KPMG

Privacy Digest

Issue 3 | June 2025

KPMG in Nigeria

The Power of Less: Privacy Considerations Around Employment Medical Assessments

Many organisations require successful recruitment candidates to undergo medical tests to determine their fitness before being given an employment offer. As a prospective hire seeking opportunities with an organisation, the rigour of the various stages of assessment ends with a sigh of hope or relief upon receiving a request for medical assessment from the organisation.

While it is a common practice to require candidates to undergo these medical assessments, what defines the scope or extent of legally permissible assessments? How much data would constitute crossing the line? Can an organisation actually rely on consent of the candidate as a basis for this? Is it ideal for an organisation to get such robust medical information because they possibly can, in a bid to safeguard the vital interest of a potential employee when eventually employed? Similarly, given that some organisations outsource these assessments to external health organisations, how adequate is the contract with such third-parties to establish the role of the controller and processor for the medical data, define responsibilities for controller and processor, and protect the interests of data subjects?

In this edition, we will focus on these questions and the importance of adopting adequate data minimisation practices when handling employee and pre-employment medical assessment data. We will explore lessons from useful case studies, practical strategies for reducing data exposure, and the stance of data protection laws on effective data management.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Medical Assessment Data and the Privacy Law in Nigeria

In Nigeria, health data falls under the category of sensitive personal data, a subset of personal data that requires greater care, due to its potential to cause significant harm if misused. Pre-employment medical assessments, which often involve the collection of health records, present a critical intersection between privacy laws and organisational needs. How so?

Employers often request health records during recruitment to evaluate a candidate's fitness for a role, ensure workplace safety, or mitigate potential liabilities. However, the existing power imbalance in the employer-employee relationship can leave prospective employees in a vulnerable position. This power imbalance is evident when employers require candidates to undergo extensive pre-employment medical tests, even when such tests may not be strictly necessary for the role. Job applicants are often left with no choice but to give consent to these tests due to likelihood of losing the employment opportunity, should they decline processing. This raises questions about the freely given nature of their consent. True balance can only be achieved when organisations adopt a targeted approach, requesting health information solely relevant to the specific demands of the position, in addition to giving job applicants clear information on why the pre-medical test is required, how their data will be used, and their right to refuse tests that should be optional or test not relevant to the role, without fear of discrimination.

The Nigeria Data Protection Act (NDPA) emphasises that data collection should adhere to the principles of necessity and proportionality. This means that organisations are expected to only collect data directly related to the requirements of the advertised job to ensure compliance with privacy laws. Over-collection of health data, can easily breach these principles, leading to legal and reputational risks.

We will now explore common practices that organisations use when conducting pre-employment medical tests.

How Adequate are Current Practices for Pre-Employment Medical Assessments?

Over the years, many organisations have approached health data handling without much consideration for the privacy or rights of the data subjects. Today, while some organisations are taking steps towards complying with data protection regulations, a closer review of certain practices they have adopted often reveal gaps in compliance or ethical considerations.

In many cases, prospective employees are required to sign consent forms without being informed about the specific medical tests they will undergo as part of the standard hiring, or processing activities associated with the health data being obtained. Alternatively, some companies rely on legal obligations to process medical data, particularly for roles involving safety-sensitive responsibilities or regulatory requirements, allowing them to mandate health screenings.

Some of these practices stem from limited understanding or interpretation of privacy requirements, while others are driven by convenience. This brings us to a crucial discussion:

- **The Question of Obtaining Valid Consent**

  Consent may often be relied upon as the lawful basis for processing sensitive health data at recruitment and during employment, but the key question remains: is it truly valid? For consent to be valid, it must be freely given, specific, informed, and unambiguous as outlined in section 26 (1) of the NDPA.

  In the case of recruitment candidates, they may feel that they have little choice but to comply with pre-employment medical tests, fearing that refusal could lead to the loss of a job offer.

  This raises concerns about whether such consent is genuinely voluntary. The NDPA sets clear conditions for valid consent, emphasising that it must be given without coercion.

  Additionally, employers must prove that consent was obtained in a manner that allows candidates to make an informed decision. Silence, inactivity, or pre-selected options do not constitute valid consent under the law.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Furthermore, section 26(4),(5) of the NDPA outlines that data subjects must be informed of their right to withdraw consent at any time, without facing negative consequences.

Despite these legal provisions, common hiring practices often contradict the requirement of the NDPA. Many organisations present medical testing as a blanket requirement, with consent forms that do not provide room for refusal or preference selection. In some cases, candidates are not fully informed about the purpose of these tests or how their data will be used. This imbalance of power between employers and job seekers can undermine the legitimacy of consent, making it more of an obligation than a choice.

The challenge, therefore, lies in ensuring that consent mechanisms align with legal and ethical standards, rather than being used as a mere formality that disregards the rights of prospective employees.

- **Overstepping Boundaries: Are we over-relying on 'legal obligation' in processing employee health data?**

  Section 8 of the Nigeria Labour Act requires that "(1) Every worker who enters into a contract shall be medically examined by a registered medical practitioner at the expense of the employer" and section 33 (1)(a) of the Labour Act states that "No citizen recruited for employment in Nigeria shall be employed until he has been medically examined under section 8 of this section and passed fit to perform the work for which he has been recruited." While this provides a legal foundation for health screenings, the Act does not specify the types of tests to be conducted for different job roles. This ambiguity highlights the need for discretion and prioritisation of data minimisation when determining the scope of pre-employment medical assessments.

  Many employers justify the collection of extensive medical data of their employees based on legal obligations, particularly workplace safety and health regulations. While certain roles and sectors may have specific pre-employment health screening requirements, care must be taken by organisations to specifically identify the lawful basis for requesting prospective employees to undergo various medical tests and for collecting or processing data in such instances. If such requirements are not based on specific laws, relying on 'legal obligation' can result in an overreach. Hence, organisations must assess whether the medical data they obtain is truly necessary for fulfilling legal obligations or if it constitutes a violation of the principle of data minimisation.

  Excessive reliance on legal obligations, without considering privacy principles, can lead to the collection of irrelevant or overly intrusive health information, potentially violating the Nigeria Data Protection Act (NDPA). Employers must strike a balance between fulfilling the Labour Act's requirements and respecting privacy rights of prospective employees.

  By adopting strong data minimisation practices, organisations can meet legal obligations without compromising prospective employees' privacy, ensuring both ethical and compliant hiring practices.

- **Transparency in the Processing of Health Data**

  Transparency is a fundamental principle in data protection, ensuring that individuals understand what personal data is collected, who will have access to it, and why it is being collected, used, and stored.

  When it comes to processing health data during recruitment, many organisations send out communications requesting pre-employment medical screenings at a designated medical facility. While some organisations inform prospective candidates about the required tests, many do not provide clear details on the specific tests to be carried out, their necessity, how the data will be handled, or whether the results could influence hiring decisions.

  Similarly, there are instances where employers require existing employees to undergo medical checkups without clearly stating how the results will be used, who within the organization will have access, and the specific impact—if any—on their employment status. In some cases, employees may not even be informed that their results will be shared directly with the employer rather than being provided to them first. This lack of transparency creates uncertainty about data handling, retention, and potential decision-making based on the result of the medical assessment.

  Section 27(3) of the NDPA emphasises that data subjects must be provided with clear, specific, and accessible information regarding the processing of their personal data, and this includes health information. It mandates that organisations communicate the purpose and legal basis for data collection in a way that allows individuals to make informed decisions.

  Many employers and data controllers fail to disclose these details upfront. Instead, they rely on vague or generalised policies that do not align with the NDPA. Without clear communication through a privacy policy or notice, candidates and employees may remain unaware of processing activities associated with their health data, who will have access to their test results and other personal data, as well as their rights over this data.

> Ensuring transparency in sensitive data processing would not only promote compliance but also foster trust between employers and prospective employees, and also between employers and existing employees.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Use Cases of Common Practices and Recommendations

Having looked at some of the common practices around handling of health data in comparison with the requirements of the NDPA, we will now consider some practical cases and discuss a few good practices and recommendations.

Case Study 1

Ada, a 29 year-old software developer, applied for a role at a multinational technology company in Lagos. After undergoing a series of interviews, she was required to undergo a comprehensive pre-employment medical assessment and given a 24-hour deadline to sign a consent form, which required her concurrence to undergo all the medical tests requested as part of the hiring requirements.

On arriving at the health facility, she discovered that the assessment included procedures such as full genetic testing and a pregnancy test. Although she felt uncomfortable with these tests and wondered the relevance to her role and application, she felt pressured to comply, to avoid jeopardising her chances.

A few days later, she was informed that her application was rejected due to "unsuitability for the role," leading her to suspect that her pregnancy test results influenced the decision. She is disappointed and is considering exercising her right to make a complaint to the NDPC.

* Please note that the names mentioned in this case study are fictional and have been used for illustrative purposes only

Key Considerations from Case Study 1

Imbalance of Power and Consent Validity:

Ada's case highlights the inherent power imbalance in employer-employee relationships. The employer's request for consent to the medical tests may not be considered valid under Section 26 of the Nigeria Data Protection Act (NDPA), which requires consent to be freely given, specific, informed, and unambiguous. The implicit pressure Ada faced undermines the "freely given" condition, and the lack of a privacy policy to provide information on the data processing activities impairs the ability to make informed consent. These, amongst others, render the reliance on consent questionable.

Over Collection of Data

The requested tests, such as genetic and pregnancy tests, were not reasonably tied to the responsibilities of the software development role. This violates the principle of data minimisation under the NDPA, which mandates that only necessary and relevant data be collected. The company's blanket policy of requesting extensive health tests, without job-specific justification, raises concerns about their compliance with this requirement.

Lack of Transparency

The company failed to provide Ada with adequate information about what test she was required to take or why the tests were necessary or how the data would be used. This lack of transparency is a violation of requirements in section 27(1) of the NDPA.

Recommendations for organisations based on Case Study 1

- **Ensure Consent is Freely Given:** Employers must recognise the power imbalance in the hiring process and ensure that where consent is to be relied upon as a lawful basis for personal data processing, such consent is truly voluntary. This means giving candidates a genuine choice to refuse unrelated medical tests without fear of negative consequences, in line with Section 26 of the NDPA. Requests for medical data should not be made a condition for employment unless the information is essential for the role or required by law.
- **Job-Related Medical Assessments:** Limit medical tests to those directly tied to the role's requirements.
- **Transparency via Privacy Notice:** Clearly communicate the purpose, use, and implications of requested medical tests to candidates via a Privacy Notice/Policy.
- **Human Resource Training:** Train the Human Resource and recruitment teams on NDPA compliance, focusing on valid consent and data minimisation.
- **Compliance Audits:** Regularly audit data collection practices associated with recruitment candidate data to ensure alignment with privacy laws and eliminate unnecessary data collection.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Case Study 2

[1] In the case of "Wunmi A. vs. Ocean Marine Solutions" (2021), the National Industrial Court of Nigeria found Ocean Marine Solutions in breach of the statutory and constitutional rights related to informed consent, privacy, and anti-discrimination of its former employee.

Wunmi A., a cleaner at Ocean Marine Solutions, was instructed by HR to undergo a medical test alongside five other employees at a facility chosen by the company. She claimed she was neither informed about the specific nature of the test nor provided consent for it, while the defendant argued it was a standard pre-employment procedure conducted with her. The results, including her HIV-positive status, were sent directly to the employer but not disclosed to her. Soon after, her health status became known to colleagues, leading to discrimination and stigmatisation. Wunmi alleged the company shared her medical information, but the defendant denied this, insisting it maintained confidentiality. The court found that the defendant violated statutory and constitutional rights related to informed consent, privacy, and anti-discrimination. It ruled in favour of the claimant, awarding her compensation for wrongful termination, discrimination, stigmatisation, and emotional distress.

[1] www.nicnadr.gov.ng/judgement/details.php?id=6444

Key Considerations from Case Study 2

Failure to Comply with the Data Minimisation Principle:

The case highlights a breach of the data minimisation principle, which requires that organisations collect only the necessary and relevant personal data for a specific, lawful purpose. In this case, the employer mandated a broad medical test and subsequently obtained the detailed results without adequately defining its necessity or limiting it to job-related health assessments.

Lack of Informed Consent:

Akinola stated that she was not informed about the specific nature of the test, nor was she given an opportunity to provide explicit and voluntary consent before undergoing the medical examination. The court found this to be a violation of statutory and constitutional rights, affirming that consent must be freely given, specific, and informed.

Discriminatory Practices and Unauthorised Disclosure of Confidential Information:

The claimant's HIV-positive status became known to colleagues, leading to stigmatisation and workplace discrimination. While the employer denied sharing this information, the court recognised that such a disclosure, whether deliberate or due to poor data security practices, resulted in reputational harm and workplace discrimination.

Recommendations for organisations based on Case Study 2

- **Adhere to Data Minimisation Principles:** Employers should ensure that health records, especially sensitive information like HIV status, are only collected when it is absolutely necessary. These can be achieved by:
  - **Purpose Limitation:** Only collect health information that is necessary to the job role. Avoid gathering unnecessary data, unless directly relevant to the employee's role.
  - **Data Sharing on a Need-to-Know Basis:** Implement strict controls to ensure that health information is only accessed by designated personnel with professional and ethical responsibilities for handling such data. Where an employee's health status, such as HIV status, is relevant to a specific job requirement (e.g., in healthcare), access should be restricted to those responsible for medical support, or compliance not with the entire team or management.
  - **Data Minimisation in Communications:** If health information needs to be shared, ensure it's done securely and in a way that minimises exposure. For example, instead of sending sensitive data or files via email, use secure channels or send passworded files.
- **Obtain Informed Consent:** In cases where medical tests are absolutely necessary, employers must rely on a lawful basis other than consent. However, when consent is the chosen basis, it must be clear, informed, and voluntary. Employers should ensure that employees fully understand the nature and implications of the tests. This can be achieved by:
  - **Clear Communication:** Provide employees with straightforward information about any required health test, why it's being done, what's involved, and how results will be used.
  - **Voluntary Participation:** Clearly specify which tests are required based on the job role, function, and any applicable legal obligations. Most importantly, indicate which tests are optional. For example, say, "You are not required to participate, and there will be no negative impact on your job if you choose not to."

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Recommendations for organisations based on Case Study 2 *(cont'd)*

- **Privacy and Confidentiality:** Reassure employees that their health status/results will be kept private and only shared with authorised personnel. For instance, explain that HIV test results will be handled confidentially and will not affect employment decisions. If HIV testing is deemed necessary, it should be justified by legitimate job-related requirements, such as roles involving exposure to bloodborne pathogens or other occupational health risks.

- **Train Staff on Data Privacy Principles and Enforce Anti-Discrimination Measures:** Provide training to relevant process owners (eg., HR, Customer Care Representatives, Physical and IT Security, etc.) and management on privacy laws, anti-discrimination policies, and handling sensitive employee health information to prevent similar issues. These can be achieved by:
  - **Regular Data Privacy Training:** Provide ongoing training for strategic process owners on handling sensitive health data (e.g., HIV status) through annual workshops on data protection.
  - **Anti-Discrimination Policies:** Train staff to recognise and prevent discrimination based on health information. Use scenario-based learning to reinforce policies.
  - **Clear Handling Procedures:** Establish clear policies for accessing and sharing sensitive health information, ensuring only authorised personnel can view it. Communicate that violations will lead to disciplinary actions.
  - **Conduct Regular Data Protection Audits:** Organisations should undertake regular audits of their data privacy practices to ensure compliance with relevant privacy laws and practices.

How Can Organisations Balance Health Data Collection with Privacy Laws? - Striking the Balance Between Necessity and Convenience

In the interest of convenience, many employers implement a one-size-fits-all approach to pre-employment medical screening, requiring all candidates to undergo the same standard tests regardless of their specific job roles. While this simplifies administrative processes, it often results in the violation of the principle of data minimisation. This blanket approach not only raises privacy concerns but may also discourage qualified applicants, particularly those who feel uncomfortable disclosing sensitive health information unrelated to their prospective role. Employers must recognise that medical assessments should be limited to the business need, ensuring that only health information relevant to the job role is gathered. By aligning medical screenings with job requirements rather than prioritising administrative ease, organisations can maintain a fair, legally compliant, and ethically responsible recruitment process.

It is generally accepted that certain medical examinations may be necessary to determine whether a candidate is fit for a specific role. For instance, physical fitness tests may be required for jobs involving manual labour or heavy lifting, vision and hearing tests for roles such as driving or operating machinery, and immunisation records or infectious disease screenings for healthcare positions. Similarly, psychological evaluations may be relevant for high-stress jobs. However, employers must ensure that these assessments are directly related to job requirements rather than applied indiscriminately. Employers must carefully evaluate the specific medical requirements for each role and ensure that the data collected is strictly necessary for assessing the candidate's ability to perform the job. Collecting unnecessary data not only violates privacy principles but may also discourage potential candidates from applying.

To reduce privacy risks and simplify the process, obtaining a certificate of fitness from health facilities is considered leading practice. Instead of handling sensitive medical data directly, employers can rely on medical/health facilities to conduct the necessary examinations and issue a certificate confirming whether the candidate is medically fit for the role. This approach ensures that the employer only receives information relevant to their decision-making while leaving the details and test results under the control of the healthcare provider. By adopting this method, employers eliminate the burden of storing and securing sensitive medical data, reducing the risk of privacy breaches.

Employers should ensure that medical assessments are not used as a basis for unfairly excluding candidates or creating discriminatory barriers. Collecting health information without a clear job-related purpose can perpetuate bias, particularly against individuals with disabilities, chronic illnesses, or other medical conditions that do not impair their ability to perform the role. Any additional medical information that is not essential to the role should not be requested, as this could lead to actual or perceived unjustified exclusion or bias against candidates.

Transparent and accountable practices should be adopted to ensure that candidates are properly informed about the reasons medical data is being requested, how it will be used, who will have access to it, and how it will be protected.

Striking the right balance between necessity and convenience in pre-employment medical data processing is essential for protecting candidate privacy and maintaining compliance with data protection laws. Employers should limit their focus to information critical for the role and consider adopting practices like requesting certificates of fitness to avoid handling sensitive medical data directly. Employers should also ensure that medical assessment results are not used to unfairly exclude candidates, perpetuate bias, or create discriminatory barriers. By doing so, they can ensure a fair and lawful recruitment process that respects the privacy of all candidates.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Exploring Scenarios of Possible Violation

Below, we will explore use cases involving the processing of medical data in the workplace, taking cognisance of the principle of data minimisation and examining the rationale for identifying them as a violation of a data protection principle or otherwise.

S/N	Scenario	Data Protection Principle Being Violated	Recommendation based on good practices
1	OGB & Sons ventures require that pre-medical tests be conducted before the employment of its drivers. Part of the tests include tests for Sexually Transmitted Infections (STIs) and genetic predispositions to diseases.	Data Minimisation (Section 24(c) NDPA)	Tests for STIs and genetic predispositions are generally not relevant to the company's advertised job role and this action may constitute an excessive and unjustified intrusion into candidates' private health information. OGB & Sons Ventures is expected to process only data necessary for the purpose required for the job role.
2	SteezeTech requires a basic fitness assessment for all employees but does not collect or store specific health data from the medical diagnostic center; only a "fit" or "unfit" result is recorded in a certificate of fitness. Employees are informed in advance about the specific tests being conducted, which are directly related to their job roles.	None	By limiting its records to the final fitness status ("fit" or "unfit") rather than storing detailed health data, SteezeTech minimises the risk of exposing sensitive information and aligns with data protection best practices. Additionally, ensuring transparency by informing employees about the nature and purpose of the tests reinforces trust and compliance with data minimisation principles.
3	Laolu & Sons Diagnostics Center requires all job applicants including janitors, receptionists, ambulance drivers, etc. to submit details of their family members' medical history as part of the recruitment process for all types of roles. This information is then shared with a medical teaching institute for genetic research, without the knowledge of the job applicants.	• Data Minimisation (Section 24(c) NDPA) • Purpose Limitation (Section 24(d) NDPA) • Lawfulness, Fairness and Transparency (Section 24(a) NDPA)	Collecting excessive and sensitive personal data unrelated to the hiring decision of the diagnostics center violates data minimisation principles. Furthermore, sharing this sensitive health data with a third-party institute for research—without the knowledge of the data subjects and without a valid lawful basis—breaches the principles of transparency, fairness, and lawfulness under the NDPA. Thus, the diagnostics center is expected to review its data collection requirements for job applicants and ensure it aligns with the principle of data mimimisation and purpose limitation. It should collect only job-related information necessary for a job role.
4	Sapa Beverages retains pre-employment health screening data indefinitely, even after candidates are not hired or employees leave the company. There is no data retention policy in place.	• Storage Limitation (Section 24(d), NDPA)	Retaining health data indefinitely without a lawful purpose violates the principle of storage limitation. Beta Sapa Beverages should develop and implement a data retention policy specifying how long personal data is stored and the criteria for its deletion. Unsuccessful applicant data should be securely deleted within a reasonable timeframe.
5	Mustapha Logistics Enterprise uses a third-party recruitment platform that collects applicants' biometric data (e.g., facial scans) for video interviews but does not inform applicants about this in advance.	• Transparency (Section 24(a), NDPA) • Lawfulness and Consent (Section 25, NDPA)	Processing biometric data without clear, prior notice and explicit consent does not align with good practices of data subjects' privacy rights. Mustapha Logistics Enterprise should ensure that all third-party processors comply with the NDPA and provide clear, accessible information about data collection practices. Informed and freely given consent should be obtained before collecting sensitive personal data.

* Please note that the names of companies and organisations mentioned in this table are fictional and have been used for illustrative purposes only.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Examples where these practices have been adopted in other jurisdictions

- The European Data Protection Supervisor (EDPS) agrees with the practice adopted by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) in sharing medical certificates of fitness with the HR team and only sharing medical reports with the EMCDDA Medical Officer. EMCDDA is asked to:
  - Re-assess the data obtained via the medical questionnaire to ensure compliance with the principles of data minimisation and
  - Ensure appropriate data retention for individuals who have undergone medical exams (and whose medical data is being stored) but subsequently decline employment.

  European Data Protection Supervisor's Opinion on EMCDDA's Pre-Employment Medicals
- The ICO in its publication informs that "Organisations should avoid relying on consent unless you are confident you can demonstrate it is freely given. This means that a worker must be able to say 'no' without fear of a penalty being imposed and must be able to withdraw their consent at any time". It is also important to note that ICO advises "it should be left to medical professionals to have access to and interpret detailed medical information for you". Furthermore, the ICO also says "…interpretation of medical information should be left to a suitably qualified health professional".

  https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/information-about-workers-health/data-protection-and-workers-health-information/
- n organisation located in Schiphol, Netherlands, which contracts with an external medical provider, explicitly states in its privacy notice that it only collects 'Certificates of Fitness' from candidates during its recruitment process, rather than full medical reports:

  European Medicine Agency's Data Protection Notice ***(Section 4, Certificate of Fitness)***

Conclusion

In conclusion, balancing health data collection with privacy laws in Nigeria requires a clear examination by the organisation as to what is the basis for collection and why. If an organisation intends to collect and use health information about its employees and job applicants, it must clearly define the reasons for doing so and ensure those reasons are justifiable. These justifications should be documented in a privacy policy, which must be read and understood by the data subject before providing his/her consent to such processing, where applicable.

When relying on consent for health data processing employers should ensure that such consent is freely given, specific, informed, and unambiguous, as the imbalance of power between employers and employees/job seekers can raise questions on the legitimacy of consent. Processing of health data needs to be performed in a transparent manner. This requires that employees or job seekers are clearly informed about what the pre-employment medical tests would cover, how and why their health information is used, etc. Many employers justify the collection of extensive medical data on the grounds of compliance with a legal obligation. However, excessive reliance on this legal basis, without considering privacy principles, can lead to the collection of irrelevant or overly intrusive health information.

Striking the right balance between necessity and convenience in processing health data is essential for protecting employees/job applicants privacy and maintaining compliance with data protection laws. Employers should limit medical data collection to what is strictly necessary to assess a candidate's fitness for a specific role. It is equally critical for employers to embed anti-discriminatory safeguards when processing health data, as this kind of sensitive information, if mishandled, can lead to subtle yet impactful forms of exclusion or bias.

Employers should prioritise data minimisation and align their practices with legal requirements, while employees should be informed of their rights and encouraged to hold organisations accountable. By adopting these measures, a more equitable and privacy-conscious recruitment process can be achieved.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

We would love to have your take

1. How does your organisation balance the need for medical information for its employees and job applicants with the principles of data minimisation?
2. Have you encountered any real-life scenarios where data minimisation practices helped mitigate potential data breaches in your workplace?
3. What challenges have you faced in implementing data minimisation practices during collection of health information for pre-employment medical assessment in your organisation?

Kindly send us your feedback at:
tinyurl.com/4vp33rx7

For further information, contact:

John Anyanwu
Partner & Head,
Cyber & Privacy
KPMG in West Africa
E: john.anyanwu@ng.kpmg.com

Olaoluwa Agbaje
Senior Manager,
Cyber & Privacy
KPMG in West Africa
E: olaoluwa.agbaje@ng.kpmg.com

Contributors

Kudirat Tobi Mustapha
Cyber & Privacy
kudirat.mustapha@ng.kpmg.com

Sandra Eke
Cyber & Privacy
sandra.eke@ng.kpmg.com

Obehi Emiowele
Cyber & Privacy
obehi.emiowele@ng.kpmg.com

Glory Obi
Cyber & Privacy
glory.obi@ng.kpmg.com

home.kpmg/ng
home.kpmg/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.