Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

IAPP-CIPP-C MCQs
IAPP-CIPP-C Exam Questions
IAPP-CIPP-C Practice Test
IAPP-CIPP-C TestPrep
IAPP-CIPP-C Study Guide

killexams.com

IAPP

IAPP-CIPP-C

Certified Information Privacy Professional/ Canada (CIPP/C)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/IAPP-CIPP-C

privacy rights and ensure compliance with the legislation.

Question: 1122

An organization subject to an OPC investigation requests to negotiate a consent order to avoid a formal enforcement hearing. What is a key element of such an agreement?

A. The organization commits to specific corrective actions and compliance timelines
B. The OPC waives all enforcement authority indefinitely
C. The investigation is discontinued without any follow-up
D. The organization pays a fine in exchange for no further oversight

Answer: A
Explanation: Consent orders involve negotiated agreements where organizations undertake specific corrective measures under timelines to resolve complaints without formal hearings.

Question: 1123

onboarding, automating role-based access controls for data handlers. What IAM policy template in Okta best enforces PIPEDA's limiting use principle?

A. { "role": "handler", "access": "read_only_pii", "audit": "log_all", "expiry": "90_days_post_role" }
B. Manual approval per request.
C. Group-based without expiry.
D. Unlimited access for all new hires.

Answer: A
Explanation: Programs require controls to limit use to necessary roles, with audits and time-bound access. The template enforces least privilege, aligning with PIPEDA's collection/use limits and reducing insider risks during scaling.

Question: 1124

Under Quebec's Law 25, which of the following is a required component of a breach notification to affected individuals?

A. The full legal text of the privacy law.
B. Detailed technical description of the vulnerability exploited.
C. Measures the organization has taken to mitigate harm.

D. Personal information of the individual who caused the breach.

Answer: C
Explanation: Quebec's Law 25 requires that breach notifications include the measures taken to mitigate harm and instructions for protecting oneself, but not technical details or personal data of the perpetrator.

Question: 1125

patients' phones, including test codes. A phishing attack intercepts messages. Under breach rules, what notification timeline applies if harm risk is low?

A. Notify affected patients and Ombud within 7 days of discovery
B. Wait for patient inquiry
C. Immediate SMS recall attempt
D. No individual notice if low risk, but record internally

Answer: D
Explanation: Section 51.1 requires recording all breaches, but individual notice only for real harm risks;

for minor incidents.

Question: 1126

During a compliance review, a company discovers that it has not implemented a privacy policy as required by law. What should be the company's immediate action?

A. Wait for a complaint before taking action
B. Develop and implement a privacy policy
C. Notify all customers about the lack of a policy
D. Conduct training for employees on privacy issues

Answer: B
Explanation: The company's immediate action should be to develop and implement a privacy policy. This is a fundamental requirement under Canadian privacy laws, and having a policy in place demonstrates the organization's commitment to protecting personal information.

Question: 1127

An organization is planning a marketing campaign that involves profiling individuals based on their online

behavior. What must the organization do to comply with privacy regulations?

A. Anonymize the data used for profiling
B. Obtain explicit consent from individuals before profiling
C. Limit profiling to individuals over the age of 18
D. Inform individuals about the profiling in a general privacy notice

Answer: B
Explanation: The organization must obtain explicit consent from individuals before profiling them based on their online behavior. This requirement helps protect individual privacy and ensures compliance with privacy regulations regarding consent.

Question: 1128

video consultations revealing Indigenous community health trends. PIPEDA's transborder accountability requires contractual safeguards. What clause template in the service agreement most rigorously enforces comparable protection standards?

A. Standard indemnity for data losses, with optional encryption add-on.
B. "Provider shall maintain PIPEDA-equivalent safeguards, including annual audits and immediate breach notification within 24 hours."
C. Jurisdiction clause limiting disputes to Alberta courts only.
D. Data localization to Canadian servers for all Indigenous-related files.

Answer: B
Explanation: Organizations remain accountable for offshore processors under PIPEDA, mandating contracts that ensure equivalent protections, audits, and prompt notifications. This clause aligns with OPC guidelines on transborder flows, especially for sensitive group data, preventing adequacy gaps despite EU-like decisions.

Question: 1129

A provincial health ministry in Alberta is implementing a new AI-driven predictive analytics tool to identify at-risk patients for resource allocation, using aggregated personal health data from multiple public bodies.

primary compliance obligation for the ministry prior to deployment to ensure alignment with privacy by design principles?

A. Obtain explicit consent from all data subjects for secondary uses of health information
B. Conduct a privacy impact assessment (PIA) only if the tool involves cross-border data flows

C. Develop and implement a privacy management program that includes risk identification, mitigation strategies, and automated decision-making notifications
D. Limit data retention to 12 months regardless of the program's operational needs

Answer: C

provincial health ministries to establish a comprehensive privacy management program under section 5, which encompasses documented policies for risk assessment, mitigation, and safeguards. This includes embedding privacy by design for AI systems, such as notifying individuals of automated decision-making per section 32.1, to proactively address risks in predictive analytics tools. While PIAs are required in prescribed scenarios (e.g., new information systems under the PPA Regulation), the broader program ensures ongoing compliance. Consent is not typically required for public health secondary uses under health-specific exemptions, and retention must align with necessity rather than a fixed period.

Question: 1130

Quebec Law 25: A retailer app defaults Quebec PI sharing with affiliates without PI
A.
A. PIA + disable defaults + granular consent
B. Vendor audit
C. Opt-out post-notice
D. Policy update only

Answer: A
Explanation: S.8.1 requires max privacy defaults; PIA (s.26.2) assesses sharing risks, mitigations; consent granular (s.14). CAI methodology demands residual risk eval.

Question: 1131

A health service provider in New Brunswick is required to retain patient records for a specific period. What is the minimum retention period mandated by the Personal Health Information Privacy and Access Act?

A. Indefinitely
B. 1 year
C. 10 years
D. 5 years

Answer: C
Explanation: The Personal Health Information Privacy and Access Act in New Brunswick mandates that patient records must be retained for a minimum period of 10 years. This retention period ensures that

health information is available for necessary future reference while respecting privacy rights.

Question: 1132

During an internal audit, a privacy officer discovers that sensitive personal information is being stored without proper safeguards. What principle of PIPEDA should the organization focus on to address this issue?

A. Accuracy
B. Safeguards
C. Limiting use, disclosure, and retention
D. Transparency

Answer: B
Explanation: The principle of safeguards requires organizations to protect personal information with appropriate security measures against loss, theft, and unauthorized access. Addressing this issue is critical to ensuring compliance with PIPEDA and protecting individuals' privacy.

Question: 1133

outreach on privacy training, claiming CASL exemption for business contact information (BCI) but triggering a PIPEDA investigation after a recipient alleges unauthorized collection of LinkedIn data linked to personal emails. The firm's scraping script includes no consent check, violating both laws' interaction on address harvesting. What code snippet should the developer insert into the scraping function to enforce CASL's BCI limits alongside PIPEDA's consent at collection?

A. if (profile.is_bci()) { collect_email(); } // Ignores PIPEDA consent for personal linkage
B. scrape_all() unless (year < 2014); // Relies on expired transitional consent
C. validate_bci_casl(profile) && check_pipeda_consent(email_source) ? scrape() : log_violation();
D. add_to_list(email) if (domain == 'business'); // Bypasses re-identification risks

Answer: C
Explanation: CASL exempts BCI like work emails from CEM consent if used purely for professional communication, but PIPEDA applies if personal information is collected without consent, especially via scraping that risks linking to identifiable individuals. The snippet enforces CASL's BCI validation per CRTC rules while requiring PIPEDA's knowledge and consent at source, logging violations for OPC

preventing $1 million individual fines under CASL and PIPEDA findings of unreasonable collection, ensuring ethical data practices in B2B scenarios.

Question: 1134

Rogers Communications, FWUB, outsources employee benefit admin to Alberta firm "benefits_pipeda_outsource --federal=true". Admin fees charged. PIPEDA oversight?

A. Benefits exempt
B. Alberta firm only
C. Rogers accountability
D. Outsourcing commercial

Answer: C
Explanation: FWUBs accountable for employee PI with third parties, including provincial outsourcers, per PIPEDA contracts. Federal telecom employee scope.

Question: 1135

offshore affiliate, a Saskatoon retailer faces class-action threats. Under Challenging Compliance Principle, what escalation pathway must the retailer's response outline for complainants?

A. Internal closure post-audit.
B. Collective settlement without individual recourse.
C. Internal fair investigation with documented resolution, plus OPC/Federal Court referral options.
D. Vendor-led resolution only.

Answer: C
Explanation: Challenges require fair response, documentation, and further recourse info. Outlines ensure process integrity, per 2024 OPC class findings. Vendor-only abdicates, settlements need recourse, closure premature.

Question: 1136

A privacy breach occurs at a hospital in Ontario, and sensitive patient information is accessed without authorization. What is the hospital required to do under PHIPA?

A. Wait for the patients to report the breach before taking action.
B. Immediately delete the compromised information.
C. Notify the affected patients and the Information and Privacy Commissioner.
D. Conduct a risk assessment and take no further action if the risk is low.

Answer: C

Explanation: Under PHIPA, hospitals must notify affected patients and the Information and Privacy Commissioner about privacy breaches to ensure transparency and allow for proper investigation and remediation.

Question: 1137

In the midst of an OPC investigation into a media streaming service's personalized recommendation engine, the service redacts portions of its recommendation algorithm pseudocode, arguing competitive sensitivity. Findings reveal consent gaps in data use for training models. For enforcement, the OPC must weigh disclosure against innovation. What is the appropriate oversight balance?

A. Oversight concludes without code review if consent forms are updated
B. Enforcement proceeds on redacted versions, limiting findings to observable outputs
C. Full code disclosure is mandated, with trade secret protections applied post-review
D. The OPC defers to intellectual property tribunals for code access decisions

Answer: C
Explanation: PIPEDA section 9 demands production of relevant records, including code, with courts protecting trade secrets via in-camera reviews under section 14 warrants. Here, redacted pseudocode hinders verification of consent in model training, justifying full disclosure for enforcement. OPC's 2023 AI guidance emphasizes this balance, ensuring oversight of high-risk processing without stifling innovation, as applied in streaming investigations.

Question: 1138

A company in Quebec is developing a new marketing strategy that involves collecting personal data from consumers. Which of the following must they include in their strategy to comply with the Quebec Private Sector Act?

A. A requirement to collect data only from individuals over 18 years old.
B. A disclaimer stating that data collection is for internal use only.
C. A process for individuals to opt-out of data collection at any time.
D. A clause that allows them to share data with third parties without consent.

Answer: C
Explanation: To comply with the Quebec Private Sector Act, the company must include a process for individuals to opt-out of data collection at any time. This ensures that individuals have control over their personal data and can make informed choices about their privacy.

Question: 1139

An Regina school board pilots iris scans for student attendance, integrating with parent portals but facing equity concerns for diverse eye colors. OPC youth privacy requires what in the PIA?

A. Data sharing with local police for security.
B. Assessing biases, offering non-biometric options, and parental consent with impact mitigation.
C. Annual reviews only after year one.
D. Mandatory scans for all without alternatives.

Answer: B
Explanation: OPC's 2024 biometric/youth guidance mandates PIAs for bias (accuracy across diversity), alternatives, verifiable parental consent (PIPEDA 4.3.5 for minors). Mandatory coercive; sharing disproportionate; delayed reviews reactive.

Question: 1140

An Edmonton e-learning platform aggregates user quiz responses containing disclosed trauma histories for sentiment analysis to refine course content, but collects extraneous demographic details beyond stated learning objectives. User feedback highlights overreach. PIPEDA's Limiting Collection Principle requires what data hygiene step in the platform's update cycle?

A. Outsource collection to a vendor for independent minimization.
B. Retain aggregates as de-identified, exempting from limits.
C. Bundle all details under "personalized learning" without pruning.
D. Conduct purpose-fit assessments pruning non-essential demographics, with user-facing collection notices specifying exact fields.

Answer: D
Explanation: Collection must be necessary and fair; trauma histories demand strict limits, with assessments ensuring fit and notices detailing fields. OPC's 2024 edtech reports stress pruning, de-identification doesn't retroactively validate collection, bundling violates specificity, outsourcing requires oversight.

Question: 1141

A Canadian charity receives donor personal information (name, address, donation amount) with express consent limited to issuing tax receipts and annual thank-you communications. The charity later wishes to share the donor list with a partnered non-profit for joint fundraising. Under PIPEDA clause 4.3, what applies?

A. Section 7(3)(f) exception allows disclosure without consent for fundraising
B. No consent required as donor information is publicly available

C. New express consent is required as the disclosure is for a purpose not previously identified
D. Implied consent suffices because both are non-profit entities

Answer: C
Explanation: Clause 4.3 and 4.3.3 require consent for disclosures, and clause 4.3.5 mandates that when an organization decides to use or disclose information for a new purpose, it must inform the individual and obtain consent. Fundraising by a third party is a new purpose not within typical receipt/thank-you scope, and no specific non-profit fundraising exception exists in section 7 comparable to the business transaction or investigation exceptions.

Question: 1142

During an OPC investigation into a university's research database sharing with international collaborators, findings expose lapses in data subject access request handling due to outdated query functions in the database schema. The university argues academic freedom limits enforcement. Which enforcement response best upholds OPC authority?

A. Deferral to institutional ethics boards for internal resolution
B. Federal Court order to modernize schema functions and process pending requests
C. Limitation of findings to non-binding educational guidelines
D. Acceptance of academic exemptions from PIPEDA's access principles

Answer: B
Explanation: PIPEDA applies fully to federal works like universities, with no academic exemptions; section 15 enables court orders for technical fixes like schema updates to enforce access rights. This counters the freedom argument, as OPC findings in 2024 research cases affirm privacy's precedence, mandating verifiable compliance in data sharing.

Question: 1143

GreenTech Innovations, a Saskatchewan-based cleantech firm, pilots drone surveillance for environmental monitoring on farms, capturing landowner images tied to property records, with intra-provincial analysis. Which framework governs this image data collection?

A. Saskatchewan's HIPA, classifying images as health data.
B. PIPEDA, due to Saskatchewan's lack of substantially similar private sector law.
C. Federal Aerial Surveillance Regulations, requiring image anonymization.
D. Provincial Land Titles Act, mandating record disclosures.

Answer: B
Explanation: Saskatchewan has no general private sector law similar to PIPEDA, so PIPEDA applies to

commercial drone image collection linking to identifiable individuals, emphasizing consent and safeguards. HIPA is PHI-specific, inapplicable to environmental images. Aerial regulations address safety, not privacy,

surveillance tech.

Question: 1144

pseudonymized faces, re-ids 10%. What duty?

A. Exempt generative.
B. Disclose post-harm.
C. Voluntary.
D. 'mitigate_bias --aida_highimpact && reid_threshold=0'.

Answer: D
Explanation: AIDA duties for high-impact include zero-tolerance re-id mitigation, with assessments preventing harm, fines up to 5% revenue, integrating CPPA transparency.

Question: 1145

A children's educational app in Nova Scotia collects drawings and voice notes from users 6-10, using CASL for parent newsletters based on child activity summaries without verified parental consent. What PIPEDA-CASL violation occurs?

A. CASL's commercial message definition for summaries
B. PIPEDA's sensitive child data consent needing parental verification
C. PIPEDA's limiting use for voice notes
D. CASL's implied consent for educational content

Answer: B
Explanation: PIPEDA requires parental consent for sensitive child data collection (e.g., creative works implying identity), which CASL's implied consent for messages cannot satisfy. Message definitions are secondary; implied consent limited; use limiting post-consent.

Question: 1146

In a recent privacy breach, a healthcare provider accidentally disclosed personal health information of patients. What is the first action the provider should take following the discovery of the breach?

A. Report the breach to the Privacy Commissioner of Canada
B. Notify the affected patients immediately
C. Implement new security measures to prevent future breaches
D. Investigate the cause of the breach

Answer: D
Explanation: The first action the provider should take is to investigate the cause of the breach. Understanding how the breach occurred is critical to addressing the issue and implementing effective measures to prevent future incidents.

Question: 1147

An Ottawa news aggregator app collects device IDs and page dwell times to serve ads for mental health resources based on time spent on wellness articles, raising OBA concerns under OPC guidelines. What is the correct approach to obtaining valid implied consent in this scenario involving potentially sensitive health inferences?

A. Embedding consent in the app's terms of service without user acknowledgment.
B. Requiring express consent only for users over 18, implied for minors.
C. Displaying a layered notice at first launch detailing tracking for ads, sensitivity handling, and persistent opt-out via settings, with no data use until opted in or out.
D. Using supercookies that auto-renew consent every 30 days.

Answer: C
Explanation: For OBA with health inferences, OPC Guidelines (2011, 2024 updates) permit implied consent for non-sensitive but require clear, multi-layered notices explaining purposes, data types, and easy, persistent opt-outs before collection, per PIPEDA's meaningful consent (Schedule 1, 4.3.2). Layered formats (summary + details) enhance comprehension, especially for sensitivity. Terms burial lacks prominence; age-based express ignores uniform rules; supercookies evade control.

Question: 1148

A company’s privacy program requires a data inventory. What challenge is most likely to occur during this activity?

A. Data collection never changes and can be documented once and ignored
B. Privacy officers usually do not need to involve other departments
C. Data inventory is typically automated and error-free
D. Identifying all data flows across diverse systems and jurisdictions may be complex and resource-intensive

Answer: D

Explanation: Data inventories require cooperation across departments and locations to map personal data flows accurately, making the process complex and demanding. Automation helps but is not error-free, and data use evolves over time. Collaboration is essential for accuracy.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.