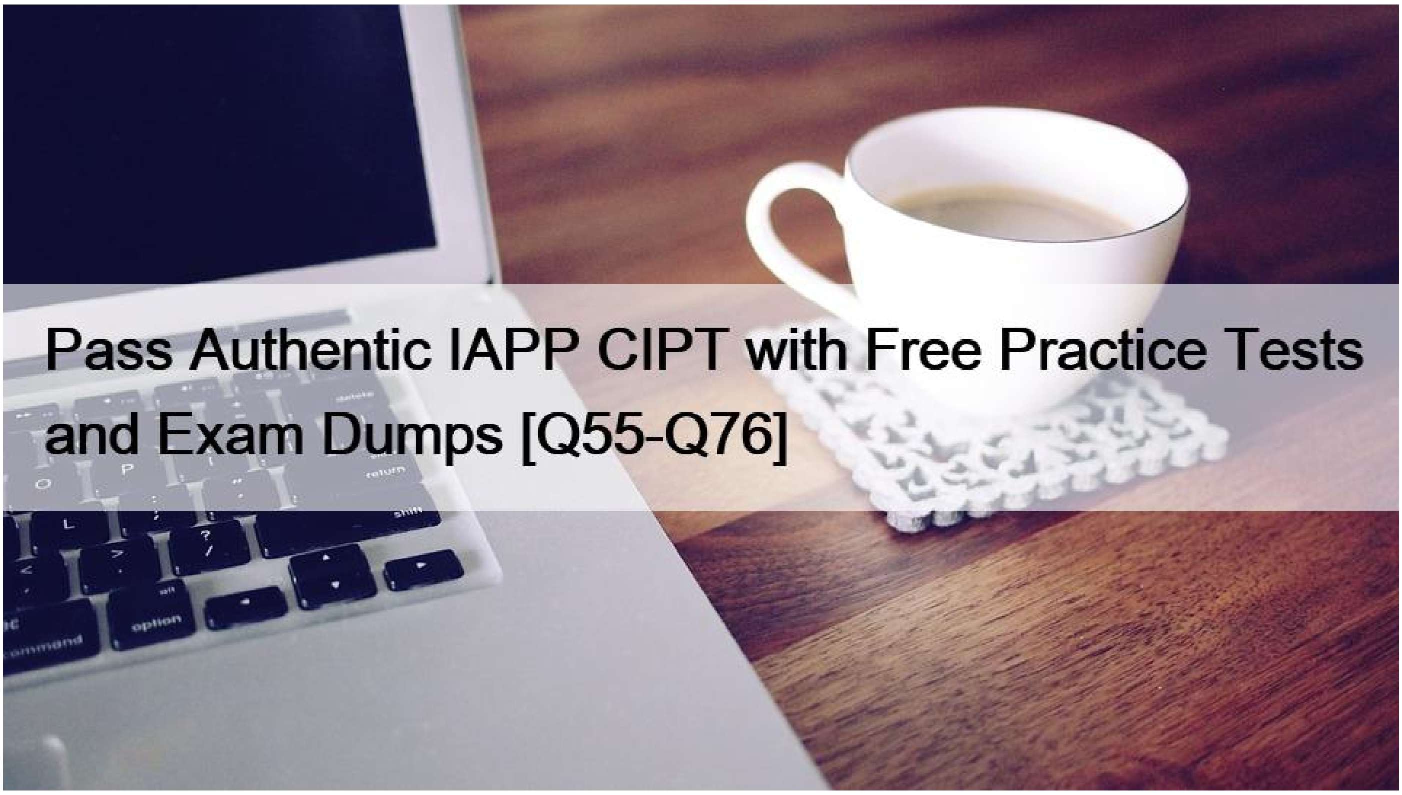
# Pass Authentic IAPP CIPT with Free Practice Tests and Exam Dumps [Q55-Q76



**Pass Authentic IAPP CIPT with Free Practice Tests and Exam Dumps New CIPT Exam Questions Real IAPP Dumps NEW QUESTION 55**

SCENARIO

Please use the following to answer the next question:

Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.

The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.

LBH&#8217;s privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.

The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.

What is the best way to ensure that the application only collects personal data that is needed to fulfill its primary purpose of providing potential medical and healthcare recommendations?
* Obtain consent before using personal health information for data analytics purposes.
* Provide the user with an option to select which personal data the application may collect.
* Disclose what personal data the application the collecting in the company Privacy Policy posted online.
* Document each personal category collected by the app and ensure it maps to an app function or feature.

**NEW QUESTION 56**

What is the distinguishing feature of asymmetric encryption?
* It has a stronger key for encryption than for decryption.
* It employs layered encryption using dissimilar methods.
* It uses distinct keys for encryption and decryption.
* It is designed to cross operating systems.

**NEW QUESTION 57**

Which is NOT a drawback to using a biometric recognition system?
* It can require more maintenance and support.
* It can be more expensive than other systems
* It has limited compatibility across systems.
* It is difficult for people to use.

**NEW QUESTION 58**

What risk is mitigated when routing video traffic through a company&#8217;s application servers, rather than sending the video traffic directly from one user to another?
* The user is protected against phishing attacks.
* The user&#8217;s identity is protected from the other user.
* The user&#8217;s approximate physical location is hidden from the other user.
* The user is assured that stronger authentication methods have been used.

**NEW QUESTION 59**

SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card.

You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

&#8220;We were hacked twice last year,&#8221; Dr. Batch says, &#8220;and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again.&#8221; She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility&#8217;s wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

Why would you recommend that GFC use record encryption rather than disk, file or table encryption?
* Record encryption is asymmetric, a stronger control measure.
* Record encryption is granular, limiting the damage of potential breaches.
* Record encryption involves tag masking, so its metadata cannot be decrypted
* Record encryption allows for encryption of personal data only.

**NEW QUESTION 60**

Which of the following entities would most likely be exempt from complying with the General Data Protection Regulation (GDPR)?
* A South American company that regularly collects European customers personal data.
* A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state.
* A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers.
* A North American company servicing customers in South Africa that uses a cloud storage system made by a European company.

**NEW QUESTION 61**

SCENARIO

Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.

As business grew, Carol couldn&#8217;t keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, &#8220;I don&#8217;t know what you are doing, but keep doing it!&#8221; But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane&#8217;s first impressions.

At the meeting, Carol could not wait to hear Jane&#8217;s thoughts, but she was unprepared for what Jane had to say. &#8220;Carol, I know that he doesn&#8217;t realize it, but some of Sam&#8217;s efforts to increase sales have put you in a vulnerable position. You are not protecting customers&#8217; personal information like you should.&#8221; Sam said, &#8220;I am protecting our information. I keep it in the safe with our bank deposit. It&#8217;s only a list of customers&#8217; names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That&#8217;s the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase.&#8221; Carol replied, &#8220;Jane, that doesn&#8217;t sound so bad. Could you just fix things and help us to post even more online?&#8221;

&#8216;I can,&#8221; said Jane. &#8220;But it&#8217;s not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy.&#8221; Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. &#8220;Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand.&#8221; What type of principles would be the best guide for Jane&#8217;s ideas regarding a new data management program?

- Collection limitation principles.
- Vendor management principles.
- Incident preparedness principles.
- Fair Information Practice Principles

**NEW QUESTION 62**

SCENARIO

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary&#8217;s operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as &#8220;My Cool Ride&#8221; for automobile-related products or &#8220;Zoomer&#8221; for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company&#8217;s culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company&#8217;s product lines as well as products from affiliates. This new omnibus site will be known, aptly, as &#8220;Under the Sun.&#8221; The Director of Marketing wants the site not only to sell Ancillary&#8217;s products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?
* Unseen web beacons that combine information on multiple users.
* Latent keys that trigger malware when an advertisement is selected.
* Personal information collected by cookies linked to the advertising network.
* Sensitive information from Structured Query Language (SQL) commands that may be exposed.

**NEW QUESTION 63**

SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card.

You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

&#8220;We were hacked twice last year,&#8221; Dr. Batch says, &#8220;and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again.&#8221; She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility&#8217;s wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

Why would you recommend that GFC use record encryption rather than disk, file or table encryption?
* Record encryption is asymmetric, a stronger control measure.
* Record encryption is granular, limiting the damage of potential breaches.
* Record encryption involves tag masking, so its metadata cannot be decrypted
* Record encryption allows for encryption of personal data only.
Explanation

**NEW QUESTION 64**

SCENARIO

WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure&#8217;s privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.

This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome &#8211; a partnership that will not require any data sharing. SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.

To get an idea of the scope of work involved, you have decided to start reviewing the company&#8217;s documentation and interviewing key staff to understand potential privacy risks.

The results of this initial work include the following notes:

* There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.

* You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance of the cloud infrastructure.

* There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.

* Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.

* All the WebTracker and SmartHome customers are based in USA and Canada.

Which of the following issues is most likely to require an investigation by the Chief Privacy Officer (CPO) of WebTracker?
* Data flows use encryption for data at rest, as defined by the IT manager.
* AmaZure sends newsletter to WebTracker customers, as approved by the Marketing Manager.
* Employees&#8217; personal data are being stored in a cloud HR system, as approved by the HR Manager.
* File Integrity Monitoring is being deployed in SQL servers, as indicated by the IT Architect Manager.

**NEW QUESTION 65**

Users of a web-based email service have their accounts breached through compromised login credentials. Which possible consequences of the breach illustrate the two categories of Calo&#8217;s Harm Dimensions?
* Financial loss and blackmail.
* Financial loss and solicitation.
* Identity theft and embarrassment.
* Identity theft and the leaking of information.

**NEW QUESTION 66**

SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card.

You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

&#8220;We were hacked twice last year,&#8221; Dr. Batch says, &#8220;and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again.&#8221; She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility&#8217;s wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

What type of wireless network does GFDC seem to employ?
* A hidden network.
* A reluctant network.
* A user verified network.
* A wireless mesh network.

**NEW QUESTION 67**

SCENARIO &#8211; Please use the following to answer the next question:

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun. including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary s operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving.

However, the company now sells online through retail sites designated for industries and demographics, sites such as &#8220;My Cool Ride11 for automobile-related products or &#8220;Zoomer&#8221; for gear aimed toward young adults.

The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company s culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company s product lines as well as products from affiliates. This new omnibus site will be known, aptly, as &#8220;Under the Sun.&#8221; The Director of Marketing wants the site not only to sell Ancillary s products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?
* Unseen web beacons that combine information on multiple users.
* Latent keys that trigger malware when an advertisement is selected.
* Personal information collected by cookies linked to the advertising network.
* Sensitive information from Structured Query Language (SQL) commands that may be exposed.

**NEW QUESTION 68**

What term describes two re-identifiable data sets that both come from the same unidentified individual?
* Pseudonymous data.
* Anonymous data.
* Aggregated data.
* Imprecise data.

**NEW QUESTION 69**

SCENARIO &#8211; Please use the following to answer the next question:

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun. including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary s operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving.

However, the company now sells online through retail sites designated for industries and demographics, sites such as &#8220;My Cool Ride11 for automobile-related products or &#8220;Zoomer&#8221; for gear aimed toward young adults.

The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company s culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company s product lines as well as products from affiliates. This new omnibus site will be known, aptly, as &#8220;Under the Sun.&#8221; The Director of Marketing wants the site not only to sell Ancillary s products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

Which should be used to allow the home sales force to accept payments using smartphones?
* Field transfer protocol.
* Cross-current translation.
* Near-field communication.
* Radio Frequency Identification.

**NEW QUESTION 70**

What is an Access Control List?
* A list of steps necessary for an individual to access a resource.
* A list that indicates the type of permission granted to each individual.
* A list showing the resources that an individual has permission to access.
* A list of individuals who have had their access privileges to a resource revoked.

**NEW QUESTION 71**

When should code audits be concluded?
* At code check-in time.
* At engineering design time.
* While code is being sent to production.
* Before launch after all code for a feature is complete.

**NEW QUESTION 72**

Which of the following is a vulnerability of a sensitive biometrics authentication system?
* False positives.
* False negatives.
* Slow recognition speeds.
* Theft of finely individualized personal data.

**NEW QUESTION 73**

SCENARIO

Please use the following to answer the next question:

Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.

The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.

LBH&#8217;s privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.

The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.

The Privacy Team is conducting a Privacy Impact Assessment (PIA) for the new Light Blue Health application currently in development. Which of the following best describes a risk that is likely to result in a privacy breach?
* Limiting access to the app to authorized personnel.
* Including non-transparent policies, terms and conditions in the app.
* Insufficiently deleting personal data after an account reaches its retention period.
* Not encrypting the health record when it is transferred to the Light Blue Health servers.

**NEW QUESTION 74**

How should the sharing of information within an organization be documented?
* With a binding contract.
* With a data flow diagram.
* With a disclosure statement.
* With a memorandum of agreement.

**NEW QUESTION 75**

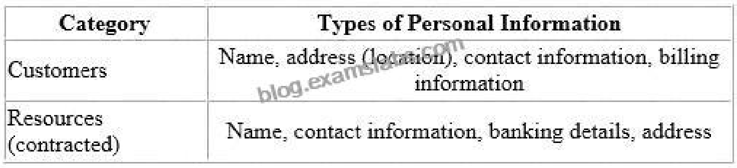
Which of the following is considered a client-side IT risk?
* Security policies focus solely on internal corporate obligations.
* An organization increases the number of applications on its server.
* An employee stores his personal information on his company laptop.
* IDs used to avoid the use of personal data map to personal data in another database.

**NEW QUESTION 76**

SCENARIO

Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database &#8211; currently managed in-house by Clean-Q IT Support. Because of Clean-Q&#8217;s business model, resources are contracted as needed instead of permanently employed.

The table below indicates some of the personal information Clean-Q requires as part of its business operations:



| Category | Types of Personal Information |
|---|---|
| Customers | Name, address (location), contact information, billing information |
| Resources (contracted) | Name, contact information, banking details, address |

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.

With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q&#8217;s traditional supply and demand system that has caused some overlapping bookings.

Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q&#8217;s solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q&#8217;s operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

* A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.

* A resource facing web interface that enables resources to apply and manage their assigned jobs.

* An online payment facility for customers to pay for services.

Which question would you most likely ask to gain more insight about LeadOps and provide practical privacy recommendations?
*  What is LeadOps&#8217; annual turnover?
*  How big is LeadOps&#8217; employee base?
*  Where are LeadOps&#8217; operations and hosting services located?
*  Does LeadOps practice agile development and maintenance of their system?

**CIPT Exam Info and Free Practice Test Professional Quiz Study Materials:** https://www.examslabs.com/IAPP/Information-Privacy-Technologist/best-CIPT-exam-dumps.html]